

Contents

[Azure Stack Edge Documentation](#)

[Azure Stack Edge Pro 2](#)

[Overview](#)

[What is Azure Stack Edge Pro 2?](#)

[Tutorials](#)

[0 - Get checklist](#)

[1 - Order, prepare](#)

[2 - Install](#)

[3 - Connect](#)

[4 - Configure network](#)

[5 - Configure device](#)

[6 - Configure certificates](#)

[7 - Activate](#)

[8 - Configure compute](#)

[Concepts](#)

[Ready safety](#)

[Review requirements](#)

[Understand limits](#)

[Review specifications](#)

[Clustering \(preview\)](#)

[What is clustering?](#)

[Cluster witness](#)

[Kubernetes failover on clustered device](#)

[How to](#)

[Mount your device](#)

[Using a 2-post rackmount](#)

[Using wallmount](#)

[Azure Stack Edge Pro - GPU](#)

[Overview](#)

What is Azure Stack Edge Pro with GPU?

Quickstarts

[Get started](#)

Tutorials

[0 - Get checklist](#)

[1 - Order, prepare](#)

[2 - Install](#)

[3 - Connect](#)

[4 - Configure network](#)

[5 - Configure device](#)

[6 - Configure certificates](#)

[7 - Activate](#)

Concepts

[Review requirements](#)

[For Azure Stack Edge](#)

[For Azure Stack Edge Blob storage](#)

[Understand limits](#)

[Security overview](#)

[Review specifications](#)

[Device specifications](#)

[Power cord specifications](#)

[FAQ - Billing model](#)

[Clustering \(preview\)](#)

[What is clustering?](#)

[Cluster witness](#)

[Cluster failover scenarios](#)

[Cluster management](#)

[Kubernetes failover on clustered device](#)

Azure Stack Edge Pro R

Overview

[What is Azure Stack Edge Pro R?](#)

Concepts

[Ready safety](#)

[Review requirements](#)

[Understand limits](#)

[Review specifications](#)

Tutorials

[0 - Get checklist](#)

[1 - Order, prepare](#)

[2 - Install](#)

[3 - Connect](#)

[4 - Configure network](#)

[5 - Configure device](#)

[6 - Configure security](#)

[7 - Activate](#)

[8 - Configure compute](#)

How to

[Configure VPN \(preview\)](#)

[Configure via Azure PowerShell](#)

[Configure for BCDR](#)

Azure Stack Edge Mini R

Overview

[What is Azure Stack Edge Mini R?](#)

Concepts

[Ready safety](#)

[Review requirements](#)

[Understand limits](#)

[Review specifications](#)

Tutorials

[0 - Get checklist](#)

[1 - Order, prepare](#)

[2 - Install](#)

[3 - Connect](#)

[4 - Configure network](#)

- 5 - Configure device
- 6 - Configure security
- 7 - Activate
- 8 - Configure compute

How to

- Configure VPN (preview)
- Configure via Azure PowerShell
- Configure for BCDR
- Manage Wi-Fi
- Use Wi-Fi profiles

Shared features - Pro 2, Pro GPU, Pro R, Mini R

Local Azure Resource Manager

- What is local Azure Resource Manager?
- Connect via Azure PowerShell
- Set Azure Resource Manager password
- Configure client TLS settings
- Troubleshoot Azure Resource Manager issues

Certificates

- What are certificates?
- View requirements
- Create certificates
 - Via Azure PowerShell
 - Via Azure Stack Readiness Checker tool
- Prepare certificates to upload on device
- Upload, import, view expiry
- Troubleshoot certificate errors

Virtual machines

- What are VMs?
- View supported VMs
- View supported API profiles
- What are GPU VMs?
- Create VM image

[Custom image from Azure VM](#)

[Windows generalized image from VHD](#)

[Generalized image from ISO](#)

[Use specialized image](#)

[Use Azure Marketplace image](#)

[Deploy](#)

[VMs - Azure portal \(preview\)](#)

[VMs - templates](#)

[VMs - GPU](#)

[VMs - HPN](#)

[VMs - Azure PowerShell cmdlets](#)

[VMs - Azure PowerShell script](#)

[VMs - Azure CLI/Python](#)

[Install extensions](#)

[Custom script extension](#)

[GPU extension](#)

[Password reset extension](#)

[Manage](#)

[Network interfaces](#)

[Disks](#)

[Edge resource groups](#)

[VM sizes](#)

[Virtual switches](#)

[VM tags](#)

[Reset VM password](#)

[Back up VM disks](#)

[Monitor](#)

[VM metrics](#)

[VM activity](#)

[Troubleshoot](#)

[Connect to VM console](#)

[Collect VM guest logs](#)

- VM image upload
- VM deployment
- GPU extension issues

Kubernetes

- What is Kubernetes?
- Kubernetes storage
- Kubernetes networking
- Kubernetes RBAC
- Kubernetes workloads
- Configure Kubernetes
- Deploy Kubernetes workloads

Via kubectl

- Kubernetes cluster access
- Compute acceleration
- Stateless app
- Statically provisioned stateful app
- Dynamically provisioned stateful app
- GPU shared workload

Via IoT Edge

- Stateless app
- GPU shared workload
- Develop C# module

Via Azure Arc

- Enable Arc on Kubernetes cluster
- Deploy stateless app via GitOps
- Deploy Azure Arc Data Controller

How to

- Configure MetallB

IoT Edge

- Deploy IoT Edge samples (Self-serve)
- IoT Edge on VM
- Nvidia DeepStream module

[Deploy IoT Edge samples \(Managed\)](#)

- [Module from Nvidia gallery](#)
- [GPU module from Git repo](#)
- [GPU module via Marketplace](#)
- [Modules from FPGA devices](#)
- [Module via Azure portal](#)
- [Sync data from local share](#)

[Troubleshoot IoT Edge issues](#)

[Cloud storage gateway](#)

- [Add, connect to share](#)
- [Add, connect to storage accounts](#)
- [Shares](#)
- [Users](#)
- [Storage accounts](#)
- [Bandwidth schedules](#)
- [Troubleshoot blob storage issues](#)

[Shared device - Pro 2, Pro GPU, Pro R, Mini R](#)

[Shared concepts](#)

- [Understand region selection](#)
- [What is GPU sharing?](#)
- [Understand data residency](#)
- [Understand data resiliency](#)
- [View key vault integration](#)
- [Understand disconnected use](#)
- [FAQ - Operational guidelines](#)

[Shared security](#)

- [Security overview](#)
- [Security baseline](#)

[Shared how-tos](#)

- [Check network readiness](#)
- [Manage Edge compute](#)
- [Manage Edge container registry](#)

Manage device

- Power, access, connectivity
- Via PowerShell
- Apply updates
- Reset, reactivate device
- Return device
- Replace device
- Prepare for device failure
- Recover from device failure

Monitor

- Review alerts
- Use rules for alert notifications
- Use metrics charts
- Use Kubernetes dashboard
- Use Azure Monitor

Troubleshoot

- Ordering issues
- Activation issues
- Device logs and diagnostics
- Enable proactive logging
- Enable remote support
- Contact Microsoft Support

Shared release notes

[2207 - Current](#)

[2205](#)

[2203](#)

[2202](#)

[2111](#)

[2110](#)

[2106](#)

[2105](#)

[2103](#)

2101

2010

2008

Shared reference

Azure PowerShell

REST API

.NET SDK

Azure CLI

Azure Policy built-ins

Azure Stack Edge Pro - FPGA

Overview

What is Azure Stack Edge Pro with FPGA?

Tutorials

1 - Prepare

2 - Install

3 - Connect, set up, activate

4 - Add, connect to share

5A - Configure compute (simple)

5B - Configure compute (advanced)

Concepts

Review requirements

Understand limits

Security overview

Review specifications

Device specifications

Power cord specifications

How to

Develop C# module

Manage

Edge compute

Edge compute network

Shares

[Users](#)

[Bandwidth schedules](#)

[Power, access, connectivity](#)

[Via PowerShell](#)

[Troubleshoot](#)

[Via logs](#)

[Ordering issues](#)

[IoT Edge](#)

[Contact Microsoft Support](#)

[Monitor](#)

[Return device](#)

[Replace device](#)

[Migrate to GPU device](#)

[Release notes](#)

[2101 - Current](#)

[2007](#)

[1911](#)

[1906](#)

[1905](#)

[General availability \(GA\)](#)

[Resources](#)

[Azure Stack Edge Pro C# module samples \(.NET\)](#)

[Azure Stack Edge product](#)

[Pricing](#)

[Azure Stack Edge Hardware Additional Terms](#)

What is Azure Stack Edge Pro 2?

9/21/2022 • 6 minutes to read • [Edit Online](#)

Azure Stack Edge Pro 2 is a new generation of an AI-enabled edge computing device offered as a service from Microsoft. This article provides you an overview of the Azure Stack Edge Pro 2 solution. The overview also details the benefits, key capabilities, and the scenarios where you can deploy this device.

The Azure Stack Edge Pro 2 offers the following benefits over its precursor, the Azure Stack Edge Pro series:

- This series offers multiple models that closely align with your compute, storage, and memory needs. Depending on the model you choose, the compute acceleration could be via one or two Graphical Processing Units (GPU) on the device.
- This series has flexible form factors with multiple mounting options. These devices can be rack mounted, mounted on a wall, or even placed on a shelf in your office.
- These devices have low acoustic emissions and meet the requirements for noise levels in an office environment.

Use cases

The Pro 2 series is designed for deployment in edge locations such as retail, telecommunications, manufacturing, or even healthcare. Here are the various scenarios where Azure Stack Edge Pro 2 can be used for rapid Machine Learning (ML) inferencing at the edge and preprocessing data before sending it to Azure.

- **Inference with Azure Machine Learning** - With this solution, you can run ML models to get quick results that can be acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models. For more information, see how to [Deploy Azure ML hardware accelerated models on Azure Stack Edge](#).
- **Preprocess data** - Transform data before sending it to Azure via compute options such as containerized workloads and Virtual Machines to create a more actionable dataset. Preprocessing can be used to:
 - Aggregate data.
 - Modify data, for example, to remove personal data.
 - Subset data to optimize storage and bandwidth, or for further analysis.
 - Analyze and react to IoT Events.
- **Transfer data over network to Azure** - Use this solution to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

Key capabilities

Azure Stack Edge Pro 2 has the following capabilities:

CAPABILITY	DESCRIPTION
Accelerated AI inferencing	Enabled by the compute acceleration card. Depending on your compute needs, you may choose a model that comes with one, two or no Graphical Processing Units (GPUs). For more information, see Technical specifications for Azure Stack Edge Pro 2 .

CAPABILITY	DESCRIPTION
Edge computing	<p>Supports VM and containerized workloads to allow analysis, processing, and filtering of data.</p> <p>For information on VM workloads, see VM overview on Azure Stack Edge.</p> <p>For containerized workloads, see Kubernetes overview on Azure Stack Edge</p>
Data access	<p>Direct data access from Azure Storage Blobs and Azure Files using cloud APIs for additional data processing in the cloud. Local cache on the device is used for fast access of most recently used files.</p>
Cloud-managed	Device and service are managed via the Azure portal.
Offline upload	Disconnected mode supports offline upload scenarios.
Supported file transfer protocols	<p>Support for standard Server Message Block (SMB), Network File System (NFS), and Representational state transfer (REST) protocols for data ingestion.</p> <p>For more information on supported versions, see Azure Stack Edge Pro 2 system requirements.</p>
Data refresh	<p>Ability to refresh local files with the latest from cloud.</p> <p>For more information, see Refresh a share on your Azure Stack Edge.</p>
Double encryption	<p>Use self-encrypting drives to provide a layer of encryption. BitLocker support to locally encrypt data and secure data transfer to cloud over https. For more information, see Configure encryption-at-rest</p>
Bandwidth throttling	<p>Throttle to limit bandwidth usage during peak hours.</p> <p>For more information, see Manage bandwidth schedules on your Azure Stack Edge.</p>
Easy ordering	<p>Bulk ordering and tracking of the device via Azure Edge Hardware Center.</p> <p>For more information, see Order a device via Azure Edge Hardware Center.</p>
Specialized network functions	<p>Use the Marketplace experience from Azure Network Function Manager to rapidly deploy network functions. The functions deployed on Azure Stack Edge include mobile packet core, SD-WAN edge, and VPN services.</p> <p>For more information, see What is Azure Network Function Manager? (Preview).</p>
Scale out file server	<p>The device is available as a single node or a two-node cluster.</p> <p>For more information, see What is clustering on Azure Stack Edge devices? (Preview).</p>

Components

The Azure Stack Edge Pro 2 solution consists of Azure Stack Edge resource, Azure Stack Edge Pro 2 physical device, and a local web UI.

- **Azure Stack Edge Pro 2 physical device** - A compact 2U device supplied by Microsoft that can be configured to send data to Azure.



To procure a device, go to the Azure Edge Hardware Center and place an order. Azure Edge Hardware Center service lets you choose from a variety of Azure Stack Edge SKUs as per your business need. You can order multiple units of a device type, ship multiple devices to different locations, save addresses for future orders, and also track the status of your orders.

Once the order is delivered, you can configure your device and create an Azure Stack Edge resource to manage the device.

For more information, go to [Create an order for your Azure Stack Edge Pro 2 device](#).

- **Azure Stack Edge resource** - A resource in the Azure portal that lets you manage an Azure Stack Edge Pro 2 device from a web interface that you can access from different geographical locations. Use the Azure Stack Edge resource to create and manage resources, view, and manage devices and alerts, and manage shares.
- **Azure Stack Edge Pro 2 local web UI** - A browser-based local user interface on your Azure Stack Edge Pro 2 device primarily intended for the initial configuration of the device. Use the local web UI also to run diagnostics, shut down and restart the device, or view copy logs.

The local web UI on the device currently supports the following languages with their corresponding language codes:

LANGUAGE	CODE	LANGUAGE	CODE	LANGUAGE	CODE
English {default}	en	Czech	cs	German	de
Spanish	es	French	fr	Hungarian	hu
Italian	it	Japanese	ja	Korean	ko
Dutch	nl	Polish	pl	Portuguese - Brazil	pt-br
Portuguese - Portugal	pt-pt	Russian	ru	Swedish	sv
Turkish	tr	Chinese - simplified	zh-hans	Chinese - traditional	zh-hant

For information about using the web-based UI, go to [Use the web-based UI to administer your Azure Stack Edge](#).

Region availability

The Azure Stack Edge Pro 2 physical device, Azure resource, and target storage account to which you transfer data don't all have to be in the same region.

- **Resource availability** - For this release, the resource is available in East US, West EU, and South East Asia regions.
- **Device availability** - You should be able to see Azure Stack Edge Pro 2 as one of the available SKUs when placing the order.

For a list of all the countries/regions where the Azure Stack Edge Pro 2 device is available, go to **Availability** section in the **Azure Stack Edge Pro** tab for [Azure Stack Edge Pro 2 pricing](#).
- **Destination Storage accounts** - The storage accounts that store the data are available in all Azure regions. The regions where the storage accounts store Azure Stack Edge Pro 2 data should be located close to where the device is located for optimum performance. A storage account located far from the device results in long latencies and slower performance.

Azure Stack Edge service is a non-regional service. For more information, see [Regions and Availability Zones in Azure](#). Azure Stack Edge service doesn't have dependency on a specific Azure region, making it resilient to zone-wide outages and region-wide outages.

To understand how to choose a region for the Azure Stack Edge service, device, and data storage, see [Choosing a region for Azure Stack Edge](#).

Billing and pricing

These devices can be ordered via the Azure Edge Hardware center. These devices are billed as a monthly service through the Azure portal. For more information, see [Azure Stack Edge Pro 2 pricing](#).

Next steps

- Review the [Azure Stack Edge Pro 2 system requirements](#).
- Understand the [Azure Stack Edge Pro 2 limits](#).
- Deploy [Azure Stack Edge Pro 2](#) in Azure portal.

Deployment checklist for your Azure Stack Edge Pro 2 device

9/21/2022 • 5 minutes to read • [Edit Online](#)

This article describes the information that can be gathered ahead of the actual deployment of your Azure Stack Edge Pro 2 device.

Use the following checklist to ensure you have this information after you've placed an order for an Azure Stack Edge Pro 2 device and before you've received the device.

Deployment checklist

STAGE	PARAMETER	DETAILS
Device management	<ul style="list-style-type: none">- Azure subscription.- Resource providers registered.- Azure Storage account.	<ul style="list-style-type: none">- Enabled for Azure Stack Edge, owner or contributor access.- In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for Microsoft.EdgeOrder and register. Repeat for Microsoft.Devices if deploying IoT workloads.- Need access credentials.
Device installation	One power cable in the package.	For more information, see the list of Supported power cords by country
	<ul style="list-style-type: none">- At least one X 1-GbE RJ-45 network cable for Port 1.- At least 100-GbE QSFP28 Passive Direct Attached Cable (tested in-house) for each data network interface Port 3 and Port 4 to be configured.- At least one 100-GbE network switch to connect a 1 GbE or a 100-GbE network interface to the Internet for data.	Customer needs to procure these cables. For a full list of supported cables, modules, and switches, see Connect-X6 DX adapter card compatible firmware .
First-time device connection	Laptop whose IPv4 settings can be changed. This laptop connects to Port 1 via a switch or a USB to Ethernet adapter.	
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.

STAGE	PARAMETER	DETAILS
Network settings	<p>Device comes with 2 x 10/1-GbE, 2 x 100-GbE network ports.</p> <ul style="list-style-type: none"> - Port 1 is used to configure management settings only. One or more data ports can be connected and configured. - At least one data network interface from among Port 2 to Port 4 needs to be connected to the Internet (with connectivity to Azure). - DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.
Advanced networking settings	<ul style="list-style-type: none"> - Require 2 free, static, contiguous IPs for Kubernetes nodes, and one static IP for IoT Edge service. - Require one additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	Web proxy server IP/FQDN, port	HTTPS URLs are not supported.
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	<p>Configure primary and secondary NTP server on local network.</p> <ul style="list-style-type: none"> - If local server isn't available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public windows update server is used.
Device settings	<ul style="list-style-type: none"> - Device fully qualified domain name (FQDN). - DNS domain. 	
(Optional) Certificates	<p>To test non-production workloads, use Generate certificates option</p> <p>If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.</p>	Configure certificates only if you change the device name and/or DNS domain.
Activation	Require activation key from the Azure Stack Edge resource.	Once generated, the key expires in three days.
STAGE	PARAMETER	DETAILS

Stage	Parameter	Details
Device management	<ul style="list-style-type: none"> - Azure subscription - Resource providers registered - Azure Storage account 	<p>Enabled for Azure Stack Edge, owner or contributor access.</p> <p>- In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for <code>Microsoft.EdgeOrder</code> and register.</p> <p>Repeat for <code>Microsoft.Devices</code> if deploying IoT workloads.</p> <ul style="list-style-type: none"> - Need access credentials
Device installation	One power cable in the package per device node.	<p>For more information, see the list of Supported power cords by country</p>
	<ul style="list-style-type: none"> - At least two 1-GbE RJ-45 network cables for Port 1 on the two device nodes - You would need two 1-GbE network cables to connect Port 2 on each device node to the internet. <p>Depending on the network topology you wish to deploy, you may also need at least one 100-GbE QSFP28 Passive Direct Attached Cable (tested in-house) to connect Port 3 and Port 4 across the device nodes.</p> <ul style="list-style-type: none"> - You would also need at least one 10/1-GbE network switch to connect Port 1 and Port 2. You would need a 100/10-GbE switch to connect Port 3 or Port 4 network interface to the Internet for data. 	<p>Customer needs to procure these cables and switches. Exact number of cables and switches would depend on the network topology that you deploy.</p> <p>For a full list of supported cables, modules, and switches, see Connect-X6 DX adapter card compatible firmware.</p>
First-time device connection	Via a laptop whose IPv4 settings can be changed. This laptop connects to Port 1 via a switch or a USB to Ethernet adapter.	
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.
Network settings	<p>Device comes with 2 x 10/1-GbE network ports, Port 1 and Port 2. Device also has 2 x 100-GbE network ports, Port 3 and Port 4.</p> <ul style="list-style-type: none"> - Port 1 is used for initial configuration. Port 2, Port 3, and Port 4 are also connected and configured. - At least one data network interface from among Port 2 - Port 4 needs to be connected to the Internet (with connectivity to Azure). - DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.

Stage	Parameter	Details
Advanced networking settings	<ul style="list-style-type: none"> - Require 3 free, static, contiguous IPs for Kubernetes nodes, and one static IP for IoT Edge service. - Require one additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	Web proxy server IP/FQDN, port	HTTPS URLs are not supported.
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	Configure primary and secondary NTP server on local network. If local server isn't available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public windows update server is used.
Device settings	<ul style="list-style-type: none"> - Device fully qualified domain name (FQDN) - DNS domain 	
(Optional) Certificates	<p>To test non-production workloads, use Generate certificates option</p> <p>If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.</p>	Configure certificates only if you change the device name and/or DNS domain.
Activation	Require activation key from the Azure Stack Edge resource.	Once generated, the key expires in three days.

Next steps

Prepare to deploy your [Azure Stack Edge Pro device](#).

Tutorial: Prepare to deploy Azure Stack Edge Pro 2

9/21/2022 • 11 minutes to read • [Edit Online](#)

This tutorial is the first in the series of deployment tutorials that are required to completely deploy Azure Stack Edge Pro 2. This tutorial describes how to prepare the Azure portal to deploy an Azure Stack Edge resource.

You need administrator privileges to complete the setup and configuration process. The portal preparation takes less than 20 minutes.

In this tutorial, you learn how to:

- Create a new resource
- Get the activation key

Get started

For Azure Stack Edge Pro 2 deployment, you need to first prepare your environment. Once the environment is ready, follow the required steps and if needed, optional steps and procedures to fully deploy the device. The step-by-step deployment instructions indicate when you should perform each of these required and optional steps.

STEP	DESCRIPTION
Preparation	These steps must be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information before and during the deployment.
Deployment prerequisites	These prerequisites validate that the environment is ready for deployment.
Deployment tutorials	These tutorials are required to deploy your Azure Stack Edge Pro 2 device in production.
1. Prepare the Azure portal for Azure Stack Edge Pro 2	Create and configure your Azure Stack Edge resource before you install an Azure Stack Box Edge physical device.
2. Install Azure Stack Edge Pro 2	Unpack, rack, and cable the Azure Stack Edge Pro 2 physical device.
3. Connect to Azure Stack Edge Pro 2	Once the device is installed, connect to its local web UI.
4. Configure network settings for Azure Stack Edge Pro 2	Configure network including the compute network and web proxy settings for your device.
5. Configure device settings for Azure Stack Edge Pro 2	Assign a device name and DNS domain, configure update server and device time.
6. Configure security settings for Azure Stack Edge Pro 2	Configure certificates for your device. Use device-generated certificates or bring your own certificates.

STEP	DESCRIPTION
7. Activate Azure Stack Edge Pro 2	Use the activation key from service to activate the device. The device is ready to set up SMB or NFS shares or connect via REST.
8. Configure compute	Configure the compute role on your device. A Kubernetes cluster is also created.
9A. Transfer data with Edge shares	Add shares and connect to shares via SMB or NFS.
9B. Transfer data with Edge storage accounts	Add storage accounts and connect to blob storage via REST APIs.

You can now begin to gather information regarding the software configuration for your Azure Stack Edge Pro 2 device.

Deployment configuration checklist

Before you deploy your device, you need to collect information to configure the software on your Azure Stack Edge Pro 2 device. Preparing some of this information ahead of time helps streamline the process of deploying the device in your environment. Use the [Azure Stack Edge Pro 2 deployment configuration checklist](#) to note down the configuration details as you deploy your device.

Prerequisites

Following are the configuration prerequisites for your Azure Stack Edge resource, your Azure Stack Edge Pro 2 device, and the datacenter network.

For the Azure Stack Edge resource

Before you begin, make sure that:

- Your Microsoft Azure subscription is enabled for an Azure Stack Edge resource. Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#).
- You have owner or contributor access at resource group level for the Azure Stack Edge, IoT Hub, and Azure Storage resources.
- To create an order in the Azure Edge Hardware Center, you need to make sure that the Microsoft.EdgeOrder provider is registered. For information on how to register, go to [Register resource provider](#).
- To create any Azure Stack Edge resource, you should have permissions as a contributor (or higher) scoped at resource group level. You also need to make sure that the `Microsoft.DataBoxEdge` provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create any IoT Hub resource, make sure that Microsoft.Devices provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create a Storage account resource, again you need contributor or higher access scoped at the resource group level. Azure Storage is by default a registered resource provider.
- You have admin or user access to Azure Active Directory Graph API. For more information, see [Azure Active Directory Graph API](#).
- You have your Microsoft Azure storage account with access credentials.

For the Azure Stack Edge Pro 2 device

Before you begin, make sure that:

- You've reviewed the safety information for this device at: [Safety guidelines for your Azure Stack Edge device](#).
- You have a 2U slot available in a standard 19" rack in your datacenter if you plan to mount the device on a rack.
- You have access to a flat, stable, and level work surface where the device can rest safely.
- The site where you intend to set up the device has standard AC power from an independent source or a rack power distribution unit (PDU) with an uninterruptible power supply (UPS).
- You have access to a physical device.

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured per the networking requirements for your Azure Stack device. For more information, see [Azure Stack Edge Pro 2 System Requirements](#).
- For normal operating conditions of your Azure Stack Edge, you have:
 - A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
 - A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Create a new resource

If you have an existing Azure Stack Edge resource to manage your physical device, skip this step and go to [Get the activation key](#).

Create an order

You can use the Azure Edge Hardware Center to explore and order various hardware from the Azure hybrid portfolio including Azure Stack Edge Pro 2 devices.

When you place an order through the Azure Edge Hardware Center, you can order multiple devices, to be shipped to more than one address, and you can reuse ship to addresses from other orders.

Ordering through Azure Edge Hardware Center will create an Azure resource that will contain all your order-related information. One resource each will be created for each of the units ordered. You'll have to create an Azure Stack Edge resource after you receive the device to activate and manage it.

To place an order through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.
2. Select **+ Create a resource**. Search for and select **Azure Edge Hardware Center**. In the Azure Edge Hardware Center, select **Create**.

Home > Create a resource > Marketplace >

Azure Edge Hardware Center

Microsoft



Azure Edge Hardware Center

Microsoft
☆☆☆☆ 0.0 (0 ratings)

[Create](#)

Overview Plans Usage Information + Support Reviews

Use Azure Edge Hardware Center to order first-party Azure hardware that lets you build and run hybrid apps across datacenters, edge locations, remote offices and the cloud.

Azure Edge Hardware Center lets you choose from a variety of hardware as per your business need and helps you keep track of all the ordered hardware at a single place.

More offers from Microsoft [See All](#)

 Workspace Microsoft Virtual Machine Azure Virtual Desktop resource	 Microsoft HPC Pack 2012 R2 Microsoft Virtual Machine Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux workloads.	 Windows 10 IoT Core Services Microsoft Azure Service Commercialize your project with enterprise-grade security and support	 Web App + SQL Microsoft Azure Service Enjoy secure and flexible development, deployment, and scaling options for your web app
--	--	--	--

[Create](#) [Create](#) [Create](#) [Create](#)

3. Select a subscription, and then select **Next**.

Home > Create a resource > Marketplace > Azure Edge Hardware Center >

Get started ...

Get started [...](#) [X](#)

Info Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select a subscription

Select a subscription to manage deployed resources and costs.

Subscription [Contoso_USEast](#)

[Next](#)

4. To start your order, select **Order** beside the product family that you want to order - for example, **Azure Stack Edge**. If you don't see the product family, you may need to use a different subscription; select **Try selecting a different subscription**.

Get started



i Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select product family

Showing 1 product families for selected subscription: ExpressPod BVT (Creates order in BVT env)

Azure Stack Edge

Azure managed physical edge compute device

Order

Can't see the product family you are looking for? [Try selecting a different subscription.](#)

5. Select the shipping destination for your order.

Azure Edge Hardware Center



i Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select shipping destination

Azure Stack Edge

Order to be billed against subscription: Contoso_USWest ([Change](#))

Select the country/region where you would like your device to be shipped. *

United States

Next

6. On the **Select Hardware** page, use the **Select** button to select the hardware product to order. For example, here **Azure Stack Edge Pro - GPU** was selected.

 Select Hardware ... X

Hardware family: Azure Stack Edge ([Change](#)) Subscription: Contoso_USWest Ship to country/region: United States

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Device specifications	<ul style="list-style-type: none"> • 1U rack mount device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Azure Private Edge Zones enabled 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Pro R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Portable, server class device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Specialized rugged casing tailored for harsh environments 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Mini R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Ultra-portable, WiFi enabled device with battery • Hardware accelerated ML using VPU • Specialized rugged casing tailored for harsh environments 	\$\$\$ USD	Select

After you select a hardware product, you'll select the device configuration to order. For example, if you chose Azure Stack Edge Pro - GPU, you can choose from Azure Stack Edge Pro - 1 GPU and Azure Stack Edge Pro - 2 GPU models.

7. Select the device configuration, and then choose **Select**. The available configurations depend on the hardware you selected. The screen below shows available configurations for Azure Stack Edge Pro - GPU devices.

If you're ordering Azure Stack Edge Mini R devices, which all have the same configuration, you won't see this screen.

Home >
Select Hardware ...

Hardware family: Azure Stack Edge ([Change](#)) Azure managed physical edge compute device

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Hardware specifications	<p>Azure Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. The device is powered with NVIDIA T4 GPUs to provide accelerated AI inferencing at the edge. You can choose from the available configurations with one or two GPUs basis your business need</p> <p>Select a configuration</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Usable compute</th> <th>Usable memory</th> <th>Usable storage</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> <tr> <td><input type="radio"/> Azure Stack Edge Pro - 2 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> </tbody> </table> <p>Learn more Azure Stack Edge Pro - GPU documentation</p>				Model	Usable compute	Usable memory	Usable storage	<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB	<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB
Model	Usable compute	Usable memory	Usable storage													
<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB													
<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB													

Select

The **Create order** wizard opens.

8. On the **Basics** tab, provide an **Order name**, **Resource group**, and **Region**. Then select **Next: Shipping + quantity >**.

Create order

X

Basics Shipping + quantity Notifications Tags Review + create

Hardware details

 Azure Stack Edge Pro - 1 GPU

Usable compute : 40 vCPU Usable memory : 102 GB

Usable storage : 4.2 TB

Order details

Order name *

Pro1GPUdevices

The selected subscription will be used to manage deployed resources and billing. Select or create a new resource group to organize and manage all your resources.

Subscription *

Contoso_USEast

Resource group *

USEast_ASE



[Create new](#)

Region *

East US



Review + create

< Previous

Next : Shipping + quantity >

Next, you'll add each ship to address you want to send devices to and then specify how many devices to send to each address. You can order up to 20 units (devices) per order.

9. On the **Shipping + quantity** tab, add each ship to address to send devices to:

- To add a new ship to address, select **Add a new address**.

A required **Address alias** field on the **New address** screen identifies the address for later use. Select **Add** when you finish filling in the address fields. Then use **Select address(es)** to add the address to your order.

- To use a ship to address from a previous order, or to use an address that you just added, choose **Select address(es)**. Then, on the **Select address(es)** screen, select one or more addresses, and choose **Select**.

<input type="checkbox"/>	Contact person	Address
<input checked="" type="checkbox"/>	Gus Poland 4255555555 gusp@contoso.com Contoso LE	contoso-redmond One Microsoft Way Building 52 Redmond WA 98152 United States
<input type="checkbox"/>	Gus Poland 4085555555 gusp@contoso.com Contoso LE	contoso-sunnyvale 1020 Enterprise Way Building 2 Sunnyvale CA 94089 United States
<input checked="" type="checkbox"/>	Claudia Olivares 4085555555 gusp@contoso.com Contoso LE	SVBldg2 1020 Enterprise Way Building 2 Sunnyvale

The **Shipping + quantity** tab now has a separate item for each ship to address.

Each order item name includes a name prefix (the order name followed by the address alias), with an item number for each device that is shipped to that address.

Create order

Basics **Shipping + quantity** Notifications Tags Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Su CA 94089 US	1	Pro1GPUDevicesSVBldg2-01 Order name Address alias Item #
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01

[Review + create](#)
 [< Previous](#)
 [Next : Notifications >](#)

- For each address, enter the **Quantity** of devices to ship on the **Shipping + quantity** tab.

When you enter a quantity of more than one, a **+n more** label appears after the order item name.

Create order

Basics **Shipping + quantity** Notifications Tags Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Sunnyva CA 94089 US	3	Pro1GPUDevicesSVBldg2-... +2 more [Delete]
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01 [Delete]

[Add a new address](#)
 [Select address\(es\)](#)

[Review + create](#)
 [< Previous](#)
 [Next : Notifications >](#)

- If you want to change the names of order items, select and click the order item name to open the **Rename order item** pane. If you're shipping more than one item to an address, select **+n more**.

You can make two types of name change:

- To use a different name prefix for all of the order items, edit the **Name prefix** and then select

Apply, as shown on the following screen.

- You can also edit the name of each order item individually.

When you finish, select **Done**.

Select **Next: Notifications** > to continue.

12. If you want to receive status notifications as your order progresses, enter the email address for each recipient on the **Notifications** tab.

To add an email address, enter the address, and select **Add**. You can add up to 20 email addresses.

The screenshot shows the 'Create order' interface. At the top, there's a breadcrumb trail: Home > Select Hardware >. Below it is a title bar with 'Create order' and a close button ('X'). The main area has several tabs: Basics, Shipping + quantity, Notifications (which is highlighted with a red box), Tags, and Review + create. A note below the tabs states: 'We will update you regarding your order progress. You can specify up to 20 email address(es) to receive updates for your order status. Your subscription owner and admin will receive email notifications by default.' Under the 'Email' section, there's a text input field containing 'claudiao@contoso.com' and a blue 'Add' button. Below this, two email addresses are listed: 'gusp@contoso.com' and 'OpsMgmt@contoso.com', each with a 'Remove' link. At the bottom, there are navigation buttons: a blue 'Review + create' button (also highlighted with a red box), '< Previous', and 'Next : Tags >'.

When you finish, select **Review + create** to continue.

13. On the **Review + create** tab:

- Review your order. The order is automatically validated when you open this screen. If you see a **Validation failed** banner, you'll have to fix the issues before you create the order.
- Review the **Privacy terms**, and select the check box to agree to them.
- Select **Create**.



Create order

X

Validation passed.

Basics Shipping + quantity Notifications Tags Review + create

Order name Pro1GPUdevices

Total hardware units 4

Total monthly service fee <Fee>

Total shipping fee <Fee>

Hardware details

Azure Stack Edge Pro - 1 GPU

Usable compute 40 vCPU

Usable memory 102 GB

Usable storage 4.2 TB

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Basics

Subscription Contoso_USEast

Resource Group USEast_ASE

Region East US

Notifications

Emails gusp@contoso.com, OpsMgmt@contoso.com

Shipping + quantity

Total hardware units (4)

Shipping address	Order item name
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-01
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-02
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-03
contoso-sunnyvale, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicescontoso-su-01

Create

< Previous

Next >

During deployment, the order opens in the portal, with the status of each order item displayed. After deployment completes, you may need to click the Down arrow by **Deployment details** to see the status of individual items.

Resource	Type	Status	Operation details
SVBldg2	Microsoft.EdgeOrder/addresses	OK	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	OK	Operation details
Pro1GPUDevicesSunnyvale2-02	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-03	Microsoft.EdgeOrder/orderItems	OK	Operation details

- To view details for an order item, shown below, select the item in the **Resource** column of the deployment details.

Order item information			
Placed on	: 8/6/2021	Shipping address	1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US
Order name	: Pro1GPUDevices	Contact information	Claudia Olivares 4085550111, claudiao@contoso.com
View Updates			

Hardware information	
Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage	
While your hardware arrives, configure your infrastructure. Learn more	

- After a device ships (**Shipped** tag is green), a **Configure hardware** option is added to the item details. Select that option to create a management resource for the device in Azure Stack Edge.

The screenshot shows the Azure Edge Hardware Center interface for an order named 'DemoOrderASAdd1-03'. The 'Overview' tab is selected. Key details shown include:

- Resource group: USEast_ASE
- Location: eastus2euap
- Subscription: Contoso_USEast
- Subscription ID: 1a23bc45-678d-90f1-2ghi-j34klm6n6780
- Tags: Ordered, Shipped (highlighted with a red box), Delivered
- Order name: Pro1GPUDevices
- Order item name: Pro1GPUDevicesSunnyvale2-02 -03
- Placed on: 6/24/2021
- Order name: DemoOrderAS
- Shipping address: abc street, xyz city, pqr state 7698798 US
- Contact information: Anam Shaher, 8768789798, ashaher@hotmail.com
- Hardware information: Azure Stack Edge Pro - 1 GPU: 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage
- Configure hardware button (highlighted with a red box)

The subscription, resource group, and deployment area are filled in from the order, but you can change them.

The screenshot shows the 'Create management resource' wizard for an Azure Stack Edge device. The 'Basics' tab is selected. The device details are:

Device	Order resource name	Status
Azure Stack Edge Pro - 1 GPU	DemoOrderASAdd1-03	Delivered

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * (Contoso_USEast)
 Resource group * (USEast_ASE)
 Create new

INSTANCE DETAILS

Name * () Deploy Azure resource in * (US) East US

Review + create Previous Next: Tags

After you activate the device, you'll be able to open the management resource from the item, and open the order item from the management resource.

Create a management resource for each device

To create a management resource for a device ordered through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.

2. There are two ways to get started creating a new management resource:

- Through the Azure Edge Hardware Center: Search for and select **Azure Edge Hardware Center**. In the Hardware Center, display **All order items**. Select the item **Name**. In the item **Overview**, select **Configure hardware**.

The **Configure hardware** option appears after a device is shipped.



- In Azure Stack Edge: Search for and select **Azure Stack Edge**. Select **+ Create**. Then select **Create management resource**.



The **Create management resource** wizard opens.

3. On the **Basics** tab, enter the following settings:

SETTING	VALUE
Select a subscription ¹	Select the subscription to use for the management resource.
Resource group ¹	Select the resource group to use for the management resource.
Name	Provide a name for the management resource.
Deploy Azure resource in	Select the country or region where the metadata for the management resource will reside. The metadata can be stored in a different location than the physical device.

¹ An organization may use different subscriptions and resource groups to order devices than they use to manage them.

The screenshot shows the "Create management resource" wizard on the "Basics" tab. The URL in the address bar is "Home > Create a resource > Azure Stack Edge > Manage Azure Stack Edge > Create management resource".

The "Basics" tab is selected. A callout box points to the "Select a subscription" dropdown, which is set to "DataBox_Edge_Test". Below it, the "Resource group" dropdown is set to "myaserg".

The "PROJECT DETAILS" section includes fields for "Name" (set to "myasetestorder") and "Deploy Azure resource in" (set to "(US) East US").

At the bottom, there are buttons for "Review + create", "Previous", and "Next: Tags".

Select **Review + create** to continue.

4. On the **Review + create** tab, review basic settings for the management resource and the terms of use. Then select **Create**.

If you started this procedure by clicking **Configure hardware** for a delivered item in an Azure Edge Hardware Center order, the device, order resource name, and order status are listed at the top of the screen.

Terms of use'. Under the 'Basics' section, details are shown: Subscription 'ExpressPod BVT (Creates order in BVT env)', Resource group 'nidhitest', Name 'myNewDevice', and Region '(US) East US'. A note below says: 'Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.' At the bottom are 'Create', 'Previous', and 'Next' buttons."/>

Home > Azure Edge Hardware Center > nidhitest1nidhiaddr-04 >

Create management resource

Azure Stack Edge

All validations have passed.

Basics Tags Review + create

Device	Order resource name	Status
Azure Stack Edge Pro - 2 GPU	nidhitest1nidhiaddr-04	Delivered

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Basics

Subscription	ExpressPod BVT (Creates order in BVT env)
Resource group	nidhitest
Name	myNewDevice
Region	(US) East US

Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.

Create Previous Next

The **Create** button isn't available until all validation checks have passed.

5. When the process completes, the **Overview** pane for new resource opens.

Home > Sunnyvale-ASE1GPUdevices-01 | Overview

Deployment

Search (Ctrl+ /) <> Delete Cancel Redeploy Refresh

Overview

We'd love your feedback! →

Your deployment is complete

Deployment name: Sunnyvale-ASE1GPUdevices-01 Start time: 6/29/2021, 6:04:02 PM
Subscription: Azure Data Box testing Correlation ID: bee14110-d803-4ff4-82a5-6f7e1420d216
Resource group: ContosoEastRG

Deployment details (Download)

Resource	Type	Status	Operation details
Sunnyvale-ASE1GPUdevice	Microsoft.DataBoxEdge/...	OK	Operation details

Next steps

Go to resource

Security Center
Secure your apps and infrastructure
[Go to Azure security center >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

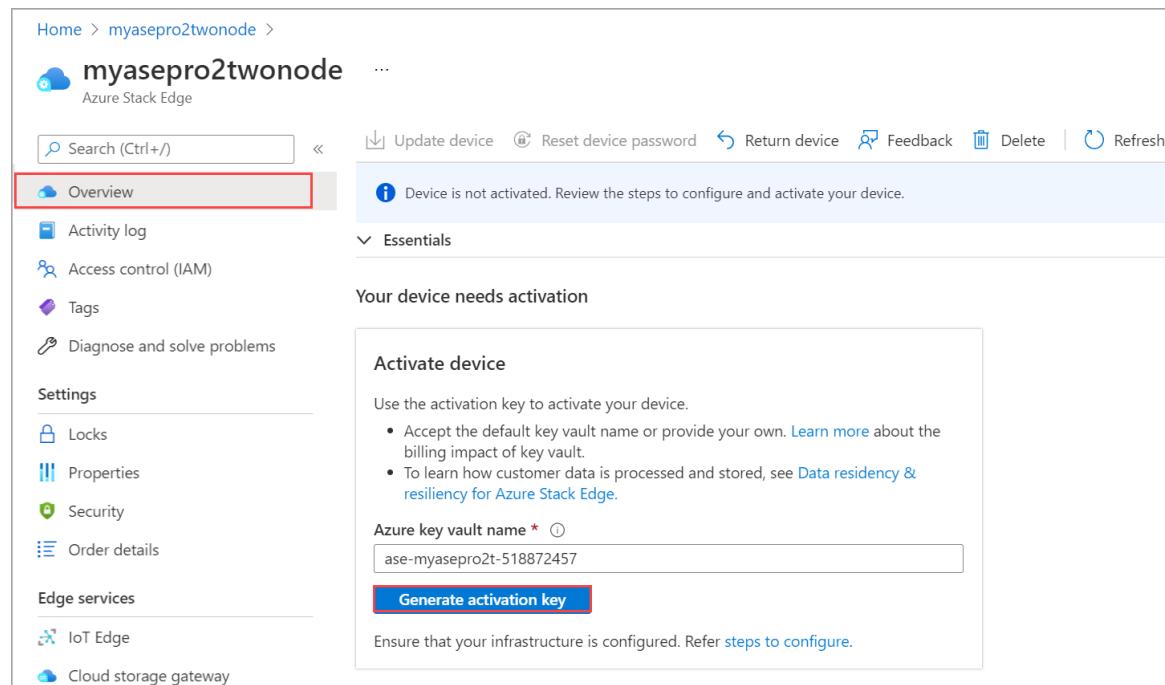
Get the activation key

After the Azure Stack Edge resource is up and running, you'll need to get the activation key. This key is used to activate and connect your Azure Stack Edge Pro 2 device with the resource. You can get this key now while you are in the Azure portal.

1. Select the resource you created, and select **Overview**.
2. In the right pane, enter a name for the Azure Key Vault or accept the default name. The key vault name can be between 3 and 24 characters.

A key vault is created for each Azure Stack Edge resource that is activated with your device. The key vault lets you store and access secrets, for example, the Channel Integrity Key (CIK) for the service is stored in the key vault.

Once you've specified a key vault name, select **Generate key** to create an activation key.



The screenshot shows the Azure Stack Edge resource overview page for a resource named "myasepro2twonode". The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Security, Order details), and Edge services (IoT Edge, Cloud storage gateway). The main content area displays a message: "Device is not activated. Review the steps to configure and activate your device." Below this, under the "Essentials" section, there's a box titled "Your device needs activation" containing instructions to "Activate device" using an activation key. It includes a note about accepting the default key vault name or providing one, and a link to "Data residency & resiliency for Azure Stack Edge". A text input field shows the key vault name "ase-myasepro2t-518872457" and a blue button labeled "Generate activation key". At the bottom of the box, it says "Ensure that your infrastructure is configured. Refer [steps to configure](#)".

Wait a few minutes while the key vault and activation key are created. Select the copy icon to copy the key and save it for later use.

IMPORTANT

- The activation key expires three days after it is generated.
- If the key has expired, generate a new key. The older key is not valid.

Next steps

In this tutorial, you learned about Azure Stack Edge Pro 2 articles such as:

- Create a new resource
- Get the activation key

Advance to the next tutorial to learn how to install Azure Stack Edge Pro 2.

[Install Azure Stack Edge Pro 2](#)

Tutorial: Install Azure Stack Edge Pro 2

9/21/2022 • 11 minutes to read • [Edit Online](#)

This tutorial describes how to install an Azure Stack Edge Pro 2 physical device. The installation procedure involves unpacking, rack mounting, and cabling the device.

The installation can take around two hours to complete.

This tutorial describes how to install a two-node Azure Stack Edge Pro 2 device cluster. The installation procedure involves unpacking, rack mounting, and cabling the device.

The installation can take around 2.5 to 3 hours to complete.

In this tutorial, you learn how to:

- Unpack the device
- Rack mount the device
- Cable the device

Prerequisites

The prerequisites for installing a physical device as follows:

For the Azure Stack Edge resource

Before you begin, make sure that:

- You've completed all the steps in [Prepare to deploy Azure Stack Edge Pro 2](#).
 - You've created an Azure Stack Edge resource to deploy your device.
 - You've generated the activation key to activate your device with the Azure Stack Edge resource.

For the Azure Stack Edge Pro 2 physical device

Before you deploy a device:

- Make sure that the device rests safely on a flat, stable, and level work surface.
- Verify that the site where you intend to set up has:
 - Standard AC power from an independent source.

-OR-

- A power distribution unit (PDU) with an uninterruptible power supply (UPS).
- An available 2U slot on the rack on which you intend to mount the device. If you wish to wall mount your device, you should have a space identified on the wall or a desk where you intend to mount the device.

For the network in the datacenter

Before you begin:

- Review the networking requirements for deploying Azure Stack Edge Pro 2, and configure the datacenter network per the requirements. For more information, see [Azure Stack Edge Pro 2 networking requirements](#).
- Make sure that the minimum Internet bandwidth is 20 Mbps for optimal functioning of the device.

Unpack the device

This device is shipped in a single box. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, don't open it. Contact Microsoft Support to help you assess whether the device is in good working order.
3. Unpack the box. After unpacking the box, make sure that you have:
 - One single enclosure Azure Stack Edge Pro 2 device.
 - One power cord.
 - One packaged bezel.
 - A pair of packaged Wi-Fi antennas in the accessory box.
 - One packaged mounting accessory which could be:
 - A 4-post rack slide rail, or
 - A 2-post rack slide, or
 - A wall mount (may be packaged separately).
 - A safety, environmental, and regulatory information booklet.

This device is shipped in two boxes. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, don't open it. Contact Microsoft Support to help you assess whether the device is in good working order.
3. Unpack the box. After unpacking the box, make sure that you have the following in each box:
 - One single enclosure Azure Stack Edge Pro 2 device.
 - One power cord.
 - One packaged bezel.
 - A pair of packaged Wi-Fi antennas in the accessory box.
 - One packaged mounting accessory which could be:
 - A 4-post rack slide rail, or
 - A 2-post rack slide, or
 - A wall mount (may be packaged separately).
 - A safety, environmental, and regulatory information booklet.

If you didn't receive all of the items listed here, [Contact Microsoft Support](#). The next step is to mount your device on a rack or wall.

Rack mount the device

The device can be mounted using one of the following mounting accessory:

- A 4-post rackmount.
- A 2-post rackmount.
- A wallmount.

If you have received 4-post rackmount, use the following procedure to rack mount your device. For other mounting accessories, see [Racking using a 2-post rackmount](#) or [Mounting the device on the wall](#).

If you decide not to mount your device, you can also place it on a desk or a shelf.

Prerequisites

- Before you begin, make sure to read the [Safety instructions](#) for your device.
- Begin installing the rails in the allotted space that is closest to the bottom of the rack enclosure.
- For the rail mounting configuration:
 - You need to use 10L M5 screws. Make sure that these are included in your rail kit.
 - You need a Phillips head screwdriver.

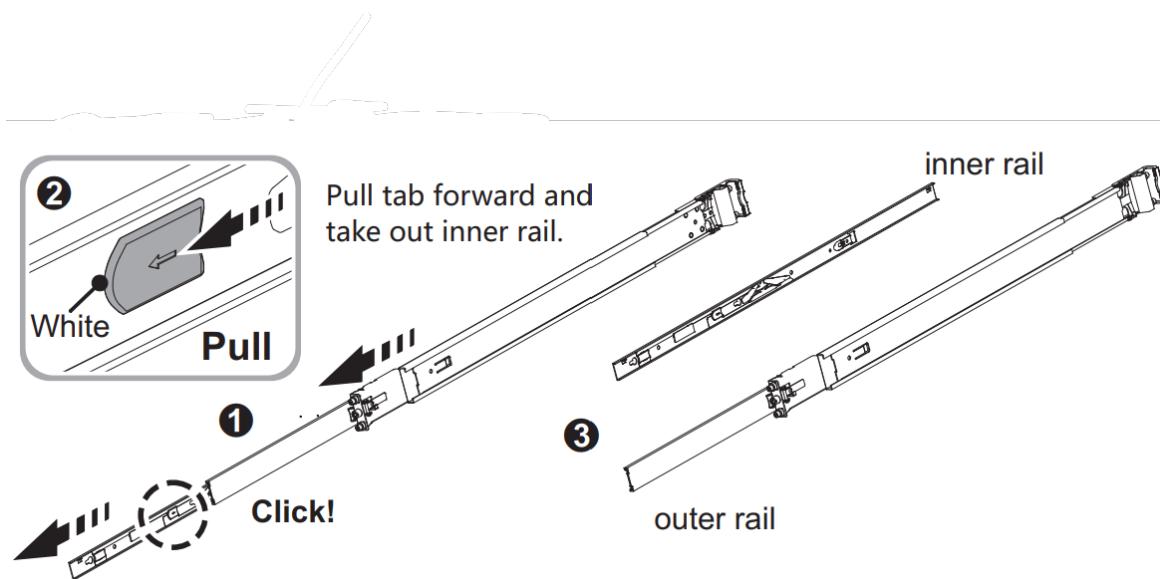
Identify the rail kit contents

Locate the components for installing the rail kit assembly:

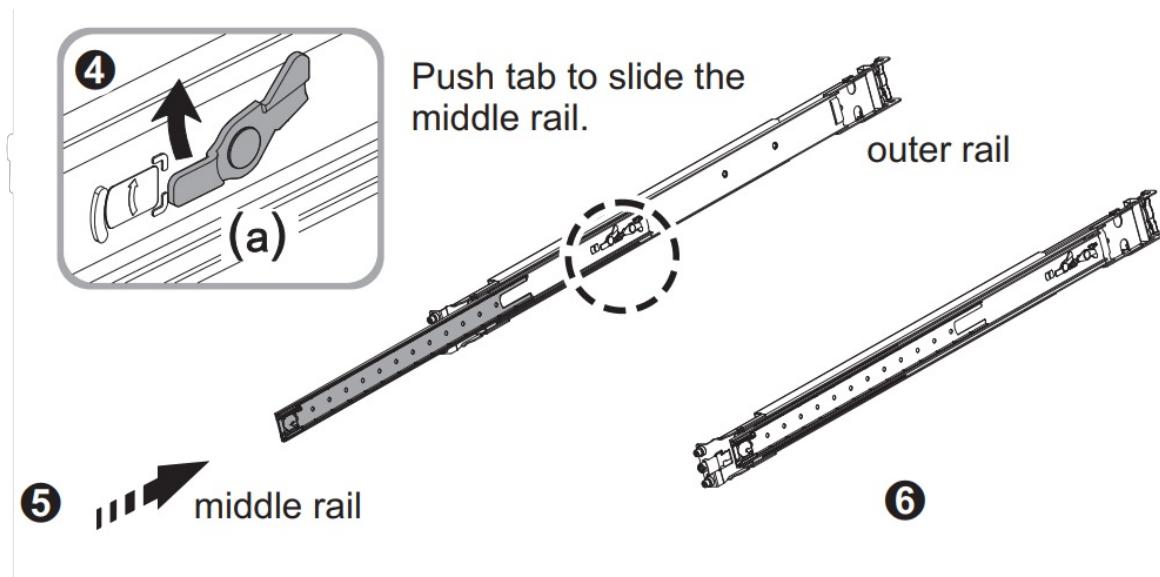
- Inner rails.
- Chassis of your device.
- 10L M5 screws.

Install rails

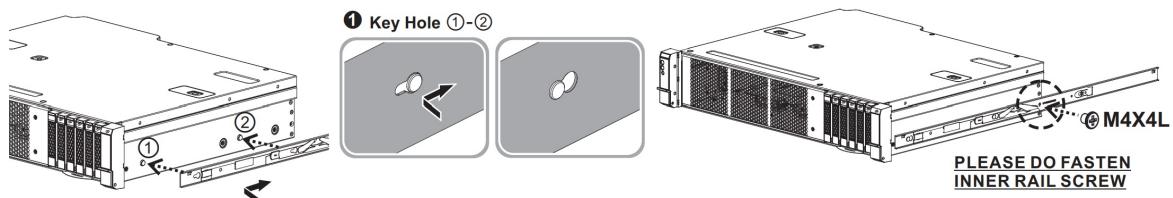
1. Remove the inner rail.



2. Push and slide the middle rail back.

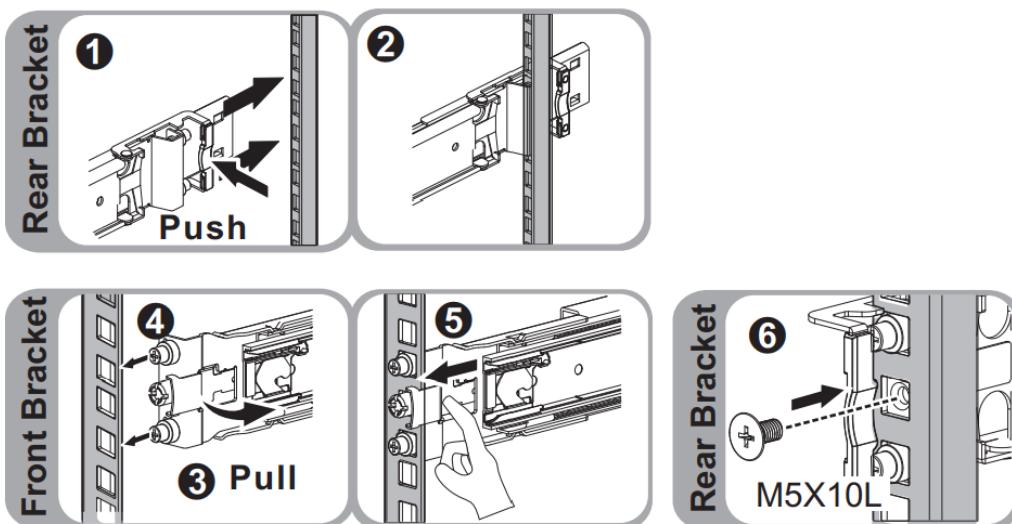


3. Install the inner rail onto the chassis. **Make sure to fasten the inner rail screw.**

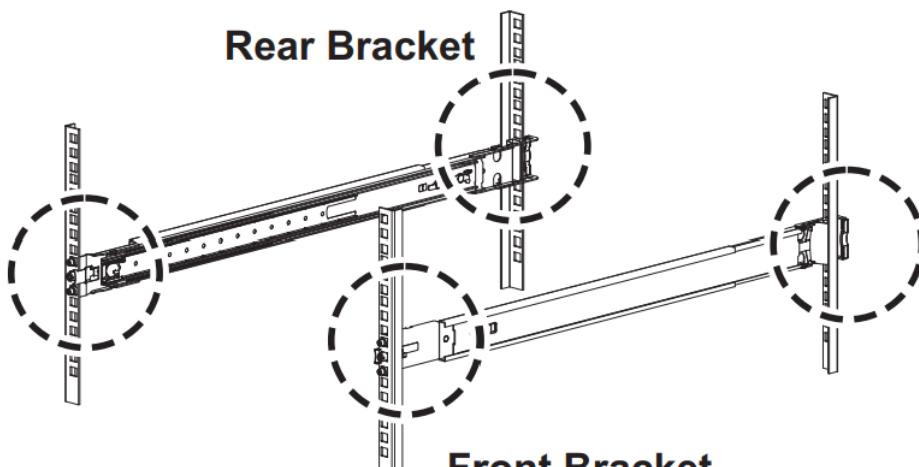


4. Fix the outer rail and the bracket assembly to the frame. Ensure the latch is fully engaged with the rack post.

1 → 2 → 3 → 4 → 5 → 6

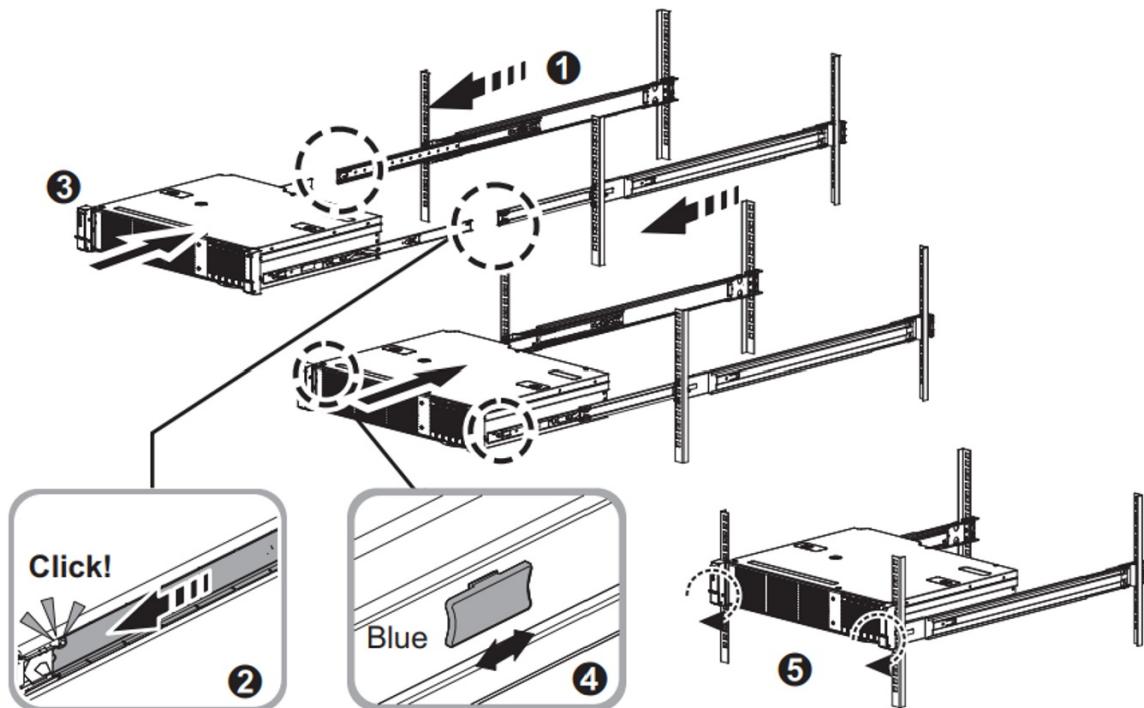


Rear Bracket



5. Insert the chassis to complete the installation.

- Pull the middle rail so that it is fully extended in lock position. Ensure the ball bearing retainer is located at the front of the middle rail (reference diagrams 1 and 2).
- Insert the chassis into the middle rail (reference diagram 3).
- Once you hit a stop, pull and push the blue release tab on the inner rails (reference diagram 4).
- Tighten the M5 screws of the chassis to the rail once the server is seated (reference diagram 5).



If deploying a two-node device cluster, make sure to mount both the devices on the rack or the wall.

Install the bezel

After the device is mounted on a rack, install the bezel on the device. Bezel serves as the protective face plate for the device.

1. Locate two fixed pins on the right side of the bezel, and two spring-loaded pins on the left side of the bezel.
2. Insert the bezel in at an angle with fixed pins going into holes in right rack ear.
3. Push  shaped latch to the right, move left side of bezel into place, then release the latch until the spring pins engage with holes in left rack ear.



4. Lock the bezel in place using the provided security key.



Cable the device

The following procedures explain how to cable your Azure Stack Edge Pro 2 device for power and network.

Cabling checklist

Before you start cabling your device, you need the following things:

- Your Azure Stack Edge Pro 2 physical device, unpacked, and rack mounted.
- One power cable (included in the device package).
- At least one 1-GbE RJ-45 network cable to connect to the Port 1. Port 1 and Port 2 the two 10/1-GbE network interfaces on your device.
- One 100-GbE QSFP28 passive direct attached cable (Microsoft validated) for each data network interface Port 3 and Port 4 to be configured. Here is an example of the QSFP28 DAC connector:



For a full list of supported cables, modules, and switches, see [Connect-X6 DX adapter card compatible firmware](#).

- Access to one power distribution unit.
- At least one 100-GbE network switch to connect a 10/1-GbE or a 100-GbE network interface to the internet for data. At least one data network interface from among Port 2, Port 3, and Port 4 needs to be connected to the Internet (with connectivity to Azure).
- A pair of Wi-Fi antennas (included in the accessory box).

Before you start cabling your device, you need the following things:

- Your two Azure Stack Edge Pro 2 physical devices, unpacked, and rack mounted.
- One power cable for each device node (included in the device package).
- Access to one power distribution unit for each device node.
- At least two 1-GbE RJ-45 network cables per device to connect to Port 1 and Port2. These are the two 10/1-GbE network interfaces on your device.
- A 100-GbE QSFP28 passive direct attached cable (Microsoft validated) for each data network interface Port 3 and Port 4 to be configured on each device. The total number needed would depend on the network topology you will deploy. Here is an example QSFP28 DAC connector:



For a full list of supported cables, modules, and switches, see [Connect-X6 DX adapter card compatible firmware](#).

- At least one 100-GbE network switch to connect a 1-GbE or a 100-GbE network interface to the internet for data for each device.
- A pair of Wi-Fi antennas (included in the accessory box).

NOTE

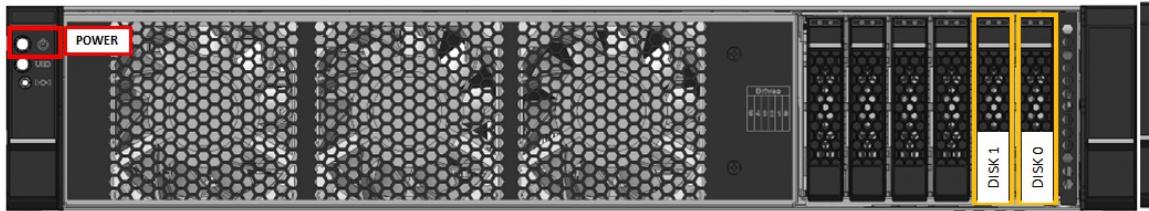
The Azure Stack Edge Pro 2 device should be connected to the datacenter network so that it can ingest data from data source servers.

Device front panel

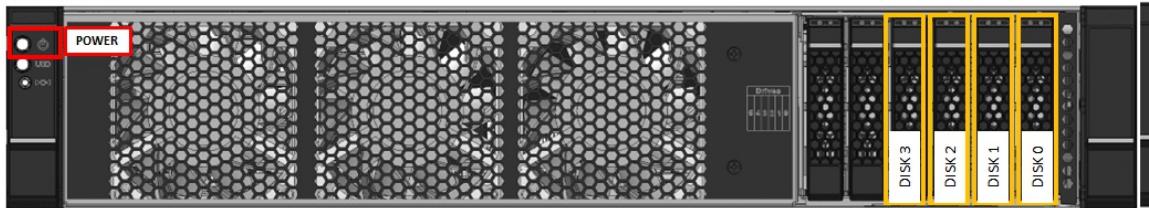
On your device:

- The front panel has disk drives and a power button. The front panel has:
 - Has six disk slots in the front of your device.
 - Has 2, 4, or 6 data disks in the 6 available slots depending on the specific hardware configuration.

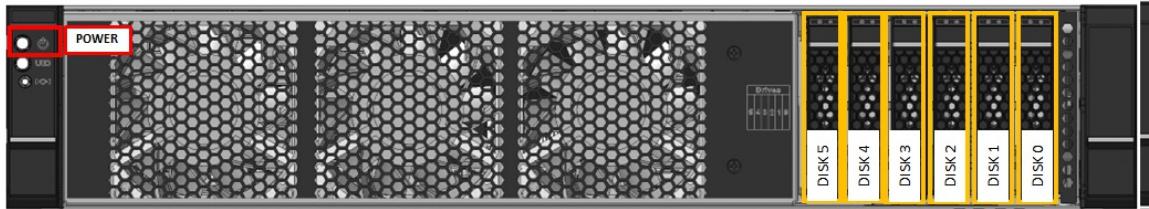
64G2T



128G4T1GPU



256G6T2GPU

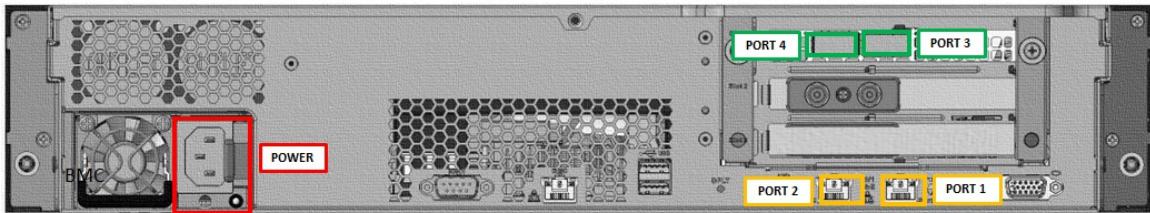


Device back plane

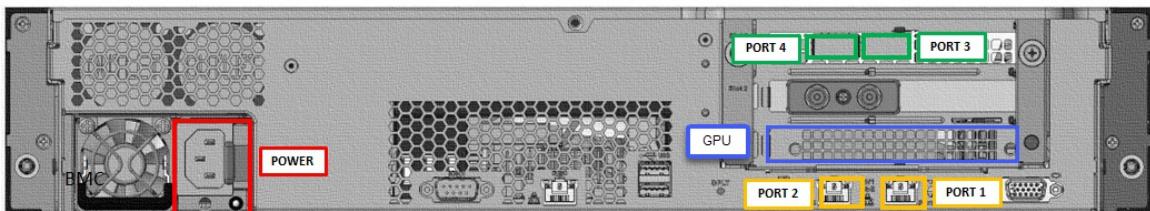
On your device:

- The back plane has:
 - Four network interfaces:
 - Two 10/1-Gbps interfaces, Port 1 and Port 2.
 - Two 100-Gbps interfaces, Port 3 and Port 4.
 - A baseboard management controller (BMC).
 - One network card corresponding to two high-speed ports and two built-in 10/1-GbE ports:
 - **Intel Ethernet X722 network adapter** - Port 1, Port 2.
 - **Mellanox dual port 100 GbE ConnectX-6 Dx network adapter** - Port 3, Port 4. See a full list of [Supported cables, switches, and transceivers for ConnectX-6 Dx network adapters](#).
 - Two Wi-Fi Sub miniature version A (SMA) connectors located on the faceplate of PCIe card slot located below Port 3 and Port 4. The Wi-Fi antennas are installed on these connectors.
 - Two, one, or no Graphical Processing Units (GPUs).

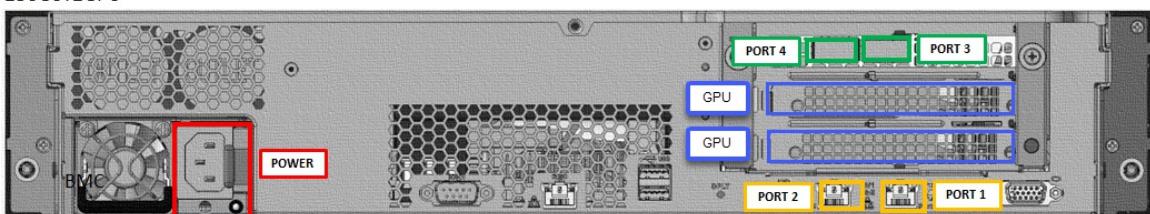
64G2T



128G4T1GPU



256G6T2GPU



Power cabling

Follow these steps to cable your device for power:

1. Identify the various ports on the back plane of your device.
2. Locate the disk slots and the power button on the front of the device.
3. Connect the power cord to the PSU in the enclosure.
4. Attach the power cord to the power distribution unit (PDU).
5. Press the power button to turn on the device.

Follow these steps to cable your device for power:

1. Identify the various ports on the back plane of each device.
2. Locate the disk slots and the power button on the front of each device.
3. Connect the power cord to the PSU in each device enclosure.
4. Attach the power cords from the two devices to two different power distribution units (PDU).
5. Press the power buttons on the front panels to turn on both the devices.

Wi-Fi antenna installation

Follow these steps to install Wi-Fi antennas on your device:

1. Locate the two Wi-Fi SMA RF threaded connectors on the back plane of the device. These gold-colored connectors are located on the faceplate of PCIe card slot, right below Port 3 and Port 4.
2. Use a clockwise motion to thread the antennas onto the SMA connectors. Secure them using only your fingers. Do not use a tool or wrench.

NOTE

Tighten the connectors sufficiently so that the antenna's rotary joints can turn without causing the threaded connectors to become loose.

3. To position the antennas as desired, articulate the hinge and turn the rotary joint.

Network cabling

Follow these steps to cable your device for network:

1. Connect the 10/1-GbE network interface Port 1 to the computer that's used to configure the physical device. Port 1 is used for the initial configuration of the device.

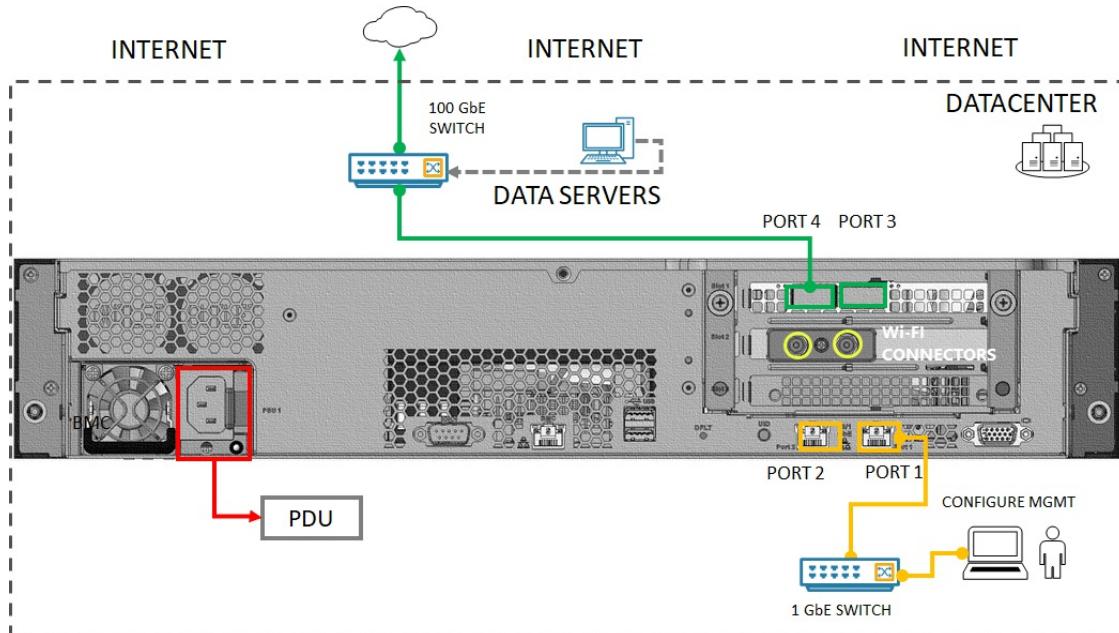
NOTE

If connecting the computer directly to your device (without going through a switch), use a crossover cable or a USB Ethernet adapter.

2. Connect one or more of Port 2, Port 3, Port 4 to the datacenter network/internet.

- If connecting Port 2, use the 1-GbE RJ-45 network cable.
- For the 100-GbE network interfaces, use the QSFP28 passive direct attached cable (tested in-house).

The back plane of a cabled device would be as follows:



NOTE

Using USB ports to connect any external device, including keyboards and monitors, is not supported for Azure Stack Edge devices.

The two-node device can be configured in the following different ways:

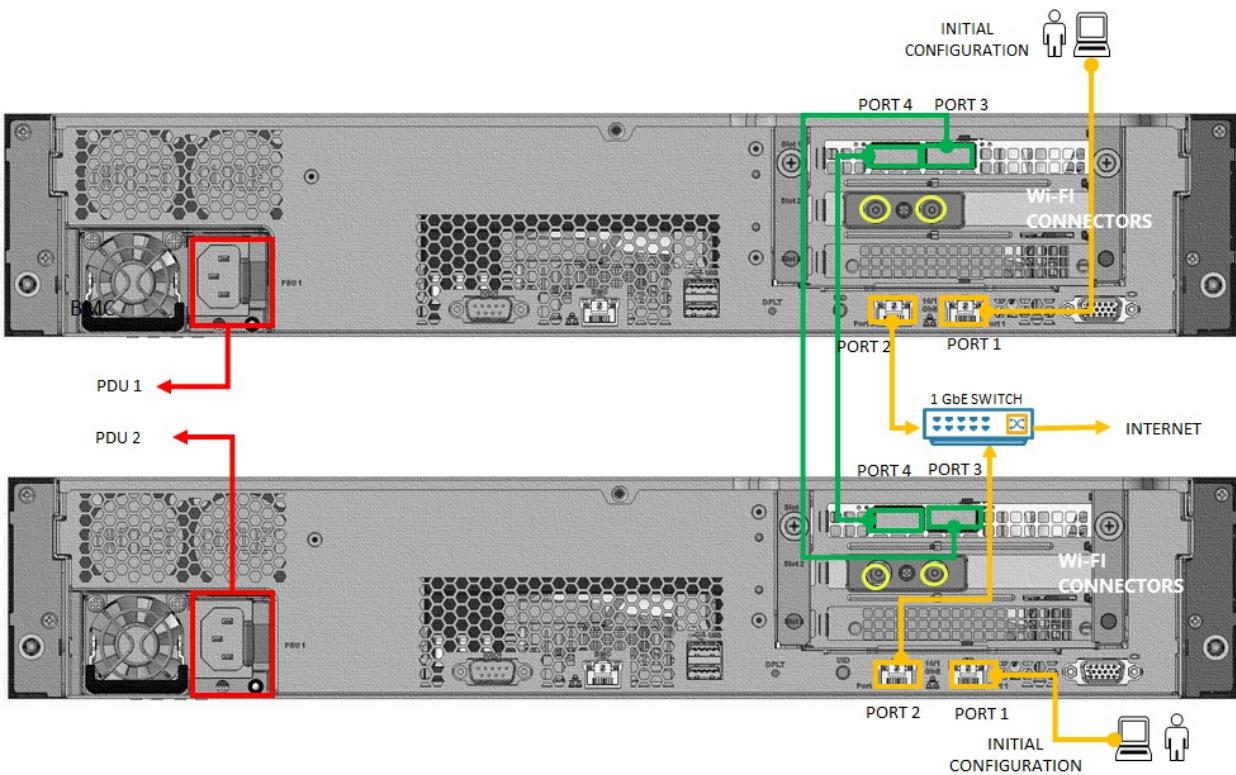
- Without switches
- Using external switches

Each of these configurations is described in the following sections. For more information on when to use these configurations, see [Supported network topologies](#).

Switchless

This configuration is used when high speed switches are not available.

Cable your device as shown in the following diagram:



1. Connect Port 1 on each node to a computer using an Ethernet crossover cable or a USB Ethernet adapter for the initial configuration of the device.
2. Connect Port 2 on each node to a 1-GbE switch via a 1-GbE RJ-45 network cable. If available, a 10-GbE switch can also be used.
3. Connect Port 3 on one device directly (without a switch) to the Port 3 on the other device node. Use a QSFP28 passive direct attached cable (tested in-house) for the connection.
4. Connect Port 4 on one device directly (without a switch) to the Port 4 on the other device node. Use a QSFP28 passive direct attached cable (tested in-house) for the connection.

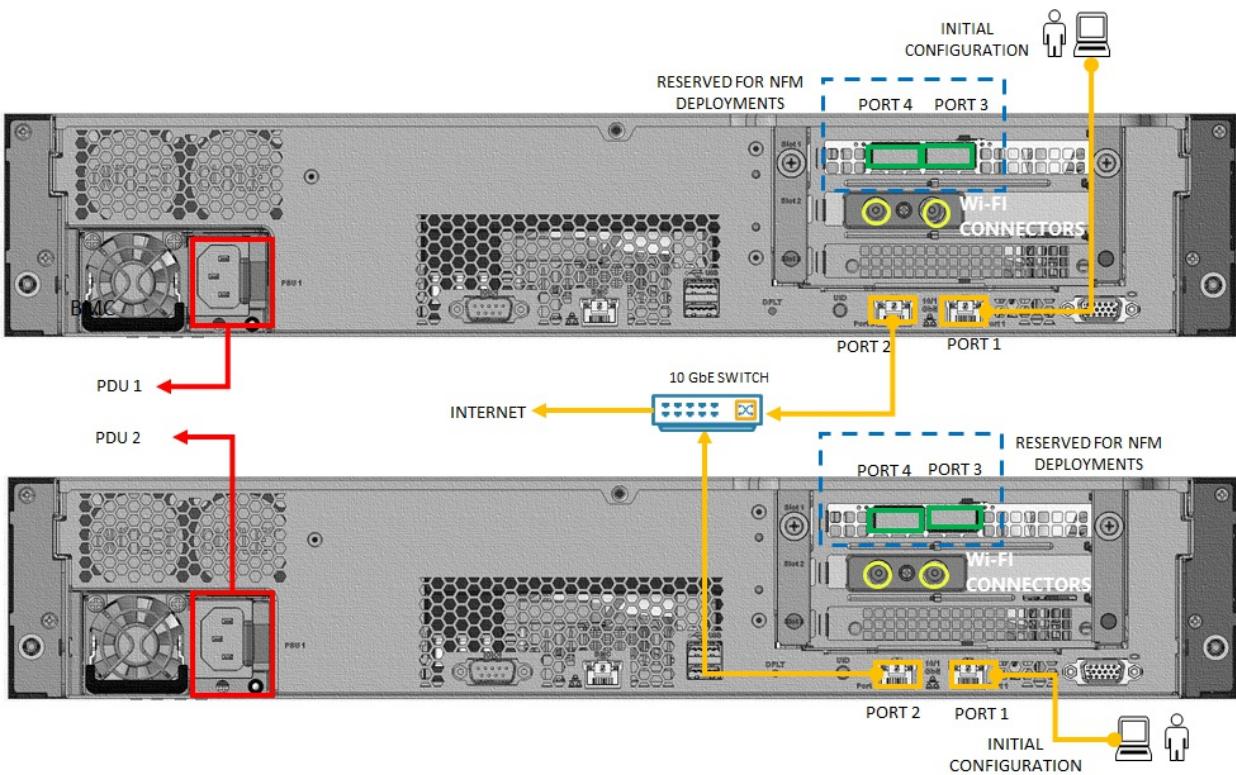
NOTE

Using USB ports to connect any external device, including keyboards and monitors, is not supported for Azure Stack Edge devices.

Using external switches

This configuration is used for Network Function Manager (NFM) workload deployments and requires 10-GbE high speed switches.

Cable your device as shown in the following diagram:



1. Connect Port 1 on each node to a computer using a crossover cable or a USB Ethernet adapter for the initial configuration of the device.
2. Connect Port 2 on each node to a 10-GbE high-speed switch via a 10-GbE RJ-45 network cable. A high speed switch must be used.
3. Port 3 and Port 4 are reserved for NFM workload deployments and must be connected accordingly.

Next steps

In this tutorial, you learned how to:

- Unpack the device
- Rack the device
- Cable the device

Advance to the next tutorial to learn how to connect to your device.

[Connect Azure Stack Edge Pro 2](#)

Tutorial: Connect to Azure Stack Edge Pro 2

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how you can connect to your Azure Stack Edge Pro 2 device by using the local web UI.

The connection process can take around 5 minutes to complete.

This tutorial describes how you can connect to the local web UI on your two-node Azure Stack Edge Pro 2 device.

The connection process can take around 10 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Connect to a physical device

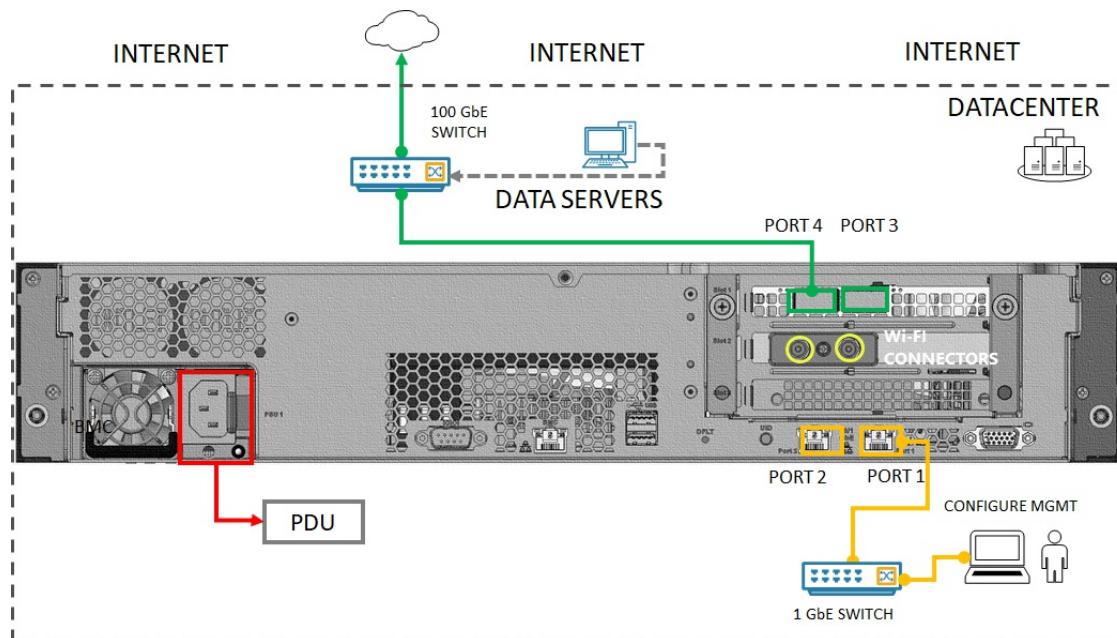
Prerequisites

Before you configure and set up your device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro 2](#).

Connect to the local web UI setup

1. Configure the Ethernet adapter on your computer to connect to your device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
2. Connect the computer to PORT 1 on your device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter. Use the following illustration to identify PORT 1 on your device.

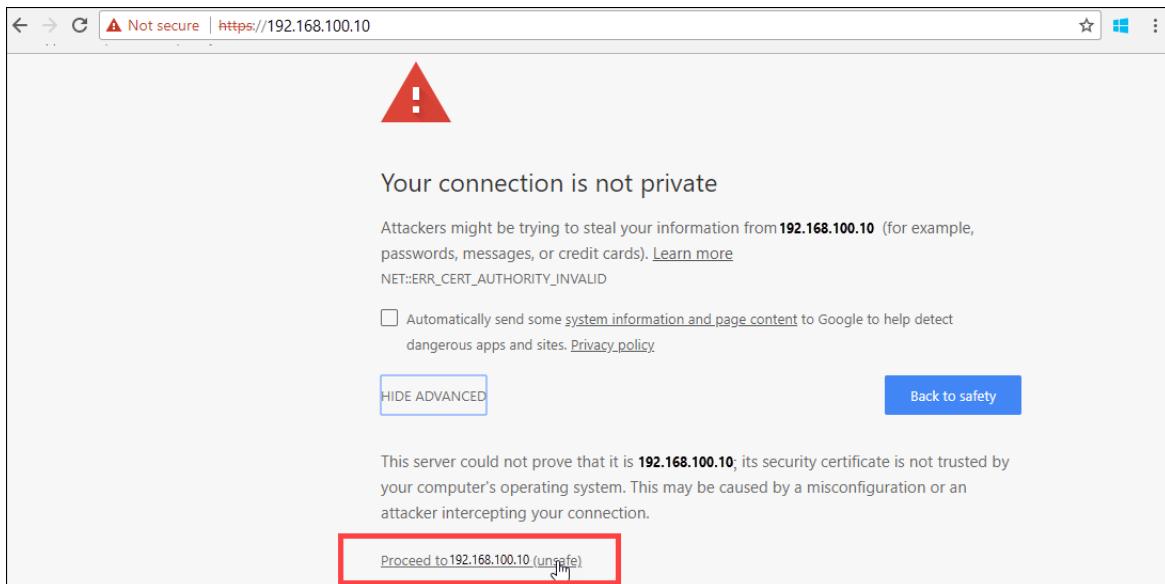


The back plane of the device may look slightly different depending on the exact model you've received. For more information, see [Cable your device](#).

3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>.

This action may take a few minutes after you've turned on the device.

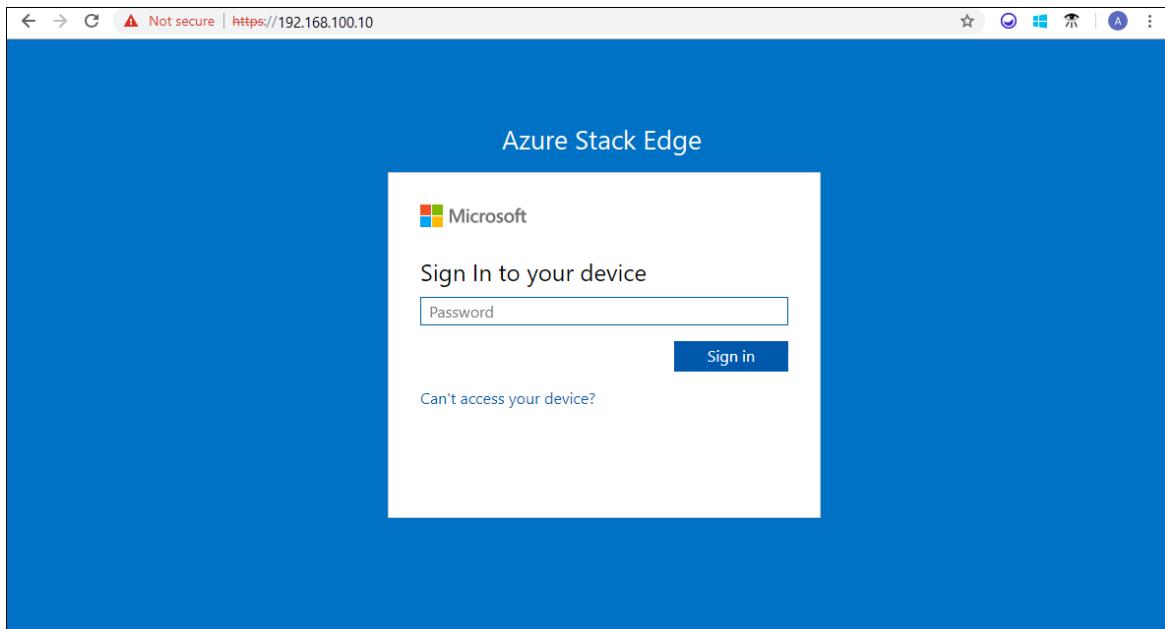
You see an error or a warning indicating that there's a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



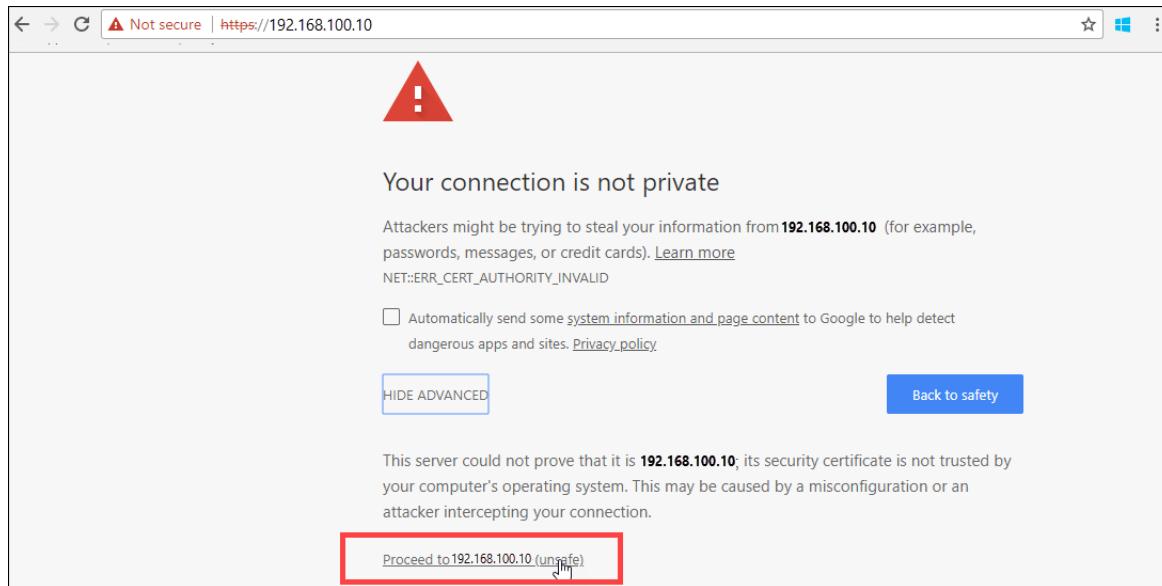
6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters.

You're now at the **Overview** page of your device. The next step is to configure the network settings for your device.

1. Configure the Ethernet adapter on your computer to connect to your device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
 2. Connect the computer to PORT 1 on your device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter.
 3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>.
- This action may take a few minutes after you've turned on the device.

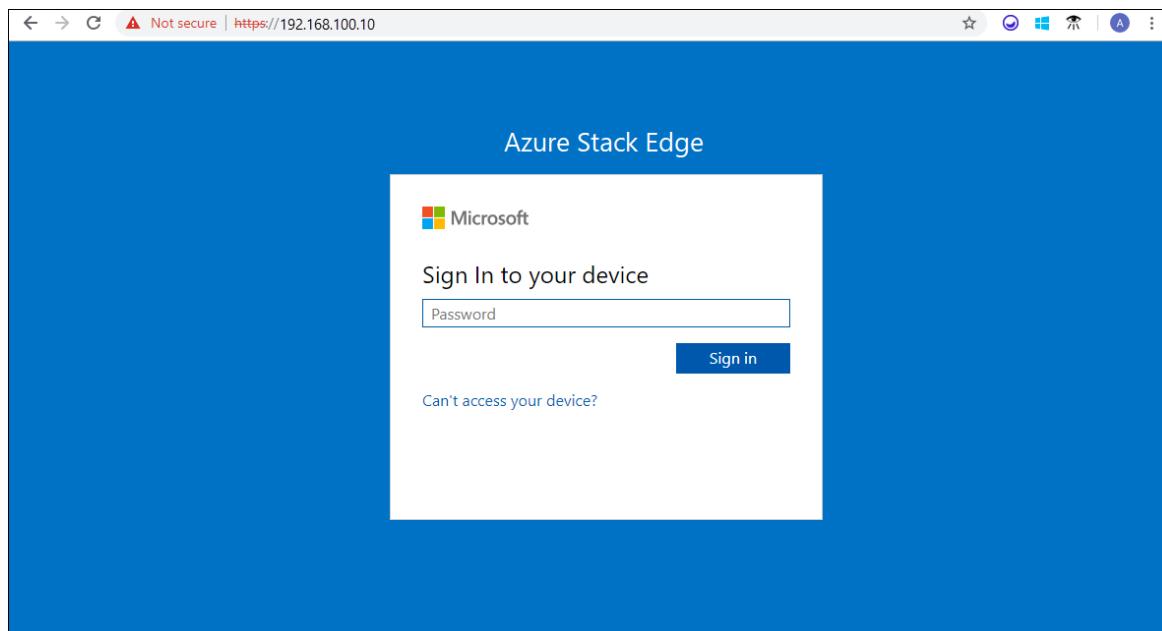
You see an error or a warning indicating that there's a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters. You're now at the **Overview** page of your 2-node device.

7. Repeat the above steps to connect to the second node of your 2-node device.

The next step is to configure the network settings for your device.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Connect to a physical device

To learn how to configure network settings on your Azure Stack Edge Pro 2 device, see:

[Configure network](#)

Tutorial: Configure network for Azure Stack Edge Pro 2

9/21/2022 • 20 minutes to read • [Edit Online](#)

This tutorial describes how to configure network for your Azure Stack Edge Pro 2 device by using the local web UI.

The connection process can take around 20 minutes to complete.

This tutorial describes how to configure network for your two-node Azure Stack Edge Pro 2 device by using the local web UI.

The procedure can take around 45 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
 - Configure network
 - Configure advanced networking
 - Configure web proxy
 - Validate network settings
-
- Prerequisites
 - Select device setup type
 - Configure network and network topology on both nodes
 - Get authentication token for prepared node
 - Configure cluster witness and add prepared node
 - Configure virtual IP settings for Azure Consistent Services and NFS
 - Configure advanced networking
 - Configure web proxy
 - Validate network settings

Prerequisites

Before you configure and set up your Azure Stack Edge Pro 2 device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro 2](#).
- You've connected to the local web UI of the device as detailed in [Connect to Azure Stack Edge Pro 2](#)

Configure network

Your **Get started** page displays the various settings that are required to configure and register the physical device with the Azure Stack Edge service.

Follow these steps to configure the network for your device.

1. In the local web UI of your device, go to the **Get started** page. On the **Set up a single node device** tile, select **Start**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. On the left, a sidebar lists various configuration options: Overview, Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time, Certificates, Cloud details, and Maintenance (Power, Hardware health, Software update, Password change, Device reset). The 'Get started' option is highlighted with a red box. The main content area is titled 'Get started' and shows three cards:

- Set up a single node device**: Configure a single node device. Contains a 'Start' button.
- Set up a 2-node cluster (Preview)**: Set up a node for a 2-node cluster. Recommended for high availability. Contains a 'Start' button.
- Prepare a node for clustering (Preview)**: Ready this node if you initiated cluster creation from another node, and want to add this node to that cluster. Recommended for high availability. Contains a 'Start' button.

2. On the **Network** tile, select **Needs setup**.

The screenshot shows the 'Get started with standalone device setup' page. The sidebar is identical to the previous one. The main content area is titled 'Get started with standalone device setup' and shows four sections:

- 1 Network**:

Network	:	⚠ Needs setup
Compute network	:	Not configured
Web proxy	:	Not configured
- 2 Device setup**:

Device	:	⚠ Needs setup
Update	:	Configured with defaults
Time	:	Configured with defaults
- 3 Security**:

Certificates	:	Configured with defaults
Encryption at rest	:	Configure
- 4 Activation**: Use the activation key from the Azure portal to activate your device. Contains an 'Activate' button.

[Go back to select setup type](#)

On your physical device, there are four network interfaces. Port 1 and Port 2 are 1-Gbps network interfaces that can also serve as 10-Gbps network interfaces. Port 3 and Port 4 are 100-Gbps network interfaces. Port 1 is used for the initial configuration of the device. For a new device, the **Network** page is as shown below.

Azure Stack Edge Pro 2 – 64G2T

Overview | Network | Configuration | Get started | Advanced networking | Cluster (Preview) | Web proxy | Device | Update server | Time | Certificates | Cloud details | Maintenance | Power

Network

DM1174466-904

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	5C-FE-9E-01-BA-3C
Port2	-	-	-	-	5C-FE-9E-01-BA-3D
Port3	-	-	-	-	08-C0-EB-81-67-10
Port4	-	-	-	-	08-C0-EB-81-67-11

Apply

< Back to Get started | Next: Advanced networking >

3. To change the network settings, select a port and in the right pane that appears, modify the IP address, subnet, gateway, primary DNS, and secondary DNS.

- If you select Port 1, you can see that it's preconfigured as static.

Network settings (Port 1)

* IP settings
 DHCP Static

* Subnet mask
 ✓

Gateway

Primary DNS

Secondary DNS

Serial number	IP address	MAC address
A4P1074002103B	192.168.100.10	5C-FE-9E-01-BA-57

Modify

- If you select Port 2, Port 3, or Port 4, all of these ports are configured as DHCP by default.

Network settings (Port 3)

* IP settings

DHCP Static

Subnet mask

255.255.0.0

Gateway

Primary DNS

192.168.0.1

Secondary DNS

Serial number	IP address	MAC address
A4P1074002103B	192.168.2.43	08-C0-EB-81-6D-98

Modify

As you configure the network settings, keep in mind:

- Port 3 and Port 4 are reserved for Network Function Manager workload deployments. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge](#).
- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.
- If DHCP isn't enabled, you can assign static IPs if needed.
- Serial number for any port corresponds to the node serial number.

Once the device network is configured, the page updates as shown below.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. The left sidebar has a dark theme with white text and icons. The 'Network' option under 'CONFIGURATION' is highlighted with a red box. The main content area has a light blue header with the text 'Azure Stack Edge Pro 2 - 64G2T' and several small icons. Below this is a 'Network' section with the ID 'DM1174466-904'. A sub-section titled 'Network interfaces' contains a table with four rows, each representing a network port. The table columns are: Name, Virtual switch, IP addresses, Subnet mask, Gateway, and MAC addresses. The rows are: Port1 (IP 192.168.100.10), Port2 (IP 10.57.53.236), Port3 (IP 192.168.2.221), and Port4 (IP 192.168.1.76). At the bottom of the table is an 'Apply' button. At the very bottom of the page are two buttons: '< Back to Get started' and 'Next: Advanced networking >'.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	5C-FE-9E-01-BA-3C
Port2	-	10.57.53.236	255.255.248.0	10.57.48.1	5C-FE-9E-01-BA-3D
Port3	-	192.168.2.221	255.255.0.0	-	08-C0-EB-81-67-10
Port4	-	192.168.1.76	255.255.0.0	-	08-C0-EB-81-67-11

NOTE

We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has activated with the service, and then change. You can then view the IPs of all the adapters in the **Device properties** in the Azure portal for your service.

After you've configured and applied the network settings, select **Next: Advanced networking** to configure compute network.

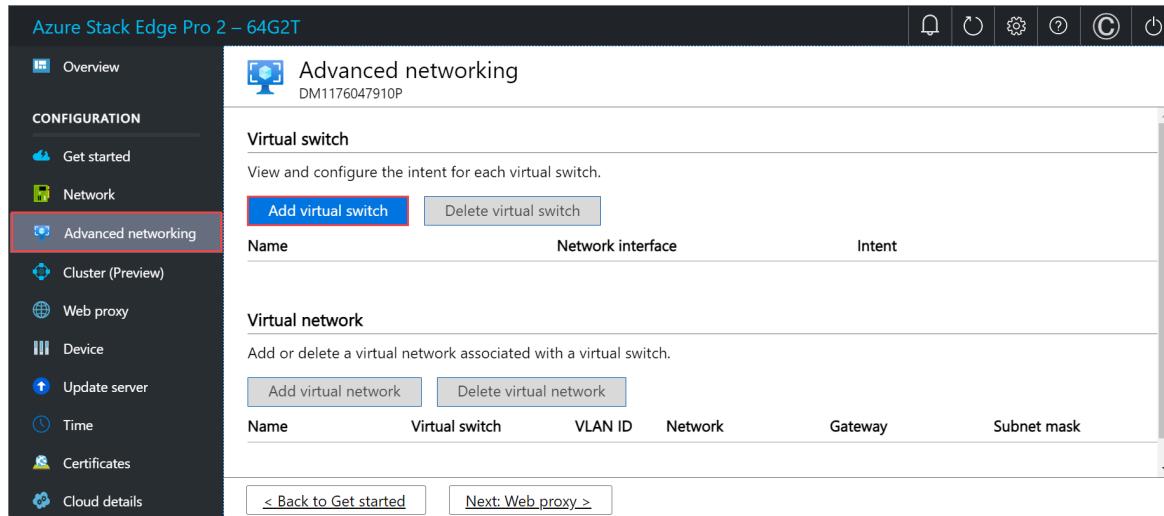
Configure advanced networking

Follow these steps to configure advanced network settings such as creating a switch for compute and associating it with a virtual network.

NOTE

There is no restriction on the number of virtual switches that you can create on your device. However, you can enable compute only on one virtual switch at a time.

1. In the local web UI of your device, go to the **Advanced networking** page. Select **Add virtual switch** to create a new virtual switch or use an existing virtual switch. This virtual switch will be used for the compute infrastructure on the device.



2. In **Add virtual switch** blade:

- a. Provide a name for your virtual switch.
- b. Associate a network interface on your device with the virtual switch you'll create. You can only have one virtual switch associated with a network interface on your device.
- c. Assign an intent for your virtual switch. To deploy compute workloads, you'll select compute as the intent.
- d. Assign **Kubernetes node IPs**. These static IP addresses are for the compute VM that will be created on this virtual switch.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. For a 1-node device, provide a minimum of 2 free, contiguous IPv4 addresses.

IMPORTANT

Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).

- e. Assign **Kubernetes external service IPs**. These are also the load-balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside of the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

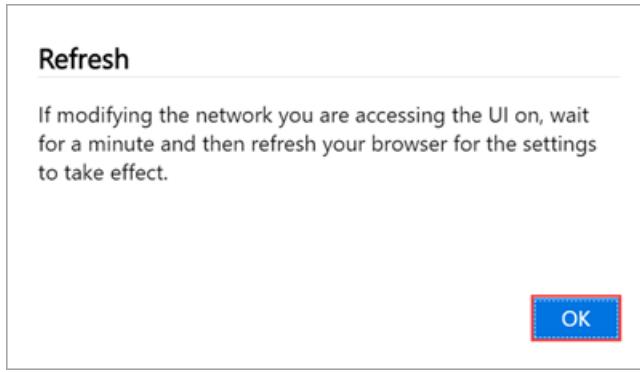
- f. Select **Apply**.

The screenshot shows the 'Add virtual switch' dialog box. It has the following fields:

- Name:** asecompute (marked with a green checkmark)
- Network interface:** Port 3
- Intent:** A dropdown menu containing the word 'compute'.
- Compute IPs:**
 - Kubernetes node IPs:** Enter a contiguous range of 2 static IPs for your device. Value: 192.168.2.45 - 192.168.2.46 (marked with a green checkmark).
 - Kubernetes external service IPs:** Specify the static IP range for services exposed outside of Kubernetes cluster. Value: 192.168.2.47 - 192.168.2.47 (highlighted with a blue border and marked with a green checkmark).
- Apply** button (blue button with white text).

3. You'll see a warning to the effect that you may need to wait for a couple minutes and then refresh the

browser. Select OK.



- After the configuration is applied and you've refreshed the browser, you can see that the specified port is enabled for compute.

A screenshot of the Azure Stack Edge Pro 2 - 64G2T management interface. The left sidebar shows 'Advanced networking' selected. The main pane displays the 'Advanced networking' configuration for the device DM1176047910P. Under 'Virtual switch', there is one entry: 'asecompute' with 'Intent' set to 'compute'. Under 'Virtual network', there are no entries. At the bottom, there are navigation links: '< Back to Get started' and 'Next: Web proxy >'.

- Optionally you can create a virtual network and associate it with your virtual switch if you wish to route your traffic. Select **Add virtual network** and then input the following information.
 - Select a **Virtual switch** to which you'll add a virtual network.
 - Provide a **Name** for the virtual network.
 - Supply a unique number from 1-4096 as your **VLAN ID**.
 - Enter a **Subnet mask** and a **Gateway** depending on the configuration of your physical network in the environment.
 - Select **Apply**.

Add virtual network

Add a virtual network to a specified virtual switch on your device.

* Virtual switch
asecompute

* Name
computevnet

* VLAN ID
200

* Subnet mask
255.255.252.0

* Gateway
192.168.40.1

Apply

6. After the configuration is applied, you can see that the specified virtual network is created.

Name	Network interface	Intent
asecompute		compute

Name	Virtual switch	VLAN ID	Network	Gateway	Subnet mask
asevnet	asecompute	200	192.168.40.0	192.168.40.1	255.255.252.0

Select **Next: Web proxy** to configure web proxy.

Configure setup type

1. In the local UI for one of the devices, go to the **Get started** page.
2. In the **Set up a 2-node cluster** tile, select **Start**.

The screenshot shows the 'Get started' page of the Azure Stack Edge Pro 2 - 64G2T local UI. The left sidebar contains navigation links for Overview, Configuration, Maintenance, and Troubleshooting. The 'Get started' link is highlighted with a red box. The main content area displays three tiles:

- Set up a single node device**: Configure a single node device. A 'Start' button is present.
- Set up a 2-node cluster (Preview)**: Set up a node for a 2-node cluster. Recommended for high availability. A 'Start' button is present.
- Prepare a node for clustering (Preview)**: Ready this node if you initiated cluster creation from another node, and want to add this node to that cluster. Recommended for high availability. A 'Start' button is present.

3. In the local UI for the second device, go to the **Get started** page.

4. In the **Prepare a node for clustering (Preview)** tile, select **Start**.

The screenshot shows the 'Get started' page of the Azure Stack Edge Pro 2 - 64G2T local UI. The left sidebar contains navigation links for Overview, Configuration, Maintenance, and Troubleshooting. The 'Get started' link is highlighted with a red box. The main content area displays three tiles:

- Set up a single node device**: Configure a single node device. A 'Start' button is present.
- Set up a 2-node cluster (Preview)**: Set up a node for a 2-node cluster. Recommended for high availability. A 'Start' button is present.
- Prepare a node for clustering (Preview)**: Ready this node if you initiated cluster creation from another node, and want to add this node to that cluster. Recommended for high availability. A 'Start' button is present.

Configure network, topology

You'll configure network and network topology on both the nodes. These steps can be done in parallel. The cabling on both nodes should be identical and should conform with the network topology you choose.

Configure network on first node

Follow these steps to configure the network for your device.

1. In the local web UI of your device, go to the **Get started** page.

2. On the **Network** tile, select **Configure**.

The screenshot shows the 'Get started' page of the Azure Stack Edge Pro 2 - 64G2T local web interface. The left sidebar has a 'CONFIGURATION' section with 'Get started' highlighted. The main pane displays four configuration sections: 1) Network (Network and Network topology both show 'Needs setup'), 2) Configure cluster (Cluster and Cluster witness both show 'Not configured'), 3) Device setup (Compute network, Web proxy, Device, Update, and Time all show 'Not configured'), and 4) Security (Certificates and Encryption at rest both show 'Configured with defaults').

On your physical device, there are four network interfaces. Port 1 and Port 2 are 1-Gbps network interfaces that can also serve as 10-Gbps network interfaces. Port 3 and Port 4 are 100-Gbps network interfaces.

For a new device, the **Network** page is as shown below.

The screenshot shows the 'Network' configuration page. The left sidebar has 'Network' selected. The main pane shows a table for 'Network interfaces' with four entries: Port1, Port2, Port3, and Port4. The table columns are Name, Virtual switch, IP addresses, Subnet mask, Gateway, and MAC addresses. The 'IP addresses' column for Port1 contains '192.168.100.10'. The 'MAC addresses' column for Port1 contains '5C-FE-9E-01-BA-3C'. At the bottom are 'Apply' and navigation buttons for 'Back to Get started' and 'Next: Advanced networking'.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	5C-FE-9E-01-BA-3C
Port2	-	-	-	-	5C-FE-9E-01-BA-3D
Port3	-	-	-	-	08-C0-EB-81-67-10
Port4	-	-	-	-	08-C0-EB-81-67-11

3. To change the network settings, select a port and in the right pane that appears, modify the IP address, subnet, gateway, primary DNS, and secondary DNS.

- If you select Port 1, you can see that it's preconfigured as static.

Network settings (Port 1)

* IP settings

DHCP Static

* Subnet mask

255.255.255.0 ✓

Gateway

[]

Primary DNS

[]

Secondary DNS

[]

Serial number

IP address

MAC address

A4P1074002103B	192.168.100.10 ✓	5C-FE-9E-01-BA- 57
----------------	------------------	-----------------------

Modify

- If you select Port 2, Port 3, or Port 4, all of these ports are configured as DHCP by default.

Network settings (Port 3)

* IP settings

DHCP Static

Subnet mask

255.255.0.0

Gateway

[]

Primary DNS

192.168.0.1

Secondary DNS

[]

Serial number

IP address

MAC address

A4P1074002103B	192.168.2.43	08-C0-EB-81-6D- 98
----------------	--------------	-----------------------

Modify

As you configure the network settings, keep in mind:

- Make sure that Port 3 and Port 4 are connected for Network Function Manager deployments. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge](#).
- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.

- If DHCP isn't enabled, you can assign static IPs if needed.
- Serial number for any port corresponds to the node serial number.

Once the device network is configured, the page updates as shown below.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	5C-FE-9E-01-BA-3C
Port2	-	10.57.53.236	255.255.248.0	10.57.48.1	5C-FE-9E-01-BA-3D
Port3	-	192.168.2.221	255.255.0.0	-	08-C0-EB-81-67-10
Port4	-	192.168.1.76	255.255.0.0	-	08-C0-EB-81-67-11

NOTE

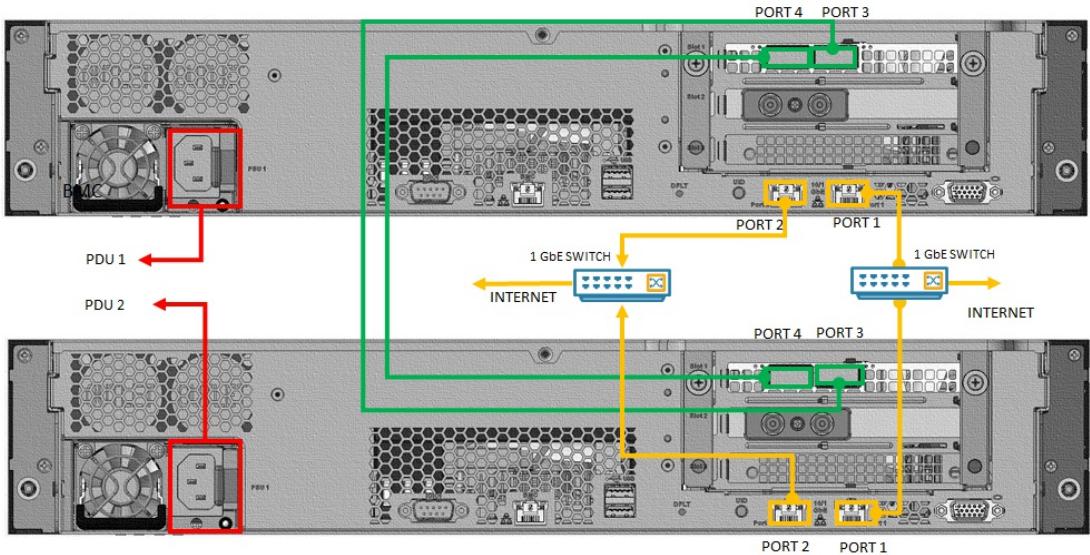
We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has activated with the service, and then change. You can then view the IPs of all the adapters in the **Device properties** in the Azure portal for your service.

Reconfigure Port 1 on first node

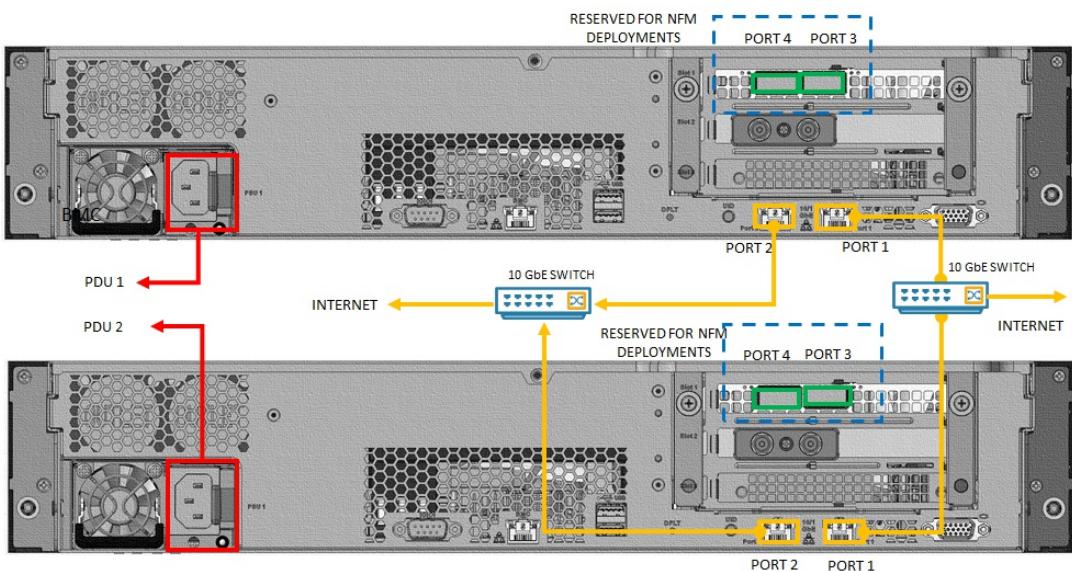
Based on the network topology you will choose, you would need to route Port 1 to the internet via a switch and assign it IPs.

Follow these steps to reconfigure Port 1:

1. Disconnect Port 1 from the laptop by removing the connecting cable.
2. Connect to the local web UI via the IP address of the Port 2 at the following URL:
`https://<IP address of Port 2>`
3. Sign in to the local web UI by providing the device password.
4. Connect the Port 1 via an appropriate cable. Use one of the following options corresponding to the supported network topologies.
 - **Switchless**



- Using external switches



5. Go to the **Network** page for the first node.
6. Configure IPs for Port 1. Depending on the network topology that you wish to deploy:
 - a. Assign Port 1 IPs that are in a different subnet as that of Port 2.
 - b. Assign Port 1 IPs that are in the same subnet as that of Port 2.
7. After Port 1 is configured, select **Next: Advanced networking >** to configure your network topology.

Configure network topology on first node

1. In the **Advanced networking** page, choose the topology for cluster and the storage traffic between nodes from the following options:
 - Use external switches, Port 1 and Port 2 in the same subnet
 - Use external switches, Port 1 and Port 2 in different subnet
 - Switchless, Port 1 and Port 2 in the same subnet
 - Switchless, Port 1 and Port 2 in different subnet

Azure Stack Edge Pro 2 – 64G2T

Overview

CONFIGURATION

- Get started
- Network
- Advanced networking**
- Cluster (Preview)
- Web proxy
- Device
- Update server
- Time
- Certificates
- Cloud details

Advanced networking
DM1174466-904

Choose the topology for cluster and storage traffic between nodes. Make sure to cable the device nodes as per the selected topology. [Learn more about how to cable the device.](#)

* Choose if you want to use external switches to connect the nodes.
 Use external switches Switchless

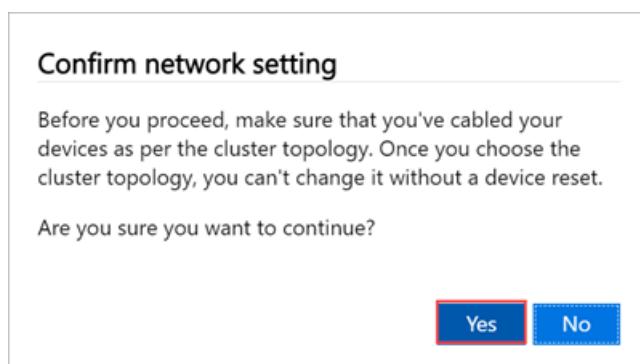
* Choose your topology for cluster and storage traffic between nodes. A virtual switch will always be created for Port 1.

Connect Port 1 and Port 2 of each node to an external switch. These ports must be in the same subnet with internet connectivity as these ports are teamed. Recommended when you need port level redundancy through teaming.
[Learn more.](#)

Connect Port 1 and Port 2 of each node to an external switch. These ports are not teamed. Recommended when Port 1 and Port 2 are required to be placed in separate subnets for additional redundancy in the network.
[Learn more.](#)

Apply [< Back to Get started](#) [Next: Cluster \(Preview\) >](#)

2. Make sure that your node is cabled as per the selected topology.
3. Select **Apply**.
4. You'll see a **Confirm network setting** dialog. This dialog reminds you to make sure that your node is cabled as per the network topology you selected. Once you choose the network cluster topology and create a cluster, you can't update the topology without a device reset. Select **Yes** to confirm the network topology.



The network topology setting takes a few minutes to apply and you see a notification when the settings are successfully applied.

If for any reason, you need to reset or update the network topology, you can use the **Update topology** option. If you update the topology, you may need to make sure the cabling for the device is changed accordingly.

Virtual switch

Name	Network interface	Intent
vSwitch1	Port 1	management, storage
vSwitch2	Port 2	management, storage

Virtual network

Name	Virtual switch	VLAN ID	Network	Gateway	Subnet mask

Network topology

Update your network topology for clustering.

Update topology

< Back to Get started | Next: Get started >

- Once the network topology is applied, the **Network** page updates. For example, if you selected network topology that uses external switches and separate virtual switches, you'll see that on the device node, a virtual switch **vSwitch1** is created at Port 1 and another virtual switch, **vSwitch2** is created on Port 2. Port 3 and Port 4 don't have any virtual switches.

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
vEthernet (vPort1)	vSwitch1 (Port1)	192.168.100.10	255.255.255.0	-	5C-FE-9E-01-BA-3C
vEthernet (vPort2)	vSwitch2 (Port2)	10.57.53.236	255.255.248.0	10.57.48.1	5C-FE-9E-01-BA-3D
Port3	-	192.168.2.221	255.255.0.0	-	08-C0-EB-81-67-10
Port4	-	192.168.1.76	255.255.0.0	-	08-C0-EB-81-67-11

Apply

< Back to Get started | Next: Advanced networking >

You'll now configure the network and the network topology of the second node.

Configure network on second node

You'll now prepare the second node for clustering. You'll first need to configure the network. Follow these steps in the local UI of the second node:

- On the **Prepare a node for clustering** page, in the **Network** tile, select **Needs setup**.

Azure Stack Edge Pro 2 – 64G2T

Overview

CONFIGURATION

Get started

Network

Advanced networking

Cluster (Preview)

Web proxy

Device

Update server

Time

Certificates

Prepare a node for clustering (Preview)
DM1176047910P

1 Network

Network : Needs setup

Network topology : Needs setup

2 Get authentication token

Get a token to authenticate this node to form a 2-node cluster if you started cluster creation on another node.

Prepare node

[Go back to select setup type](#)

2. Configure the network on the second node in a similar way that you configured the first node.

Reconfigure Port 1 on second node

Follow the steps to reconfigure Port 1 on second node as you did on the first node:

1. Disconnect the cable on Port 1. Sign in to the local web UI using Port 2 IP address.
2. Connect Port 1 via an appropriate cable and a switch on the second node.
3. Assign IPs to the Port 1 on the second node in the same way as that you did on the first node.
4. After Port 1 on the second node is configured, select **Next: Advanced networking >**.

Configure network topology on second node

1. Make sure that the second node is cabled as per the topology you selected for the first node. In the **Advanced networking** page, choose and **Apply** the same topology that you selected for the first node.

Azure Stack Edge Pro 2 – 64G2T

Overview

CONFIGURATION

Get started

Network

Advanced networking

Cluster (Preview)

Web proxy

Device

Update server

Time

Certificates

Cloud details

Advanced networking
DM1176047910P

Choose the topology for cluster and storage traffic between nodes. Make sure to cable the device nodes as per the selected topology. [Learn more about how to cable the device](#).

* Choose if you want to use external switches to connect the nodes.
 Use external switches Switchless

* Choose your topology for cluster and storage traffic between nodes. A virtual switch will always be created for Port 1.

Connect Port 1 and Port 2 of each node to an external switch. These ports must be in the same subnet with internet connectivity as these ports are teamed. Recommended when you need port level redundancy through teaming.
[Learn more](#)

Connect Port 1 and Port 2 of each node to an external switch. These ports are not teamed. Recommended when Port 1 and Port 2 are required to be placed in separate subnets for additional redundancy in the network.
[Learn more](#)

Apply < Back to Get started Next: Get started >

2. Select **Back to get started**.

Get authentication token

You'll now get the authentication token that will be needed when adding this node to form a cluster. Follow these steps in the local UI of the second node:

1. On the **Prepare a node for clustering** page, in the **Get authentication token** tile, select **Prepare node**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. On the left, a sidebar lists various configuration options: Overview, Configuration (highlighted), Get started (highlighted), Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time, and Certificates. The main content area is titled "Prepare a node for clustering (Preview)" and shows two sections: "Network" and "Get authentication token". The "Network" section displays "Network" and "Network topology" status as "Configured". The "Get authentication token" section contains a "Prepare node" button. At the bottom, there is a link to "Go back to select setup type".

2. Select **Get token**.
3. Copy the node serial number and the authentication token. You'll use this information when you add this node to the cluster on the first node.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. On the left, a sidebar lists various configuration options: Overview, Configuration (highlighted), Get started (highlighted), and Network (highlighted). The main content area is titled "Prepare a node for clustering" and shows three steps:

1. An authentication token is created for the node and requests are temporarily allowed from another node to join a cluster.
[Get token](#)
2. Use this information in the Cluster page of the node where you initiated the 2-node cluster setup.
Node serial number: A6P15140005012
Authentication token
eyJUb2tlbil6ImV5SkRaWEowYVdacFkyRjBa [Copy](#)
3. If you don't want to prepare this node to form a cluster, undo node preparation.
[Undo node preparation](#)

Configure cluster

To configure the cluster, you'll need to establish a cluster witness and then add a prepared node. You'll also need to configure virtual IP settings so that you can connect to a cluster as opposed to a specific node.

Configure cluster witness

You'll now create a cluster witness. A cluster witness helps establish quorum for a two-node device if a node goes down. To learn about quorum, see [Understanding quorum](#).

A cluster witness can be:

- **Cloud witness** if you use an Azure Storage account to provide a vote on cluster quorum. A cloud witness uses Azure Blob Storage to read or write a blob file and then uses it to arbitrate in split-brain resolution.

Use cloud witness when you have internet access. For more information on cloud witness, see [Deploy a cloud witness for Failover cluster](#).

- **File share witness** if you use a local SMB file share to provide a vote in the cluster quorum. Use a file share witness if all the servers in a cluster have spotty internet connectivity or can't use disk witness as there aren't any shared drives.

Use file share witness if you're in an IT environment with other machines and file shares. For more information on file share witness, see [Deploy a file share witness for Failover cluster](#).

Before you create a cluster witness, make sure that you've reviewed the cluster witness requirements.

Follow these steps to configure the cluster witness.

Configure cloud witness

1. In the local UI of the first node, go to the **Cluster (Preview)** page. Under **Cluster witness type**, select **Modify**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T Cluster (Preview) configuration interface. On the left, there's a navigation sidebar with sections like Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting. The 'Cluster (Preview)' section is highlighted with a red box. The main area shows the cluster name 'A4P1074000603CL'. Under 'Cluster witness', it says 'Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.' The 'Witness type' dropdown is set to 'None'. A 'Modify' button is highlighted with a red box. Below that is the 'Existing nodes' section, which has an 'Add node' button highlighted with a red box and a 'Replace node' button. It lists one node: Serial number A4P1074000603B, Version 2.2.1868.4470, Status Healthy. An 'Apply' button is highlighted with a red box at the bottom. At the very bottom, there are 'Back to Get started' and 'Next: Web proxy' buttons.

2. In the **Modify cluster witness** blade, enter the following inputs.

- a. Choose the **Witness type** as **Cloud**.
- b. Enter the **Azure Storage account name**.
- c. Specify Storage account authentication from Access key or SAS token.
- d. If you chose Access key as the authentication mechanism, enter the Access key of the Storage account, Azure Storage container where the witness lives, and the service endpoint.
- e. Select **Apply**.

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

Cloud

* Azure Storage account name

myasestoracct

* Storage account authentication

Access key SAS token

* Access key

<Access key>

Azure Storage container

myasecont

Service endpoint

core.windows.net

Apply

Configure local witness

1. In the local UI of the first node, go to the Cluster page. Under Cluster witness type, select Modify.

Azure Stack Edge Pro 2 – 64G2T

Cluster (Preview)
DM1174466-904

Add a prepared node, view existing nodes, or modify cluster witness.

Cluster name: A4P1074000603CL

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type: None

Modify

Existing nodes

Add new nodes or view existing nodes

Add node **Replace node**

Serial number	Version	Status
A4P1074000603B	2.2.1868.4470	Healthy

Apply

[< Back to Get started](#) [Next: Web proxy >](#)

The screenshot shows the 'Cluster (Preview)' configuration page. The left sidebar has a red box around the 'Cluster (Preview)' item. The main area shows a cluster named 'A4P1074000603CL'. Under 'Cluster witness', it says 'None' and has a 'Modify' button. Below that is the 'Existing nodes' section with a table showing one node: Serial number A4P1074000603B, Version 2.2.1868.4470, Status Healthy. There are 'Add node' and 'Replace node' buttons above the table, and an 'Apply' button below it. At the bottom are navigation links: '< Back to Get started' and 'Next: Web proxy >'.

2. In the **Modify cluster witness** blade, enter the following inputs.

- a. Choose the **Witness type** as **Local**.
- b. Enter the file share path as **//server/fileshare** format.
- c. Select **Apply**.

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

* Share path

Credentials required

* Username

* Password

Apply

Add prepared node to cluster

You'll now add the prepared node to the first node and form the cluster. Before you add the prepared node, make sure the networking on the incoming node is configured in the same way as that of this node where you initiated cluster creation.

1. In the local UI of the first node, go to the Cluster page. Under Existing nodes, select Add node.

Azure Stack Edge Pro 2 – 64G2T

Cluster (Preview)
DM1174466-904

Add a prepared node, view existing nodes, or modify cluster witness.

Cluster name: A4P1074000603CL

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestoracct	myasecont	core.windows.net

Existing nodes

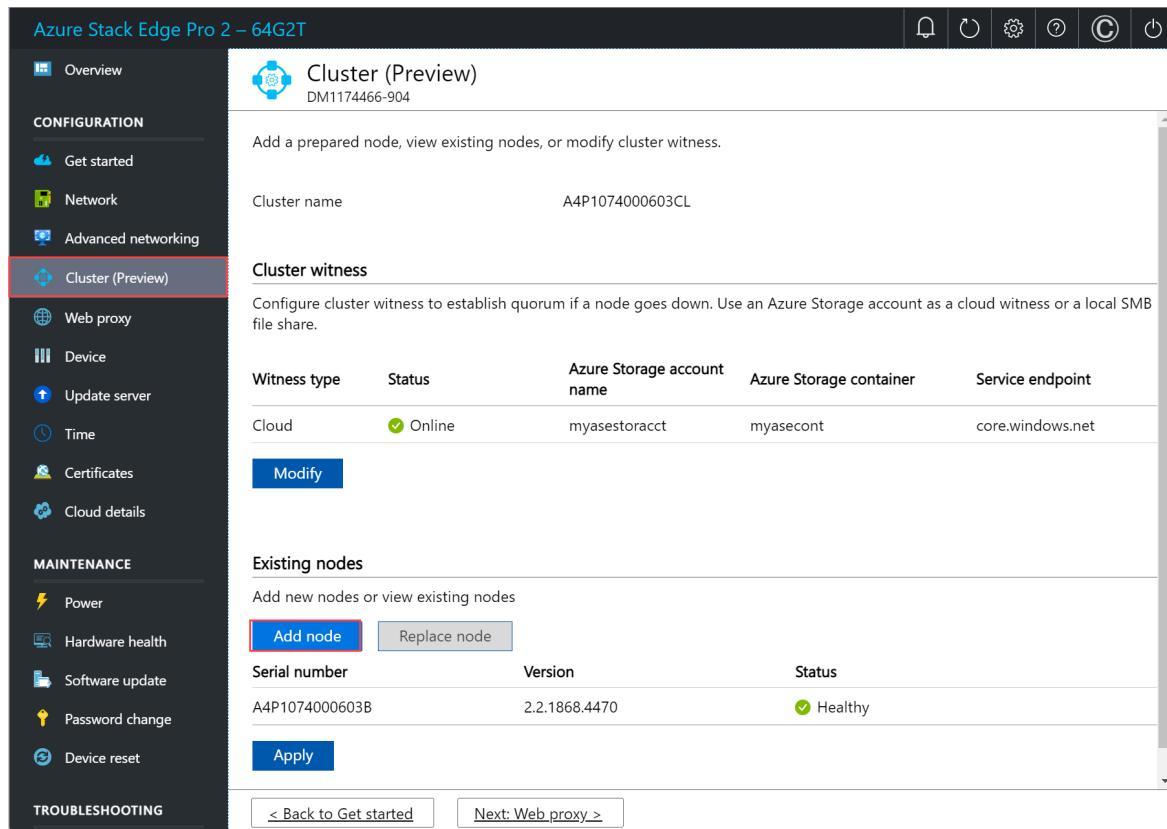
Add new nodes or view existing nodes

Add node (highlighted) | Replace node

Serial number	Version	Status
A4P1074000603B	2.2.1868.4470	Healthy

Apply

< Back to Get started | Next: Web proxy >



2. In the **Add node** blade, input the following information for the incoming node:

- a. Provide the serial number for the incoming node.
- b. Enter the authentication token for the incoming node.

3. Select **Validate & add**. This step takes a few minutes.

X

Add node

Prepare another node and add it to form a cluster. Before you add another node:

- Configure the networking on the incoming node in the same way as you set up on this node.
- Get the node serial number and authentication token by preparing the incoming node.

[Learn how to get the node serial number and token.](#)

Enter information for the incoming node.

Node serial number

A4P1074002103B ✓

Node token

..... ✓

Validate & add

You see a notification when the node is successfully validated.

4. The node is now ready to join the cluster. Select **Apply**.

Azure Stack Edge Pro 2 – 64G2T

Cluster (Preview)
DM1174466-904

Add a prepared node, view existing nodes, or modify cluster witness.

Cluster name: A4P1074000603CL

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestoracct	myasecont	core.windows.net

Existing nodes

Add new nodes or view existing nodes

Serial number	Version	Status
A4P1074000603B	2.2.1868.4470	Healthy
A6P15140005012	-	Ready to join

Actions: Modify, Add node, Replace node, Apply

< Back to Get started | Next: Web proxy >

5. A dialog pops up indicating that the cluster creation could take several minutes. Press **OK** to continue. Once the cluster is created, the page updates to show both the nodes are added.

Configure virtual IPs

For Azure consistent services and NFS, you'll also need to define a virtual IP that allows you to connect to a clustered device as opposed to a specific node. A virtual IP is an available IP in the cluster network and any client connecting to the cluster network on the two-node device should be able to access this IP.

For Azure Consistent Services

For Azure Consistent Services, follow these steps to configure virtual IP.

1. In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Azure Consistent Services**.
2. In the **Virtual IP settings** blade, input the following.
 - a. From the dropdown list, select the **Azure Consistent Services network**.
 - b. Choose IP settings from **DHCP** or **static**.
 - c. If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the Azure Consistent Services network that you specified. If you selected DHCP, a virtual IP is automatically picked from the Azure Consistent Services network that you selected.
3. Select **Apply**.

Virtual IP settings

* Azure Consistent Services network
10.126.72.0

* IP settings
DHCP **Static**

Azure Consistent Services Virtual IP
IP will be auto allocated.

Apply

For Network File System

For clients connecting via NFS protocol to the two-node device, follow these steps to configure virtual IP.

1. In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Network File System**.
2. In the **Virtual IP settings** blade, input the following.
 - a. From the dropdown list, select the **NFS network**.
 - b. Choose IP settings from **DHCP** or **Static**.
 - c. If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the NFS network that you specified. If you selected DHCP, a virtual IP is automatically picked from the NFS network that you selected.
3. Select **Apply**.

Virtual IP settings

* Network File System network
10.126.72.0

* IP settings
DHCP **Static**

Network File System Virtual IP
IP will be auto allocated.

Apply

NOTE

Virtual IP settings are required. If you do not configure this IP, you will be blocked when configuring the **Device settings** in the next step.

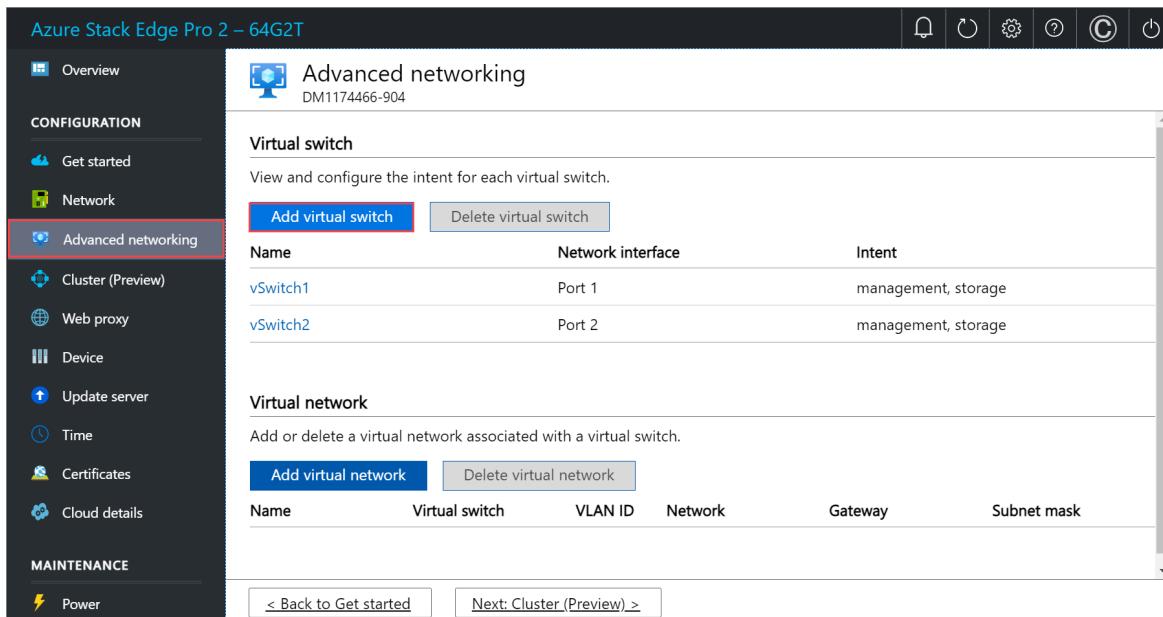
Configure virtual switches and compute IPs

After the cluster is formed and configured, you'll now create new virtual switches or assign intent to the existing virtual switches that are created based on the selected network topology.

IMPORTANT

On a two-node cluster, compute should only be configured on a virtual switch.

1. In the local UI, go to **Advanced networking** page.
2. In the **Virtual switch** section, you'll assign compute intent to a virtual switch. You can select an existing virtual switch or select **Add virtual switch** to create a new switch.



Name	Network interface	Intent
vSwitch1	Port 1	management, storage
vSwitch2	Port 2	management, storage

3. In the **Network settings** blade, if using a new switch, provide the following:

- a. Provide a name for your virtual switch.
- b. Choose the network interface on which the virtual switch should be created.
- c. If deploying 5G workloads, set **Supports accelerated networking** to Yes.
- d. Select the intent to associate with this network interface as **compute**. Alternatively, the switch can be used for management traffic as well. You can't configure storage intent as storage traffic was already configured based on the network topology that you selected earlier.

TIP

Use *CTRL + Click* to select more than one intent for your virtual switch.

4. Assign **Kubernetes node IPs**. These static IP addresses are for the Kubernetes VMs.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. For a 1-node device, provide a minimum of 2 free, contiguous IPv4 addresses. For a two-node cluster, provide a minimum of 3 free, contiguous IPv4

addresses.

IMPORTANT

- Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).
- DHCP mode is not supported for Kubernetes node IPs. If you plan to deploy IoT Edge/Kubernetes, you must assign static Kubernetes IPs and then enable IoT role. This will ensure that static IPs are assigned to Kubernetes node VMs.

5. Assign **Kubernetes external service IPs**. These are also the load-balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside of the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

6. Select **Apply**.

Compute virtual switch

Specify a virtual switch for Kubernetes compute traffic.

* Virtual switch

vSwitch2 (Port 2)



Compute IPs

For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs

Enter a contiguous range of 2 static IPs for your device.

10.126.77.50 - 10.126.77.51



Kubernetes external service IPs

Specify the static IP range for services exposed outside of Kubernetes cluster.

10.126.77.52 - 10.126.77.53



Apply

7. The configuration takes a couple minutes to apply and you may need to refresh the browser. You can see that the specified virtual switch is created and enabled for compute.

Name	Network interface	Intent
vSwitch	Port3	compute

Name	Virtual switch	VLAN ID	Network	Gateway	Subnet mask

To delete a virtual switch, under the **Virtual switch** section, select **Delete virtual switch**. When a virtual switch is deleted, the associated virtual networks will also be deleted.

IMPORTANT

Only one virtual switch can be assigned for compute.

Configure virtual network

You can add or delete virtual networks associated with your virtual switches. To add a virtual network, follow these steps:

1. In the local UI on the **Advanced networking** page, under the **Virtual network** section, select **Add virtual network**.
2. In the **Add virtual network** blade, input the following information:
 - a. Select a virtual switch for which you want to create a virtual network.
 - b. Provide a **Name** for your virtual network.
 - c. Enter a **VLAN ID** as a unique number in 1-4094 range.
 - d. Specify the **Subnet mask** and **Gateway** for your virtual LAN network as per the physical network configuration.
 - e. Select **Apply**.

To delete a virtual network, under the **Virtual network** section, select **Delete virtual network**.

Configure web proxy

This is an optional configuration. However, if you use a web proxy, you can configure it only on this page.

IMPORTANT

- Proxy-auto config (PAC) files are not supported. A PAC file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.
- Transparent proxies work well with Azure Stack Edge Pro 2. For non-transparent proxies that intercept and read all the traffic (via their own certificates installed on the proxy server), upload the public key of the proxy's certificate as the signing chain on your Azure Stack Edge Pro device. You can then configure the proxy server settings on your Azure Stack Edge device. For more information, see [Bring your own certificates and upload through the local UI](#).

1. On the **Web proxy settings** page, take the following steps:

a. In the **Web proxy URL** box, enter the URL in this format:

`http://host-IP address or FQDN:Port number`. HTTPS URLs aren't supported.

b. To validate and apply the configured web proxy settings, select **Apply**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The 'Web proxy' section is selected and highlighted with a red border. The main content area is titled 'Web proxy' and shows the device ID 'DM1174466-904'. It contains a note about configuring optional web proxy settings for communication with the cloud service provider. Below this is a form with a 'Web proxy' section containing an 'Enable' button (which is blue, indicating it's selected) and a 'Disable' button. A 'Web proxy URL' field contains the value 'http://100.10.10.10' with a green checkmark icon to its right. At the bottom are 'Apply', '< Back to Get started', and 'Next: Device >' buttons.

Validate network settings

Follow these steps to validate your network settings.

1. Go to the **Diagnostic tests** page and select the tests as shown below.

2. Select **Run test**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes (Preview), Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The 'Diagnostic tests' section is selected and highlighted with a red border. The main content area is titled 'Diagnostic tests' and shows the device ID 'DBE-HWDH1T2'. It contains a note about running diagnostic tests to troubleshoot issues. Below this is a table listing various tests with checkboxes, categorized by category (Azure connectivity, Edge compute, Certificates, Hardware, Networking, Software, Time, Update). Some checkboxes are checked (e.g., Azure Edge compute runtime, Network interfaces, Internet connectivity). At the bottom is a 'Run test' button.

3. Review test results to ensure that status shows **Healthy** for each test that was run.

Test	Category	Status	Recommended actions
Azure consistent services health check	Azure consistent services	-	-
Certificates	Certificates	-	-
<input checked="" type="checkbox"/> Azure Edge compute runtime	Edge compute	Healthy	-
<input type="checkbox"/> Disks	Hardware	-	-
<input type="checkbox"/> Power Supply Units	Hardware	-	-
<input checked="" type="checkbox"/> Network interfaces	Hardware	Healthy	-
<input type="checkbox"/> CPUs	Hardware	-	-
<input type="checkbox"/> Compute acceleration	Hardware	-	-
<input checked="" type="checkbox"/> Network settings	Networking	Healthy	-
<input checked="" type="checkbox"/> Internet connectivity	Networking	Healthy	-
<input type="checkbox"/> System software	Software	-	-
<input type="checkbox"/> Time sync	Time	-	-
<input type="checkbox"/> Software update readiness	Update	-	-

Run test

- If a test fails, select **Recommended actions** on the test results page, implement the recommended change, and then rerun the test. For example, the dialog below shows recommended actions if the Azure Edge compute runtime test fails.

Recommended actions

To resolve the issue(s), complete the following:

- The 'Node' IPs provided for kubernetes cluster '192.168.167.132' are already in use on the network. Provide unused IPs to resolve the issue. If the problem persists, contact Microsoft Support.
- The 'Service' IPs provided for kubernetes cluster '192.168.167.128,192.168.167.129,192.168.167.130' are already in use on the network. Provide unused IPs to resolve the issue. If the problem persists, contact Microsoft Support.

OK

- After network settings are validated and all tests return **Healthy** status, proceed to the device settings page.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Configure network
- Configure advanced networking
- Configure web proxy
- Validate network settings
- Prerequisites
- Select device setup type
- Configure network and network topology on both nodes

- Get authentication token for prepared node
- Configure cluster witness and add prepared node
- Configure virtual IP settings for Azure Consistent Services and NFS
- Configure advanced networking
- Configure web proxy
- Validate network settings

To learn how to set up your Azure Stack Edge Pro 2 device, see:

[Configure device settings](#)

Tutorial: Configure the device settings for Azure Stack Edge Pro 2

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you configure device-related settings for your Azure Stack Edge Pro 2 device. You can set up your device name, update server, and time server via the local web UI.

The device settings can take around 5-7 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

Prerequisites

Before you configure device-related settings on your Azure Stack Edge Pro 2, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro 2](#).
 - You've configured network and enabled and configured compute network on your device as detailed in [Tutorial: Configure network for Azure Stack Edge Pro 2](#).

Configure device settings

Follow these steps to configure device-related settings:

1. On the **Device** page of the local web UI of your device, take the following steps:
 - a. Enter a friendly name for your device. The friendly name must contain from 1 to 13 characters and can have letter, numbers, and hyphens.
 - b. Provide a **DNS domain** for your device. This domain is used to set up the device as a file server.
 - c. To validate and apply the configured device settings, select **Apply**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The 'Device' section is highlighted with a red box. The main content area shows the 'Device' configuration page with a warning message: 'To complete this step, you will need to apply the desired device name and DNS domain.' It includes fields for 'Name' (DM1174466-904) and 'DNS domain' (vdshcsso.com, also highlighted with a red box). Below this is a table of 'Device endpoints' with columns for Service, Certificate Required, and Endpoint. The table lists various services like SMB server, NFS server, Azure Resource Manager, Blob Storage, Kubernetes API, etc., with their respective endpoint URLs. At the bottom are 'Apply', '< Back to Get started', and 'Next: Update server >' buttons.

If you've changed the device name and the DNS domain, the automatically generated self-signed certificates on the device won't work. You'll see a warning to this effect.

Warning

If you change the device name or DNS domain, you must upload new certificates for the device to work properly.

Apply

Cancel

- d. When the device name and the DNS domain are changed, the SMB endpoint is created.
- e. After the settings are applied, select **Next: Update server**.

Device

Device name
Assign a friendly name and DNS domain for the device.

* Name: DM1174466-904 ✓
* DNS domain: wdshcsso.com ✓

Device endpoints
Use these device endpoints to reach the following services. Some services require a certificate. For those services, certificates must be uploaded for the endpoint to be valid.

Service	Certificate Required	Endpoint
SMB server	No	\dm1174466-904.wdshcsso.com\Share name
NFS server	No	\\\192.168.3.82\Share name
Azure Resource Manager login	Yes	https://login.dm1174466-904.microsoftdatadox.com
Azure Resource Manager	Yes	https://management.dm1174466-904.microsoftdatadox.com
Blob Storage	Yes	https://[Account name].blob.dm1174466-904.microsoftdatadox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	Yes	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.
Edge container registry	Yes	Endpoint not yet created.

Apply | < Back to Get started | **Next: Update server >**

Configure update server

- On the **Update server** page of the local web UI of your device, you can now configure the location from where to download the updates for your device.
 - You can get the updates directly from the **Microsoft Update server**.

Update server
DM1174466-904

Configure update server for your device.

* Select update server type
Microsoft Update (default)

Apply | < Back to Get started | **Next: Time >**

You can also choose to deploy updates from the **Windows Server Update services (WSUS)**. Provide the path to the WSUS server.

Update server
DM1174466-904

Configure update server for your device.

* Select update server type
Windows Server Update Services

* Server URI
http://wsusserver.microsoft.com ✓

Apply | < Back to Get started | **Next: Time >**

NOTE

If a separate Windows Update server is configured and if you choose to connect over *https* (instead of *http*), then signing chain certificates required to connect to the update server are needed. For information on how to create and upload certificates, go to [Manage certificates](#).

2. Select **Apply**.
3. After the update server is configured, select **Next: Time**.

Configure time

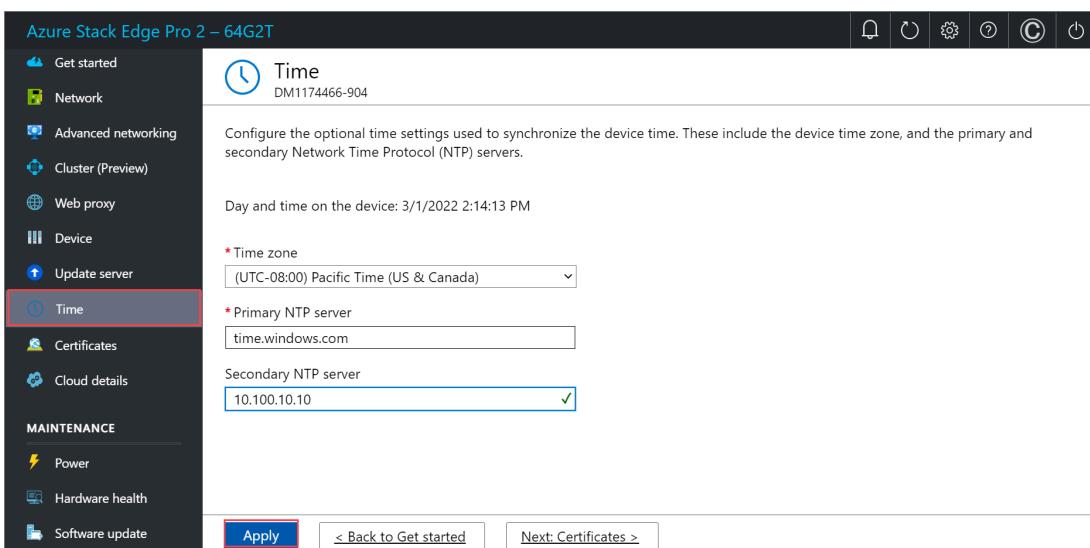
Follow these steps to configure time settings on your device.

IMPORTANT

Though the time settings are optional, we strongly recommend that you configure a primary NTP and a secondary NTP server on the local network for your device. If a local server is not available, you can configure a public NTP server.

NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

1. On the **Time** page of the local web UI of your device, you can select the time zone, and the primary and secondary NTP servers for your device.
 - a. In the **Time zone** drop-down list, select the time zone that corresponds to the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. In the **Primary NTP server** box, enter the primary server for your device or accept the default value of `time.windows.com`.
Ensure that your network allows NTP traffic to pass from your datacenter to the internet.
 - c. Optionally, in the **Secondary NTP server** box, enter a secondary server for your device.
 - d. To validate and apply the configured time settings, select **Apply**.



2. After the settings are applied, select **Next: Certificates**.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

To learn how to configure certificates for your Azure Stack Edge Pro 2 device, see:

[Configure certificates](#)

Tutorial: Configure certificates for your Azure Stack Edge Pro 2

9/21/2022 • 6 minutes to read • [Edit Online](#)

This tutorial describes how you can configure certificates for your Azure Stack Edge Pro 2 by using the local web UI.

The time taken for this step can vary depending on the specific option you choose and how the certificate flow is established in your environment.

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device
- Configure encryption-at-rest

Prerequisites

Before you configure and set up your Azure Stack Edge Pro 2 device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro 2](#).
- If you plan to bring your own certificates:
 - You should have your certificates ready in the appropriate format including the signing chain certificate.
 - If your device is deployed in Azure Government and not deployed in Azure public cloud, a signing chain certificate is required before you can activate your device.

For details on certificates, go to [Prepare certificates to upload on your Azure Stack Edge device](#).

Configure certificates for device

1. Open the [Certificates](#) page in the local web UI of your device. This page will display the certificates available on your device. The device is shipped with self-signed certificates, also referred to as the device certificates. You can also bring your own certificates.
2. *Follow this step only if you didn't change the device name or DNS domain when you [configured device settings earlier](#), and you don't want to use your own certificates.*

You don't need to perform any configuration on this page. You just need to verify that the status of all the certificates shows as valid on this page.

Name	Status	Expiration date	Thumbprint	Download
Node (A4P1074000603B)	Valid	2/28/2024	BDDDFCE394013FB8BA2D3F34C9F14AFD34C970F0	Download
Node (A6P15140005012)	Valid	2/28/2024	5F900FC9FC9719DB52E1BE75A3D713A9F95E88FD	Download
Azure Resource Manager	Valid	2/28/2024	56DE359B0219C37DE742471B7639E6BF498CBA22	Download
Blob storage	Valid	2/28/2024	11253E5C6B6794F863DFB66FD95129029D500D82	Download
Local web UI	Valid	2/28/2024	11253E5C6B6794F863DFB66FD95129029D500D82	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-
Wifi certificate	Not present	-	-	-

You're ready to configure [Encryption-at-rest](#) with the existing device certificates.

- Follow the remaining steps only if you've changed the device name or the DNS domain for your device. In these instances, the status of your device certificates will be **Not valid**. That's because the device name and DNS domain in the certificates' `subject name` and `subject alternative` settings are out of date.

You can select a certificate to view status details.

Local web UI has following errors:-

- Certificate with subject name CN=dn1174466-904.microsoftfdbbox.com and thumbprint 11253E5C6B6794F863DFB66FD95129029D500D82 does not have the correct subject name or subject alternative names for Appliance Endpoint certificate. Check the certificate you have uploaded and, if needed, bring in a new certificate.

- If you've changed the device name or DNS domain of your device, and you don't provide new certificates, **activation of the device will be blocked**. To use a new set of certificates on your device, choose one of the following options:

- Generate all the device certificates.** Select this option, and then complete the steps in [Generate device certificates](#), if you plan to use automatically generated device certificates and need to generate new device certificates. You should only use these device certificates for testing, not with production workloads.

- **Bring your own certificates.** Select this option, and then do the steps in [Bring your own certificates](#), if you want to use your own signed endpoint certificates and the corresponding signing chains. **We recommend that you always bring your own certificates for production workloads.**
 - You can choose to bring some of your own certificates and generate some device certificates. The **Generate all the device certificates** option only regenerates the device certificates.
5. When you have a full set of valid certificates for your device, select < **Back to Get started**. You can now proceed to configure [Encryption-at-rest](#).

Generate device certificates

Follow these steps to generate device certificates.

Use these steps to regenerate and download the Azure Stack Edge Pro 2 device certificates:

1. In the local UI of your device, go to **Configuration > Certificates**. Select **Generate certificates**.

Name	Status	Expiration date	Thumbprint	Download
Node (A4P1074000603B)	▲ Not valid	2/28/2024	BDDDFCE394013FB8BA2D3F34C9F14AFD34C970F0	Download
Node (A6P15140005012)	▲ Not valid	2/28/2024	5F900FC9FC9719DB52E1BE75A3D713A9F95E88FD	Download
Azure Resource Manager	▲ Not valid	2/28/2024	56DE359B0219C37DE742471B7639E6BF498CBA22	Download
Blob storage	▲ Not valid	2/28/2024	11253E5C6B6794F863DFB66FD95129029D500D82	Download
Local web UI	▲ Not valid	2/28/2024	11253E5C6B6794F863DFB66FD95129029D500D82	Download
IoT device root CA	▲ Not present	-	-	-
IoT device CA	▲ Not present	-	-	-
IoT device Key	▲ Not present	-	-	-
Kubernetes dashboard certificate	▲ Not present	-	-	-
Kubernetes dashboard key	▲ Not present	-	-	-
Edge container registry certificate	▲ Not present	-	-	-
Edge container registry key	▲ Not present	-	-	-
Wifi certificate	▲ Not present	-	-	-

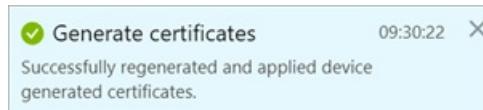
2. In the **Generate device certificates**, select **Generate**.

The device certificates are now generated and applied. It takes a few minutes to generate and apply the certificates.

IMPORTANT

While the certificate generation operation is in progress, do not bring your own certificates and try to add those via the **+ Add certificate** option.

You're notified when the operation is successfully completed. To avoid any potential cache issues, restart your browser.



3. After the certificates are generated:

- Make sure that the status of all the certificates is shown as **Valid**.

Name	Status	Expiration date	Thumbprint	Download
Node (A4P1074000603B)	Valid	2/29/2024	7F869C6C894180DF353B005A580EF0A8B32CD071	Download
Node (A6P15140005012)	Valid	2/29/2024	0354AE845853EA47A30284D834F98C27A71B2CB5	Download
Azure Resource Manager	Valid	2/29/2024	9663573EC79E3A3C12055DE1AC7A4CADCC2C443F	Download
Blob storage	Valid	2/29/2024	4D51CEFCB1C3BA406907A848D0CC2DADD6AC65C0	Download
Local web UI	Valid	2/29/2024	2EC0526170BCA57C127A53F36E86B9D4FC2C1519	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-
Wifi certificate	Not present	-	-	-

- You can select a specific certificate name, and view the certificate details.

Name	Status	Expiration date	Thumbprint
Node (A4P1074000603B)	Valid	2/29/2024	7F869C6C894180DF353B005A580EFD0AB832CD071
Node (A6P15140005012)	Valid	2/29/2024	0354AE845853EA47A302B4D834F98C27A71B2CB5
Azure Resource Manager	Valid	2/29/2024	9663573EC79E3A3C12055DE1AC7A4CADCC2C443F
Blob storage	Valid	2/29/2024	4D51CEFCB1C3BA406907A848D0CC2DADD6AC65C0
Local web UI	Valid	2/29/2024	2EC0526170BCA57C127A53F36E86B9D4FC2C1519
IoT device root CA	Not present	-	-
IoT device CA	Not present	-	-
IoT device Key	Not present	-	-
Kubernetes dashboard certificate	Not present	-	-
Kubernetes dashboard key	Not present	-	-
Edge container registry certificate	Not present	-	-
Edge container registry key	Not present	-	-
Wifi certificate	Not present	-	-

- The **Download** column is now populated. This column has links to download the regenerated certificates.

Name	Status	Expiration date	Thumbprint	Download
Node (A4P1074000603B)	Valid	2/29/2024	7F869C6C894180DF353B005A580EFD0AB832CD071	Download
Node (A6P15140005012)	Valid	2/29/2024	0354AE845853EA47A302B4D834F98C27A71B2CB5	Download
Azure Resource Manager	Valid	2/29/2024	9663573EC79E3A3C12055DE1AC7A4CADCC2C443F	Download
Blob storage	Valid	2/29/2024	4D51CEFCB1C3BA406907A848D0CC2DADD6AC65C0	Download
Local web UI	Valid	2/29/2024	2EC0526170BCA57C127A53F36E86B9D4FC2C1519	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-
Wifi certificate	Not present	-	-	-

4. Select the download link for a certificate and when prompted, save the certificate.

Name	Status	Expiration date	Thumbprint	Download
Node (A4P1074000603B)	Valid	2/29/2024	7F869C6C894180DF353B005A580EF0A8B32CD071	Download
Node (A6P15140005012)	Valid	2/29/2024	0354AE845853EA47A302B4D834F98C27A71B2CB5	Download
Azure Resource Manager	Valid	2/29/2024	9663573EC79E3A3C12055DE1AC7A4CADCC2C443F	Download
Blob storage	Valid	2/29/2024	4D51CEFCB1C3BA406907A848D0CC2DADD6AC65C0	Download
Local web UI	Valid	2/29/2024	2EC0526170BCA57C127A53F36E86B9D4FC2C1519	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-
Wifi certificate	Not present	-	-	-

5. Repeat this process for all the certificates that you wish to download.

The device generated certificates are saved as DER certificates with the following name format:

<Device name>_<Endpoint name>.cer . These certificates contain the public key for the corresponding certificates installed on the device.

You'll need to install these certificates on the client system that you're using to access the endpoints on the Azure Stack Edge device. These certificates establish trust between the client and the device.

To import and install these certificates on the client that you're using to access the device, follow the steps in [Import certificates on the clients accessing your Azure Stack Edge Pro GPU device](#).

If using Azure Storage Explorer, you'll need to install certificates on your client in PEM format and you'll need to convert the device generated certificates into PEM format.

IMPORTANT

- The download link is only available for the device generated certificates and not if you bring your own certificates.
- You can decide to have a mix of device generated certificates and bring your own certificates as long as other certificate requirements are met. For more information, go to [Certificate requirements](#).

Bring your own certificates

You can bring your own certificates.

- Start by understanding the [Types of certificates that can be used with your Azure Stack Edge device](#).

- Next, review the [Certificate requirements for each type of certificate](#).
- You can then [Create your certificates via Azure PowerShell](#) or [Create your certificates via Readiness Checker tool](#).
- Finally, [Convert the certificates to appropriate format](#) so that they're ready to upload on to your device.

Follow these steps to upload your own certificates including the signing chain.

1. To upload certificate, on the Certificate page, select + Add certificate.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T interface. On the left, there's a sidebar with various configuration options like Overview, Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time, Certificates (which is selected and highlighted with a red box), Cloud details, Power, Hardware health, Software update, Password change, and Device reset. Below these are sections for Maintenance and Troubleshooting. The main area is titled 'Certificates' and shows a list of existing certificates with columns for Name, Status, and Expiration date. A red box highlights the '+ Add certificate' button. An 'Add certificate' dialog box is overlaid on the right, prompting the user to choose the certificate type to upload. The 'Signing Chain' option is selected in a dropdown menu. There's also a 'Select a file' input field and a 'Validate & add' button at the bottom of the dialog.

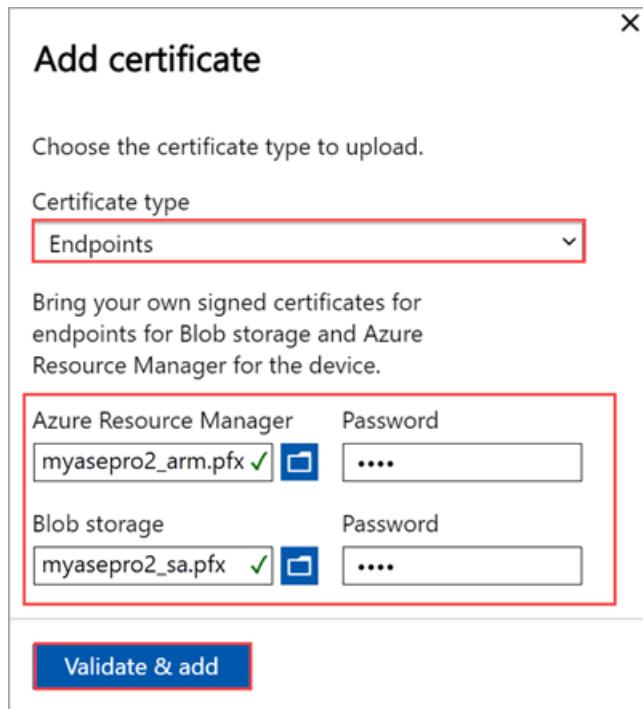
2. You can skip this step if you included all certificates in the certificate path when you [exported certificates in .pfx format](#). If you didn't include all certificates in your export, upload the signing chain, and then select **Validate & add**. You need to do this before you upload your other certificates.

In some cases, you may want to bring a signing chain alone for other purposes - for example, to connect to your update server for Windows Server Update Services (WSUS).

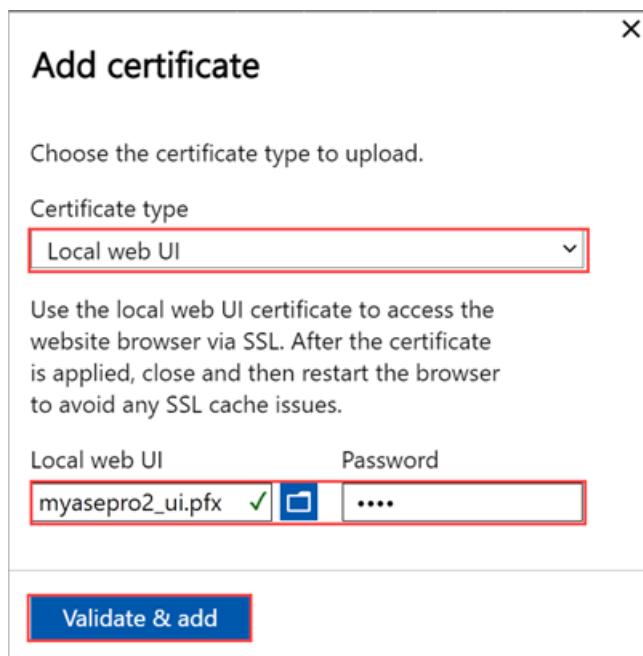
This is a detailed view of the 'Add certificate' dialog box. It starts with a header 'Add certificate' and a sub-instruction 'Choose the certificate type to upload.' A dropdown menu labeled 'Certificate type' has 'Signing Chain' selected, which is highlighted with a red box. Below this, a descriptive text explains that the user should use the certificate signing chain, including the root CA and intermediate signers, in .cer or .p7b format. A 'Signing Chain' input field contains the file path 'myasepro2_root.cer', with a green checkmark icon and a small file icon next to it. At the bottom of the dialog is a large blue 'Validate & add' button.

3. Upload other certificates. For example, you can upload the Azure Resource Manager and Blob storage

endpoint certificates.



You can also upload the local web UI certificate. After you upload this certificate, you'll be required to start your browser and clear the cache. You'll then need to connect to the device local web UI.



You can also upload the node certificate.

Add certificate

Choose the certificate type to upload.

Certificate type
Node

Upload common certificate for all nodes

Use the node certificates to connect to individual device nodes over a secure channel.

A4P1074000603B	Password
myasepro2_node1.pfx	<input type="password"/>
A6P15140005012	Password
myasepro2_node2.pfx	<input type="password"/>

Validate & add

The certificate page should update to reflect the newly added certificates. At any time, you can select a certificate and view the details to ensure that these match with the certificate that you uploaded.

Certificates

Name	Status	Expiration date	Thumbprint
Node (A4P1074000603B)	Valid	2/29/2024	7F869C6C89418C
Node (A6P15140005012)	Valid	2/29/2024	0354AE845853EA
Azure Resource Manager	Valid	2/29/2024	9663573EC79E3A3C12055DE1AC7A4CADCC2C443F
Blob storage	Valid	2/29/2024	4D51CEFCB1C3B
Local web UI	Valid	2/29/2024	2EC0526170BCA
IoT device root CA	Not present	-	-
IoT device CA	Not present	-	-
IoT device Key	Not present	-	-
Kubernetes dashboard certificate	Not present	-	-
Kubernetes dashboard key	Not present	-	-
Edge container registry certificate	Not present	-	-
Edge container registry key	Not present	-	-
Wifi certificate	Not present	-	-

NOTE

Except for Azure public cloud, signing chain certificates are needed to be brought in before activation for all cloud configurations (Azure Government or Azure Stack).

Configure encryption-at-rest

- On the **Security** tile, select **Configure** for encryption-at-rest.

NOTE

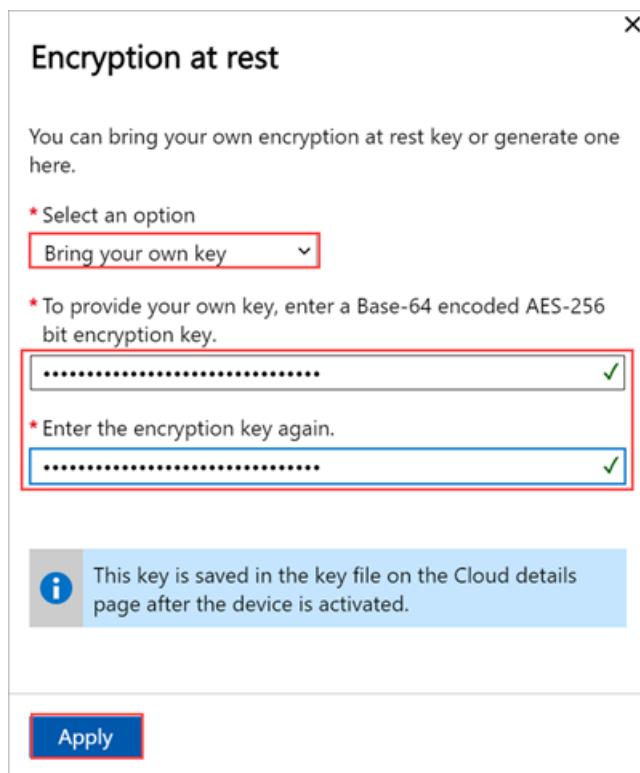
This is a required setting and until this is successfully configured, you can't activate the device.

At the factory, once the devices are imaged, the volume level BitLocker encryption is enabled. After you receive the device, you need to configure the encryption-at-rest. The storage pool and volumes are recreated and you can provide BitLocker keys to enable encryption-at-rest and thus create a second layer of encryption for your data-at-rest.

2. In the **Encryption-at-rest** pane, provide a 32 character long Base-64 encoded key. This is a one-time configuration and this key is used to protect the actual encryption key. You can choose to automatically generate this key.

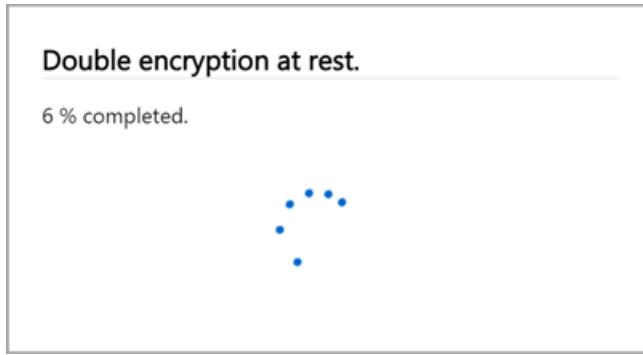


You can also enter your own Base-64 encoded AES-256 bit encryption key.



The key is saved in a key file on the **Cloud details** page after the device is activated.

3. Select **Apply**. This operation takes several minutes and the status of operation is displayed.



4. After the status shows as **Completed**, your device is now ready to be activated. Select < **Back to Get started**.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device
- Configure encryption-at-rest

To learn how to activate your Azure Stack Edge Pro 2 device, see:

[Activate Azure Stack Edge Pro 2 device](#)

Tutorial: Activate Azure Stack Edge Pro 2

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you can activate your Azure Stack Edge Pro 2 device by using the local web UI.

The activation process can take around 5 minutes to complete.

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Pro 2, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro 2](#).
 - You've configured the network and compute network settings as detailed in [Configure network, compute network, web proxy](#)
 - You've uploaded your own or generated the device certificates on your device if you changed the device name or the DNS domain via the **Device** page. If you haven't done this step, you'll see an error during the device activation and the activation will be blocked. For more information, go to [Configure certificates](#).
- You have the activation key from the Azure Stack Edge service that you created to manage the Azure Stack Edge Pro 2 device. For more information, go to [Prepare to deploy Azure Stack Edge Pro 2](#).

Activate the device

1. In the local web UI of the device, go to **Get started** page.
2. On the **Activation** tile, select **Activate**.

The screenshot shows the Azure Stack Edge Pro 2 - 64G2T configuration interface. The left sidebar contains navigation links for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The main content area is titled "Set up a 2-node cluster (Preview)" and shows the following configuration steps:

- 1 Network**: Network is Configured, Network topology is Loading.
- 2 Configure cluster**: Cluster is Configured, Cluster witness is Configured, Virtual IP settings is Configured.
- 3 Device setup**: Compute network is Not configured, Web proxy is Not configured, Device is Configured, Update is Configured with defaults, Time is Configured with defaults.
- 4 Security**: Certificates is Configured, Encryption at rest is Completed (Rotate keys).
- 5 Activation**: A note says to use the activation key from the Azure portal to activate your device. There is an "Activate" button.

- In the **Activate** pane, enter the **Activation key** from [Get the activation key for Azure Stack Edge](#).
- Select **Activate**.

Activate

Activate the device with Azure service. Learn how to [get the activation key](#). After the device is activated, the system checks for and applies any critical updates.

* Activation key
 ✓

Proactive log collection

Based on proactive log collection indicators, logs are proactively uploaded to an Azure Storage account to help Microsoft Support troubleshoot issues when they arise. [Learn more](#).

If you click the "Disable" button, you agree to deactivate the proactive log collection. After the proactive log collection is disabled, logs are not uploaded automatically if a proactive log collection indicator is detected.

Learn more about [Microsoft's privacy practices](#).

Activate

- First the device is activated. You're then prompted to download the key file.

Device activated

Successfully activated your device. Download the device key file to a secure location. These keys will be needed to facilitate a future system recovery.

[Download and continue](#)

Select **Download and continue** and save the *device-serial-nojson* file in a safe location outside of the device. **This key file contains the recovery keys for the OS disk and data disks on your device.** These keys may be needed to facilitate a future system recovery.

Here are the contents of the *json* file:

```
{  
  "Id": "<Device ID>",  
  "DataVolumeBitLockerExternalKeys": {  
    "hcsinternal": "<BitLocker key for data disk>",  
    "hcsdata": "<BitLocker key for data disk>"  
  },  
  "SystemVolumeBitLockerRecoveryKey": "<BitLocker key for system volume>",  
  "SEDEncryptionExternalKey": "<Encryption-at-rest key for encrypted disks>",  
  "ServiceEncryptionKey": "<Azure service encryption key>"  
}
```

The following table explains the various keys:

FIELD	DESCRIPTION
<code>Id</code>	This is the ID for the device.
<code>DataVolumeBitLockerExternalKeys</code>	These are the BitLocker keys for the data disks and are used to recover the local data on your device.
<code>SystemVolumeBitLockerRecoveryKey</code>	This is the BitLocker key for the system volume. This key helps with the recovery of the system configuration and system data for your device.
<code>SEDEncryptionExternalKey</code>	This user provided or system generated key is used to protect the self-encrypting data drives that have a built-in encryption.
<code>ServiceEncryptionKey</code>	This key protects the data flowing through the Azure service. This key ensures that a compromise of the Azure service won't result in a compromise of stored information.

6. Go to the **Overview** page. The device state should show as **Activated**.

System	
Health status	: Healthy
Software version	: 2.2.1868.4470
State	: Activated
Azure portal	: myasepro2twonode

Device	
Device serial number	: M1174466-904_P1074000603B
Node serial number	: A4P1074000603B
Available capacity	: 1.67 TB
Compute acceleration	: -

The device activation is complete. You can now add shares on your device.

If you encounter any issues during activation, go to [Troubleshoot activation and Azure Key Vault errors](#).

Deploy workloads

After you've activated the device, the next step is to deploy workloads.

- To deploy VM workloads, see [What are VMs on Azure Stack Edge?](#) and the associated VM deployment documentation.
- To deploy network functions as managed applications:
 - Make sure that you create a Device resource for Azure Network Function Manager (NFM) that is linked to the Azure Stack Edge resource. The device resource aggregates all the network functions deployed on Azure Stack Edge device. For detailed instructions, see [Tutorial: Create a Network Function Manager Device resource \(Preview\)](#).
 - You can then deploy Network Function Manager as per the instructions in [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).
- To deploy IoT Edge and Kubernetes workloads:
 - You'll need to first configure compute as described in [Tutorial: Configure compute on Azure Stack Edge Pro 2 device](#). This step creates a Kubernetes cluster that acts as the hosting platform for IoT Edge on your device.
 - After a Kubernetes cluster is created on your Azure Stack Edge device, you can deploy application workloads on this cluster via any of the following methods:
 - Native access via `kubectl`
 - IoT Edge
 - Azure Arc

For more information on workload deployment, see [Kubernetes workload management on your Azure Stack Edge device](#).

Next steps

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

To learn how to deploy workloads on your Azure Stack Edge device, see:

[Configure compute to deploy IoT Edge and Kubernetes workloads on Azure Stack Edge Pro 2](#)

Tutorial: Configure compute on Azure Stack Edge Pro 2

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role and create a Kubernetes cluster on your Azure Stack Edge Pro 2 device.

This procedure can take around 20 to 30 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Get Kubernetes endpoints

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro device, make sure that:

- You've activated your Azure Stack Edge Pro 2 device as described in [Activate Azure Stack Edge Pro 2](#).
- Make sure that you've followed the instructions in [Enable compute network](#) and:
 - Enabled a network interface for compute.
 - Assigned Kubernetes node IPs and Kubernetes external service IPs.

Configure compute

To configure compute on your Azure Stack Edge Pro, you'll create an IoT Hub resource via the Azure portal.

1. In the Azure portal of your Azure Stack Edge resource, go to [Overview](#), and select **IoT Edge**.

The screenshot shows the Azure Stack Edge Pro 2 Overview page. The left sidebar lists navigation options: Home, myasetest (Azure Stack Edge), Search (Ctrl+ /), Overview (highlighted with a red box), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), Monitoring (Device events, Alerts, Metrics). The main content area has a header with Update device, Reset device password, Return device, Feedback, Delete, Refresh, and JSON View. A message box says "Your device is running fine!". Below it, "Deployed edge services" shows "No deployed services". The "Edge services" section contains three cards: "Virtual machines" (New button), "IoT Edge" (highlighted with a red box), and "Cloud storage gateway". Each card has a "How to get started?" link.

2. In **Enable IoT Edge service**, select **Add**.

Home > myasetest >

IoT Edge | Overview

Azure Stack Edge

Search (Ctrl+ /) <> + Add module + Add trigger ⏪ Refresh configuration ⏴ Remove | ⏴ Refresh

Overview

Modules

Triggers

Properties

Get started with IoT Edge

Enable IoT Edge service

Enable IoT Edge service to deploy IoT Edge modules locally on your device.

To enable the service:

- 1 Set up your on-premises network for Edge computing.
- 2 Configure your Azure subscription for cloud management.

Add

Steps to deploy IoT Edge services

What's next

Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services.

3. On the **Configure Edge compute** blade, input the following information:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.
IoT Hub	Choose from New or Existing . By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.
Name	Accept the default name or enter a name for your IoT Hub resource.

Home > myasetest > IoT Edge >

Create IoT Edge service

Azure Stack Edge

Basics Review + Create

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription *	Edge Gateway Test
Resource group *	myaserg
IoT Hub *	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing myasetest-iothub

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

IoT Edge device: myasetest-edge
 IoT Gateway device: myasetest-storagegateway

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

- When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

Home > myasetest >

IoT Edge | Overview

Azure Stack Edge

Overview **Io Edge service is running fine!**
 Start processing the data using IoT Edge modules. [Learn more](#)

Modules
 IoT Edge modules are containers that run Azure services, third-party services, or your own code.
 To read data from Edge local shares for processing and uploading it to cloud, add a Module. If multiple containers are deployed, which are chained together for pipeline processing, go to [Azure IoT Hub](#).

Add module

Triggers
 Add triggers to start processing at a repeated interval or on file events such as creation of a file, modification of a file on a share.

Add trigger

Edge Shares
 For container to store or transfer files and folders to Azure Storage account (other than temp data), create a share.

[Configure Shares](#)

Edge Storage account
 For container to transfer unstructured data like binary, audio, or video streaming data to Azure Storage account, create a storage account.

[Configure Storage account](#)

Network bandwidth usage
 If containers uploads data to cloud using shares configure network bandwidth usage across multiple time-of-day schedules.

[Configure Bandwidth schedule](#)

- To confirm the Edge compute role has been configured, go to **IoT Edge > Properties**.

The screenshot shows the 'IoT Edge | Properties' page in the Azure Stack Edge portal. The left sidebar has icons for Overview, Modules, Triggers, and Properties, with 'Properties' being the active tab. The main area displays device properties in a table:

IoT Hub	myasetest-iohub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

When the Edge compute role is set up on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

It can take 20-30 minutes to configure compute because, behind the scenes, virtual machines and a Kubernetes cluster are being created.

After you have successfully configured compute in the Azure portal, a Kubernetes cluster and a default user associated with the IoT namespace (a system namespace controlled by Azure Stack Edge) exist.

Get Kubernetes endpoints

To configure a client to access Kubernetes cluster, you will need the Kubernetes endpoint. Follow these steps to get Kubernetes API endpoint from the local UI of your Azure Stack Edge device.

1. In the local web UI of your device, go to **Devices** page.
2. Under the **Device endpoints**, copy the **Kubernetes API service** endpoint. This endpoint is a string in the following format: `https://compute.<device-name>.<DNS-domain>[Kubernetes-cluster-IP-address]`.

Device name
Assign a friendly name and DNS domain for the device.

* Name: dl115
* DNS domain: teatraining1.com

Device endpoints

Service	Certificate Required	Endpoint
SMB server	No	\\\dl115.teatraining1.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.dl115.teatraining1.com
Azure Resource Manager	Yes	https://management.dl115.teatraining1.com
Blob Storage	Yes	https://[Account name].blob.dl115.teatraining1.com
Kubernetes API service	No	https://compute.dl115.teatraining1.com [10.128.45.200]
Edge IoT hub	Yes	Endpoint not yet created.

3. Save the endpoint string. You will use this endpoint string later when configuring a client to access the Kubernetes cluster via kubectl.

4. While you are in the local web UI, you can:

- Go to Kubernetes API, select **advanced settings**, and download an advanced configuration file for Kubernetes.

Device name
Assign a friendly name and DNS domain for the device.

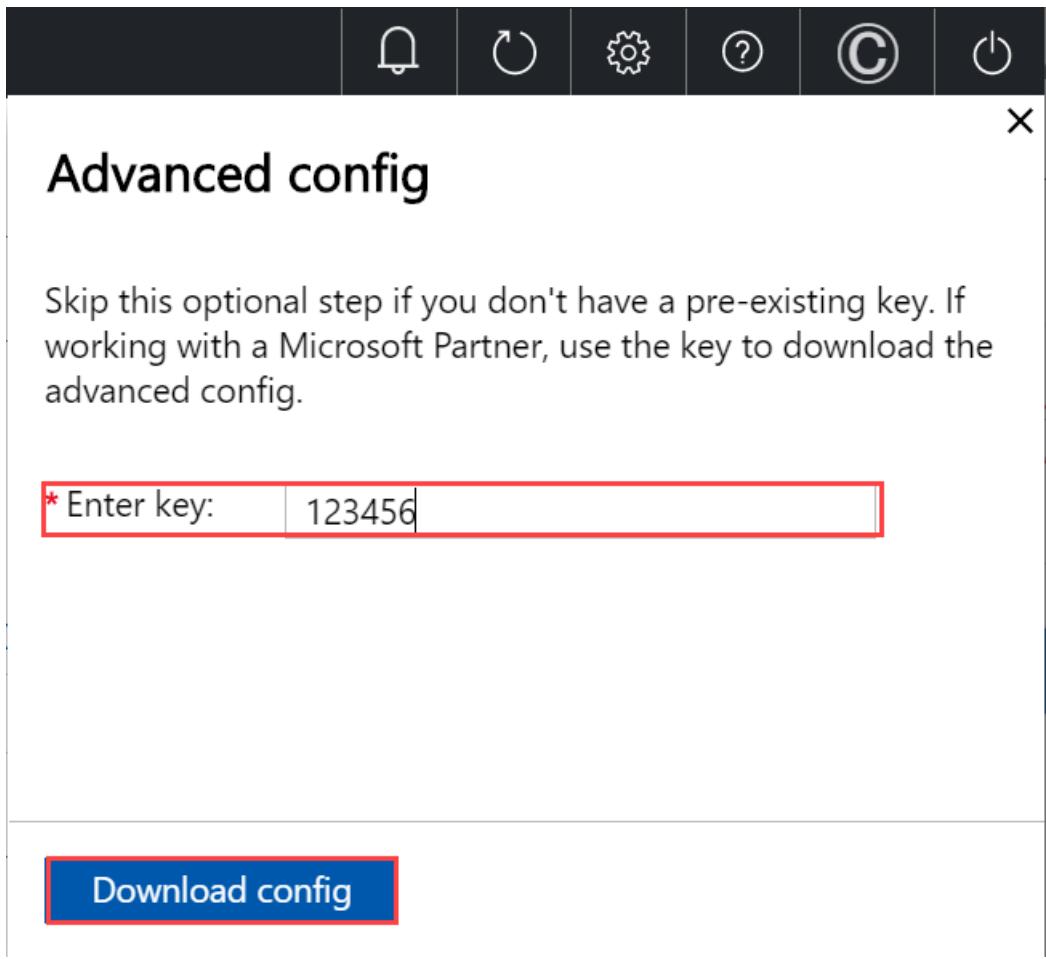
* Name: myasegpu1
* DNS domain: wdshcsso.com

Device endpoints

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241] Advanced config
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]

Buttons: Apply, < Back to Overview, Next: Update server >

If you have been provided a key from Microsoft (select users may have a key), then you can use this config file.



- You can also go to **Kubernetes dashboard** endpoint and download an `aseuser` config file.

The screenshot shows the 'Azure Stack Edge' device configuration interface. The left sidebar has a navigation menu with items like Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device), Maintenance (Power, Hardware health, Software update, Password change), and a 'CONFIGURATION' section (Update server, Time, Certificates, Cloud details). The 'Device' item in the main menu is currently selected. On the right, under the 'Device' section, there's a 'Device name' field set to 'myasegpu1'. The 'Device endpoints' section lists various services with their required certificates and endpoints:

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241]
Kubernetes dashboard	No	https://10.128.44.241:31000
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]

At the bottom, there are buttons for 'Apply', '< Back to Overview', and 'Next: Update server >'. A blue link 'Advanced config' is located near the 'Kubernetes dashboard' entry. The 'Kubernetes dashboard' row is highlighted with a red border around its 'Endpoint' column.

You can use this config file to sign into the Kubernetes dashboard or debug any issues in your Kubernetes cluster. For more information, see [Access Kubernetes dashboard](#).

Next steps

In this tutorial, you learned how to:

- Configure compute
- Get Kubernetes endpoints

To learn how to administer your Azure Stack Edge Pro 2 device, see:

[Use local web UI to administer an Azure Stack Edge Pro 2](#)

Safety instructions for your Azure Stack Edge Pro 2

9/21/2022 • 12 minutes to read • [Edit Online](#)



To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read the following safety instructions and observe all warnings and precautions in this article before unpacking, installing, or maintaining this device.

Safety icon conventions

The signal words for hazard alerting signs are:

ICON	DESCRIPTION
	DANGER: Indicates a hazardous situation that, if not avoided, will result in death or serious injury.
	WARNING: Indicates a hazardous situation that, if not avoided, could result in death or serious injury.
	CAUTION: Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

Hazard symbols identified in the manual are:

ICON	DESCRIPTION
	Read all instructions first
	Indicates information considered important, but not hazard-related.
	Hazard symbol
	Tip hazard
	Overload tip hazard

ICON	DESCRIPTION
	Electric shock hazard
	No user serviceable parts. Do not access unless properly trained.
	Crush or pinching hazard
	Hot surface. Do not touch. Allow to cool before servicing.
	Moving parts hazard

Installation and handling precautions



DANGER:

- Before you begin to unpack the equipment, to prevent hazardous situations resulting in death, serious injury and/or property damage, read, and follow all warnings and instructions.
- Inspect the as-received equipment for damages. If the equipment enclosure is damaged, [contact Microsoft Support](#) to obtain a replacement. Don't attempt to operate the device.



CAUTION:

- If you suspect the device is malfunctioning, [contact Microsoft Support](#) to obtain a replacement. Don't attempt to service the equipment.
- Always wear the appropriate clothing to protect skin from sharp metal edges and avoid sliding any metal edges against skin. Always wear appropriate eye protection to avoid injury from objects that may become airborne.
- Laser peripherals or devices may be present. To avoid risk or radiation exposure and/or personal injury, don't open the enclosure of any laser peripheral or device. Laser peripherals or devices aren't serviceable. Only use certified and rated Laser Class I for optical transceiver products.



WARNING:

- When installing into an equipment rack, the rack must be anchored to an unmovable support to prevent it from tipping before the rack-mounted equipment is installed or extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.
- When using an equipment rack, the rack may tip over causing serious personal injury. Verify the equipment rack is anchored to the floor and/or bayed to its adjacent equipment racks before installing, extending, or removing equipment. Failure to do so could allow the rack system to tip over leading to death, injury, or damage.

- When installed into an equipment rack, don't extend more than one equipment (for example, storage or server) from the rack at one time to prevent the equipment rack from becoming dangerously unstable.



WARNING:

- This equipment is not to be used as shelves or work spaces. Do not place objects on top of the equipment. Adding any type of load to a rack or wall mounted equipment can create a potential tip or crush hazard which could lead to injury, death, or product damage.



CAUTION:

- Parts enclosed within panels containing this symbol contain no user-serviceable parts. Hazardous voltage, current, and energy levels are present inside. Don't open. Return to manufacturer for servicing. Open a ticket with [Microsoft Support](#).
- The equipment contains coin cell batteries. There's a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.



CAUTION:

- If the equipment has been running, any installed component, processor(s), and heat sink(s) may be hot. Allow the equipment to cool before opening the cover to avoid the possibility of coming into contact with hot component(s). Ensure that you're wearing proper personal protective equipment (PPE) with suitable thermal insulation when hot-swapping any components.



CAUTION:

- CAUTION: Avoid wearing loose clothing items, jewelry, or loose long hair when working near an actively spinning fan.



WARNING:

- The system is designed to operate in a controlled environment. Choose a site that is:
 - Indoors, not exposed to moisture or rain.
 - Well ventilated and away from sources of heat including direct sunlight and radiators.
 - Located in a space that minimizes vibration and physical shock.
 - Isolated from strong electromagnetic fields produced by electrical devices.
 - Provided with properly grounded outlets.
 - Provided with sufficient space to access the power supply cord, because it serves as the product's main power disconnect.
- To reduce the risk of fire or electric shock, install the equipment/system in a temperature-controlled indoor area free of conductive contaminants. Don't place the equipment near liquids or in an excessively humid environment.
- Don't allow any liquid or any foreign object to enter the device. Don't place beverages or any other liquid containers on or near the device.



CAUTION:

- Elevated operating ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma} is 45°C) specified by the manufacturer.
- Reduced air flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment isn't compromised. Carefully route cables as directed to minimize airflow blockage and cooling problems.
- Don't use equipment if rails require excessive force when sliding the inner drawer assembly.



WARNING:

- This equipment has only been certified for use with mounting accessories provided with the equipment. The use of any other mounting device that hasn't been certified for use with this equipment may cause severe injuries.
- When provided with the equipment, carefully follow all instructions provided with the Wall Mount Equipment Bracket or the Slide Rail Kits. Failure to install these accessories properly can cause severe injuries.
- The two and four post Slide Rail Kits are only compatible with the rack specifications in Electronic Industries Association (EIA) standard EIA-310-D. Choosing a rack that doesn't comply with the EIA-310-D specifications can cause hazards that can lead to severe injuries.



CAUTION:

- Don't place fingers on the bearing tracks during slide rails installation (read slide rails installation instructions). Sliding of rails over bearings can pose a risk of pinching.

Electrical precautions



WARNING:

- Hazardous voltage, current, or energy levels are present inside this equipment and any component displaying this symbol: Don't service the equipment until all input power is removed, unless directed otherwise by the service instructions in an accompanying document for the component being serviced. To remove all input power, the equipment power cable must be disconnected from the AC electrical mains supply. Don't remove cover or barrier on any component that contains this label: Servicing should only be performed by qualified trained technicians.



WARNING:

- Don't install equipment into a rack or on a wall while they're energized with external cables.
- Ensure power cords aren't crushed or damaged during installation.
- Provide a safe electrical earth connection to the power supply cord. The AC cord has a three-wire grounding plug (a plug that has a grounding contact). This plug fits only a grounded AC outlet. Don't defeat the purpose of the grounding contact.
- Given that the plug on the power supply cord is the main disconnect device, ensure that the socket outlets are located near the equipment and are easily accessible.
- Unplug the power cord (by pulling the plug, not the cord) and disconnect all cables if any of the following conditions exist:
 - The power cord or plug becomes frayed or otherwise damaged
 - You spill something into the device casing

- The device is exposed to rain, excess moisture, or other liquids. The device has been dropped and the device casing is damaged
- You suspect the device needs service or repair
- Permanently unplug the unit before you move it or if you think it has become damaged in any way.
- Provide a suitable power source with electrical overload protection to meet the power specifications shown on the equipment rating label provided with the equipment.
- Don't attempt to modify or use AC power cord(s) other than the ones provided with the equipment.



WARNING:

- To reduce the risk of electrical shock, injury from moving parts, damage, or loss of data, always make sure to disconnect the equipment from the AC electrical source when working inside the equipment. Powering down the system doesn't ensure there's no electrical activity inside the equipment.

Electrostatic precautions

! NOTICE:

- Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD work-station. If one isn't available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground any unpainted metal surface on the equipment when handling parts.
- ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the equipment, place the board component side up on a grounded, static-free surface. Use a conductive foam pad if available but not the board wrapper. Don't slide board over any surface.
- Wear a grounded wrist strap. If none are available, discharge any personal static electricity by touching the bare metal chassis of the server, or the bare metal body of any other grounded device.
- Humid environments tend to have less static electricity than dry environments. A grounding strap is warranted whenever danger of static electricity exists.

! NOTICE:

- Leave all replacement components inside their static-proof packaging until you're ready to use them.

Regulatory information

Regulatory model numbers: DB040 and DB040-W

This equipment is designed for use with NRTL Listed (UL, CSA, ETL, etc.), and IEC/EN 60950-1 or IEC/EN 62368-1 compliant (CE marked) Information Technology equipment.

This equipment is designed to operate in the following environment:

- Temperature specifications
 - Storage: -40°C to 70°C (-40°F to 149°F)
 - Operating: 10°C to 45°C (50°F to 113°F)
- Relative humidity specifications
 - Storage: 5% to 95% relative humidity
 - Operating: 5% to 85% relative humidity
 - For models with GPU(s), derate allowable max operating temperature by 1°C/210m (2.6°F/1000ft) above 950m (3,117ft).
- Maximum altitude specifications

- Operating: 3,050 meters (10,000 feet)
- Storage: 9,150 meters (30,000 feet)

For electrical supply ratings, refer to the equipment rating label provided with the unit.

! NOTICE: Changes or modifications made to the equipment not expressly approved by Microsoft may void the user's authority to operate the equipment.

USA and Canada

Supplier's Declaration of Conformity

Models: DB040, DB040-W

! NOTICE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Tout changement ou modification non expressément approuvé par la partie responsable de la conformité pourrait annuler l'autorité de l'utilisateur d'utiliser cet équipement.

CAN ICES-3(A)/NMB-3(A)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA.

United States: (800) 426-9400

Canada: (800) 933-4750

For model: DB040-W only

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems. Users are advised that high-power radars are allocated as primary users (priority users) of the bands 5250–5350 MHz and 5650–5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux. Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Exposure to Radio Frequency (RF) Energy

This equipment should be installed and operated with a minimum distance of 20 cm (8 inches) between the radiator and your body. This transmitter must not be colocated or operating with any other antenna or transmitter.

This equipment complies with FCC/ISED radiation exposure limits set forth for an uncontrolled environment. Additional information about radiofrequency safety can be found on the FCC website at <https://www.fcc.gov/general/radio-frequency-safety-0> and the Industry Canada website at <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01904.html>

Detachable antenna usage This radio transmitter [IC: 7542A-MT7921] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 7542A-MT7921] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Brand	Model	Antenna Type	Connector	Max Gain (dBi)		Impedance (Ω)
				2.4GHz	5GHz	
Foxconn	ANEP2M1-CZZ02-EH	Dipole	R-SMA	3.0	4.0	50
Inpaq	DAM-D2-H-N0-000-04-02	Dipole	R-SMA	3.5	4.5	50

European Union



WARNING:

- This device is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



For Model: DB040-W only

Hereby, declares that this device is in compliance with EU Directive 2014/53/EU and UK Radio Equipment Regulations 2017 (S.I. 2017/1206). The full text of the EU and UK declaration of conformity are available on the [product webpage](#).

This device may operate in all member states of the EU. Observe national and local regulations where the device is used. This device is restricted to indoor use only when operating in the 5150 - 5350 MHz frequency range in the following countries:

	AT	BE	BG	CH	CY	CZ	DE
	DK	EE	EL	ES	FI	FR	HR
	HU	IE	IS	IT	LI	LT	LU
	LV	MT	NL	NO	PL	PT	RO
	SE	SI	SK	TR	UK(NI)		

In accordance with Article 10.8(a) and 10.8(b) of the Radio Equipment Directive (RED), the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

FREQUENCY BAND (MHZ)	MAXIMUM EIRP (DBM)
2400 - 2483.5	19.74
5150 - 5350	22.56
5470 - 5725	19.68
5725 - 5875	13.83

Notice: This device is a receiver category 1 device under EN 300 440

Disposal of waste batteries and waste electrical and electronic equipment



This symbol on the product, its batteries, or its packaging means that this product and any batteries it contains must not be disposed of with your household waste. It is your responsibility to hand this product over to an applicable collection point for the recycling of batteries and electrical and electronic equipment. This separate collection and recycling will help to conserve natural resources and prevent potential negative consequences for human health and the environment due to the possible presence of hazardous substances in batteries and electrical and electronic equipment, which could be caused by inappropriate disposal. For more information about where to drop off your batteries and waste electrical and electronic equipment (WEEE), contact your local city/municipality office, your household waste disposal service, or the shop where you purchased this product. Contact erecycle@microsoft.com for additional information on WEEE.

This product might contain Lithium-Ion and/or Lithium Metal battery(ies).

Microsoft Ireland Sandyford Ind Est Dublin D18 KX32 IRL

Telephone number: +353 1 295 3826

Fax number: +353 1 706 4110

Japan

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Declarations of conformity

A Declaration of Conformity (DoC) is a document stating that a product meets the legal standards to which it must adhere, such as safety regulations. Here is the declaration of conformity for EU:



EU Declaration of Conformity

We, Microsoft Corporation, declare under our sole responsibility that **Server** model number **DB040-W** is in conformity with the essential requirements and other relevant requirements of the following directive(s) of the European Parliament and European Council:

- *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC*
- *Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment*
- *Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products*

The following harmonized standards and technical specifications have been applied:

- **EN 63000:2018**, Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances
- **EN 300 328 V2.2.2**, Wideband Transmission Systems - Data transmission equipment operating in the 2.4GHz ISM band and using wide band modulation techniques
- **EN 301 893 V2.1.1**, 5 GHz RLAN
- **EN 300 440 V2.1.1**, Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range
- **EN 301 489-1 v.2.2.3**, EMC standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 v.3.2.4**, EMC Standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems
- **EN 62311: 2008**, Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
- **EN 55032:2015/A11:2020**, Electromagnetic compatibility of multimedia equipment, Emission requirements, Class A
- **EN 61000-3-2:2014**, Electromagnetic compatibility (EMC), Part 3-2: Limits, Limits for harmonic current emissions
- **EN 61000-3-3:2013**, Electromagnetic compatibility (EMC), Part 3-3: Limits, Limitation of voltage changes, voltage fluctuations and flicker in public low- voltage supply systems
- **EN 55035:2017/A11:2020**, Information technology equipment, Immunity characteristics, Limits and methods of measurement
- **EN 62368-1:2014/AC:2015**, Audio/video, information and communication technology equipment - Part 1: Safety requirements
- **Commission Regulation (EU) No 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013**

Manufacturer: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States

A handwritten signature in black ink.

Michele Falcon, Director, HW Engineering

February 21, 2022

DoC #: DB040-W_20220221_EU

Here is the declaration of conformity for UK:



UK Declaration of Conformity

We, Microsoft Corporation, declare under our sole responsibility that **Server** model number **DB040-W**, is in conformity with the following essential and relevant UK statutory requirements:

- The Radio Equipment Regulations 2017 (S.I. 2017/1206), as amended by the applicable 'EU Exit' legislation
- The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (UK S.I. 2012/3032) and amendments
- The Ecodesign for Energy-Related Products and Energy Information (S.I. 2010/2617), as amended by the applicable 'EU Exit' legislation

The following relevant designated standards and technical specifications have been applied in relation to which conformity is declared:

- **BS EN 55032:2015/A11:2020**, Electromagnetic compatibility of multimedia equipment, Emission requirements, Class A
- **EN 300 328 V2.2.2**, Wideband Transmission Systems - Data transmission equipment operating in the 2.4GHz ISM band and using wide band modulation techniques
- **EN 301 893 V2.1.1**, 5 GHz RLAN
- **EN 300 440 V2.1.1**, Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range
- **EN 301 489-1 v.2.2.3**, EMC standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 v.3.2.4**, EMC Standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems
- **EN 62311:2008**, Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
- **BS EN 61000-3-2:2014**, Electromagnetic compatibility (EMC), Part 3-2: Limits, Limits for harmonic current emissions
- **BS EN 61000-3-3:2013**, Electromagnetic compatibility (EMC), Part 3-3: Limits, Limitation of voltage changes, voltage fluctuations and flicker in public low- voltage supply systems
- **BS EN 55035:2017/A11:2020**, Information technology equipment, Immunity characteristics, Limits and methods of measurement
- **BS EN 62368-1:2014/AC:2015**, Audio/video, information and communication technology equipment - Part 1: Safety requirements
- **Commission Regulation (EU) No 2019/424** of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013
- **BS EN IEC 63000:2018**, Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

Manufacturer: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States

A handwritten signature in black ink.

Michele Falcon, Director, HW Engineering

February 8, 2022

DoC #: DB040-W_20220208_UK

Next steps

- Prepare to deploy Azure Stack Edge Pro 2 device

System requirements for Azure Stack Edge Pro 2

9/21/2022 • 9 minutes to read • [Edit Online](#)

This article describes the important system requirements for your Azure Stack Edge Pro 2 solution and for the clients connecting to Azure Stack Edge Pro 2 device. We recommend that you review the information carefully before you deploy your Azure Stack Edge Pro 2. You can refer back to this information as necessary during the deployment and subsequent operation.

The system requirements for the Azure Stack Edge Pro 2 include:

- **Software requirements for hosts** - describes the supported platforms, browsers for the local configuration UI, SMB clients, and any additional requirements for the clients that access the device.
- **Networking requirements for the device** - provides information about any networking requirements for the operation of the physical device.

Supported OS for clients connected to device

Here is a list of the supported operating systems for clients or hosts connected to your device. These operating system versions were tested in-house.

OPERATING SYSTEM/PLATFORM	VERSIONS
Windows Server	2016 2019
Windows	10
SUSE Linux	Enterprise Server 12 (x86_64)
Ubuntu	16.04.3 LTS
CentOS	7.0
Mac OS	10.14.1

Supported protocols for clients accessing device

Here are the supported protocols for clients accessing your device.

PROTOCOL	VERSIONS	NOTES
SMB	2.X, 3.X	SMB 1 isn't supported.
NFS	3.0, 4.1	Mac OS is not supported with NFS v4.1.

Supported Azure Storage accounts

Here is a list of the supported storage accounts for your device.

STORAGE ACCOUNT	NOTES
Classic	Standard
General Purpose	Standard; both V1 and V2 are supported. Both hot and cool tiers are supported.

Supported Edge storage accounts

The following Edge storage accounts are supported with REST interface of the device. The Edge storage accounts are created on the device. For more information, see [Edge storage accounts](#).

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob	

*Page blobs and Azure Files are currently not supported.

Supported local Azure Resource Manager storage accounts

These storage accounts are created via the device local APIs when you are connecting to local Azure Resource Manager. The following storage accounts are supported:

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob, Page Blob	SKU type is Standard_LRS
Premium	GPv1: Block Blob, Page Blob	SKU type is Premium_LRS

Supported storage types

Here is a list of the supported storage types for the device.

FILE FORMAT	NOTES
Azure block blob	
Azure page blob	
Azure Files	

Supported browsers for local web UI

Here is a list of the browsers supported for the local web UI for the virtual device.

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Google Chrome	Latest version	
Microsoft Edge	Latest version	

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Internet Explorer	Latest version	If enhanced security features are enabled, you may not be able to access local web UI pages. Disable enhanced security, and restart your browser.
FireFox	Latest version	
Safari on Mac	Latest version	

Networking port requirements

Port requirements for Azure Stack Edge Pro 2

The following table lists the ports that need to be opened in your firewall to allow for SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access to your device. *Out* or *outbound* refers to the direction in which your Azure Stack Edge Pro 2 device sends data externally, beyond the deployment, for example, outbound to the internet.

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	NOTES
TCP 80 (HTTP)	Out	WAN	No	Outbound port is used for internet access to retrieve updates. The outbound web proxy is user configurable.
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable.
UDP 123 (NTP)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based NTP server.
UDP 53 (DNS)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based DNS server. We recommend using a local DNS server.
TCP 5985 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTP.

Port No.	In or Out	Port Scope	Required	Notes
TCP 5986 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTPS.
UDP 67 (DHCP)	Out	LAN	In some cases See notes	This port is required only if you're using a local DHCP server.
TCP 80 (HTTP)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. Accessing the local UI over HTTP will automatically redirect to HTTPS.
TCP 443 (HTTPS)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. This port is also used to connect Azure Resource Manager to the device local APIs, to connect Blob storage via REST APIs, and to the Security token service (STS) to authenticate via access and refresh tokens.
TCP 445 (SMB)	In	LAN	In some cases See notes	This port is required only if you are connecting via SMB.
TCP 2049 (NFS)	In	LAN	In some cases See notes	This port is required only if you are connecting via NFS.

Port requirements for IoT Edge

Azure IoT Edge allows outbound communication from an on-premises Edge device to Azure cloud using supported IoT Hub protocols. Inbound communication is only required for specific scenarios where Azure IoT Hub needs to push down messages to the Azure IoT Edge device (for example, Cloud To Device messaging).

Use the following table for port configuration for the servers hosting Azure IoT Edge runtime:

Port No.	In or Out	Port Scope	Required	Guidance
----------	-----------	------------	----------	----------

Port No.	In or Out	Port Scope	Required	Guidance
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound open for IoT Edge provisioning. This configuration is required when using manual scripts or Azure IoT Device Provisioning Service (DPS).

For complete information, go to [Firewall and port configuration rules for IoT Edge deployment](#).

Port requirements for Kubernetes on Azure Stack Edge

Port No.	In or Out	Port Scope	Required	Guidance
TCP 31000 (HTTPS)	In	LAN	In some cases. See notes.	This port is required only if you are connecting to the Kubernetes dashboard to monitor your device.
TCP 6443 (HTTPS)	In	LAN	In some cases. See notes.	This port is required by Kubernetes API server only if you are using <code>kubectl</code> to access your device.

IMPORTANT

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are in the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your Azure Stack Edge Pro 2 device and the service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. These changes require the network administrator to monitor and update firewall rules for your Azure Stack Edge Pro 2 as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on Azure Stack Edge Pro 2 fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

NOTE

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for gateway feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.com/* https://*.servicebus.windows.net/* https://login.microsoftonline.com https://login.microsoftonline.net	Azure Stack Edge service Azure Service Bus Authentication Service - Azure Active Directory
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.windows.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt https://management.azure.com/	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://azureprofilerfrontdoor.cloudapp.net	Azure Traffic Manager
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
<a href="http://<vault-name>.vault.azure.net:443">http://<vault-name>.vault.azure.net:443	Key Vault

URL patterns for compute feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscc.io	
https://*.azurecr.io	Personal and third-party container registries (optional)
https://*.azure-devices.net	IoT Hub access (required)
https://*.docker.com	StorageClass (required)

URL patterns for monitoring

Add the following URL patterns for Azure Monitor if you're using the containerized version of the Log Analytics

agent for Linux.

URL PATTERN	PORT	COMPONENT OR FUNCTIONALITY
https://ods.opinsights.azure.com	443	Data ingestion
https://*.oms.opinsights.azure.com	443	Operations Management Suite (OMS) onboarding
https://*.dc.services.visualstudio.com	443	Agent telemetry that uses Azure Public Cloud Application Insights

For more information, see [Network firewall requirements for monitoring container insights](#).

URL patterns for gateway for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.us/* https://*.servicebus.usgovcloudapi.net/* https://login.microsoftonline.us	Azure Data Box Edge/ Azure Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.us	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.usgovcloudapi.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
https://(vault-name).vault.usgovcloudapi.net:443	Key Vault

URL patterns for compute for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscr.com	
https://*.azure-devices.us	IoT Hub access (required)
https://*.azuredcrus	Personal and third-party container registries (optional)

URL patterns for monitoring for Azure Government

Add the following URL patterns for Azure Monitor if you're using the containerized version of the Log Analytics agent for Linux.

URL PATTERN	PORT	COMPONENT OR FUNCTIONALITY
https://ods.opinsights.azure.us	443	Data ingestion
https://*.oms.opinsights.azure.us	443	Operations Management Suite (OMS) onboarding
https://*.dc.services.visualstudio.com	443	Agent telemetry that uses Azure Public Cloud Application Insights

Internet bandwidth

The devices are designed to continue to operate when your internet connection is slow or gets interrupted. In normal operating conditions, we recommend that you use:

- A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
- A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Use WAN throttling to limit your WAN throughput to 64 Mbps or higher.

Compute sizing considerations

Use your experience while developing and testing your solution to ensure there is enough capacity on your Azure Stack Edge Pro 2 device and you get the optimal performance from your device.

Factors you should consider include:

- **Container specifics** - Think about the following.
 - What is your container footprint? How much memory, storage, and CPU is your container consuming?
 - How many containers are in your workload? You could have a lot of lightweight containers versus a few resource-intensive ones.
 - What are the resources allocated to these containers versus what are the resources they are consuming (the footprint)?
 - How many layers do your containers share? Container images are a bundle of files organized into a stack of layers. For your container image, determine how many layers and their respective sizes to calculate resource consumption.
 - Are there unused containers? A stopped container still takes up disk space.
 - In which language are your containers written?
- **Size of the data processed** - How much data will your containers be processing? Will this data

consume disk space or the data will be processed in the memory?

- **Expected performance** - What are the desired performance characteristics of your solution?

To understand and refine the performance of your solution, you could use:

- The compute metrics available in the Azure portal. Go to your Azure Stack Edge resource and then go to **Monitoring > Metrics**. Look at the **Edge compute - Memory usage** and **Edge compute - Percentage CPU** to understand the available resources and how are the resources getting consumed.
- To monitor and troubleshoot compute modules, go to [Debug Kubernetes issues](#).

Finally, make sure that you validate your solution on your dataset and quantify the performance on Azure Stack Edge Pro 2 before deploying in production.

Next step

- [Deploy your Azure Stack Edge Pro 2](#)

Azure Stack Edge Pro 2 limits

9/21/2022 • 3 minutes to read • [Edit Online](#)

Consider these limits as you deploy and operate your Microsoft Azure Stack Edge Pro 2 solution.

Azure Stack Edge service limits

- The storage account should be physically closest to the region where the device is deployed (can be different from where the service is deployed).
- Moving a Data Box Gateway resource to a different subscription or resource group is not supported. For more details, go to [Move resources to new resource group or subscription](#).

Azure Stack Edge Pro 2 device limits

The following table describes the limits for the Azure Stack Edge Pro 2 device.

DESCRIPTION	VALUE
No. of files per device	100 million
No. of shares per container	1
Maximum no. of share endpoints and REST endpoints per device (GPU devices only)	24
Maximum no. of tiered storage accounts per device (GPU devices only)	24
Maximum file size written to a share	5 TB
Maximum number of resource groups per device	800

Azure storage limits

This section describes the limits for Azure Storage service, and the required naming conventions for Azure Files, Azure block blobs, and Azure page blobs, as applicable to the Azure Stack Edge / Data Box Gateway service.

Review the storage limits carefully and follow all the recommendations.

For the latest information on Azure storage service limits and best practices for naming shares, containers, and files, go to:

- [Naming and referencing containers](#)
- [Naming and referencing shares](#)
- [Block blobs and page blob conventions](#)

IMPORTANT

If there are any files or directories that exceed the Azure Storage service limits, or do not conform to Azure Files/Blob naming conventions, then these files or directories are not ingested into the Azure Storage via the Azure Stack Edge / Data Box Gateway service.

Data upload caveats

Following caveats apply to data as it moves into Azure.

- We suggest that more than one device should not write to the same container.
- If you have an existing Azure object (such as a blob or a file) in the cloud with the same name as the object that is being copied, device will overwrite the file in the cloud.
- An empty directory hierarchy (without any files) created under share folders is not uploaded to the blob containers.
- You can copy the data using drag and drop with File Explorer or via command line. If the aggregate size of files being copied is greater than 10 GB, we recommend you use a bulk copy program such as Robocopy or rsync. The bulk copy tools retry the copy operation for intermittent errors and provide additional resiliency.
- If the share associated with the Azure storage container uploads blobs that do not match the type of blobs defined for the share at the time of creation, then such blobs are not updated. For example, you create a block blob share on the device. Associate the share with an existing cloud container that has page blobs. Refresh that share to download the files. Modify some of the refreshed files that are already stored as page blobs in the cloud. You will see upload failures.
- After a file is created in the shares, renaming of the file isn't supported.
- Deletion of a file from a share does not delete the entry in the storage account.
- If using rsync to copy data, then `rsync -a` option is not supported.

Azure storage account size limits

Here are the limits on the size of the data that is copied into storage account. Make sure that the data you upload conforms to these limits. For the most up-to-date information on these limits, see [Scalability and performance targets for Blob storage](#) and [Azure Files scalability and performance targets](#).

SIZE OF DATA COPIED INTO AZURE STORAGE ACCOUNT	DEFAULT LIMIT
Block Blob and page blob	500 TB per storage account

Azure object size limits

Here are the sizes of the Azure objects that can be written. Make sure that all the files that are uploaded conform to these limits.

AZURE OBJECT TYPE	UPLOAD LIMIT
Block Blob	~ 4.75 TB
Page Blob	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

AZURE OBJECT TYPE	UPLOAD LIMIT
Azure Files	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

IMPORTANT

Creation of files (irrespective of the storage type) is allowed up to 5 TB. However, if you create a file whose size is greater than the upload limit defined in the preceding table, the file does not get uploaded. You have to manually delete the file to reclaim the space.

Next steps

- [Prepare to deploy Azure Stack Edge Pro 2](#)

Technical specifications and compliance for Azure Stack Edge Pro 2

9/21/2022 • 4 minutes to read • [Edit Online](#)

The hardware components of your Azure Stack Edge Pro 2 adhere to the technical specifications and regulatory standards outlined in this article. The technical specifications describe hardware, power supply units (PSUs), storage capacity, and enclosures.

Compute and memory specifications

- [Model 64G2T](#)
- [Model 128G4T1GPU](#)
- [Model 256G6T2GPU](#)

The Azure Stack Edge Pro 2 device has the following specifications for compute and memory:

SPECIFICATION	VALUE
CPU type	Intel® Xeon® Gold 6209U CPU @ 2.10 GHz (Cascade Lake) CPU
CPU: raw	20 total cores, 40 total vCPUs
CPU: usable	32 vCPUs
Memory type	2 x 32 GB DDR4-2933 RDIMM
Memory: raw	64 GB RAM
Memory: usable	51 GB RAM

Power supply unit specifications

This device has one power supply unit (PSU) with high-performance fans. The following table lists the technical specifications of the PSUs.

SPECIFICATION	550 W PSU
Maximum output power	550 W
Heat dissipation (maximum)	550 W
Voltage range selection	100-127 V AC, 47-63 Hz, 7.1 A
Voltage range selection	200-240V AC, 47-63 Hz, 3.4 A
Hot pluggable	No

Network interface specifications

Your Azure Stack Edge Pro 2 device has four network interfaces, Port 1 - Port 4.

- **2 X 10 GBase-T/1000Base-T(10/1 GbE) interfaces**
 - Port 1 is used for initial setup and is static by default. After the initial setup is complete, you can use the interface for data with any IP address. However, on reset, the interface reverts back to static IP.
 - Port 2 is user configurable, can be used for data transfer, and is DHCP by default. These 10/1-GbE interfaces can also operate as 10-GbE interfaces.
- **2 X 100-GbE interfaces**
 - These data interfaces, Port 3 and Port 4, can be configured by user as DHCP (default) or static.

Your Azure Stack Edge Pro 2 device has the following network hardware:

- **Onboard Intel Ethernet network adapter X722** - Port 1 and Port 2. [See here for details.](#)
- **Nvidia Mellanox dual port 100-GbE ConnectX-6 Dx network adapter** - Port 3 and Port 4. [See here for details.](#)

Here are the details for the Mellanox card:

PARAMETER	DESCRIPTION
Model	ConnectX®-6 Dx network interface card
Model Description	100 GbE dual-port QSFP56
Device Part Number	MCX623106AC-CDAT, with crypto or with secure boot

Storage specifications

- [Model 64G2T](#)
- [Model 128G4T1GPU](#)
- [Model 256G6T2GPU](#)

The following table lists the storage capacity of the device.

SPECIFICATION	VALUE
Boot disk	1 NVMe SSD
Boot disk capacity	960 GB
Number of data disks	2 SATA SSDs
Single data disk capacity	960 GB
Total capacity	2 TB
Total usable capacity	720 GB
RAID configuration	Storage Spaces Direct with mirroring

Enclosure dimensions and weight specifications

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The Azure Stack Edge Pro 2 is designed to fit in a standard 19" equipment rack and is two rack units high (2U).

The enclosure dimensions are identical across all models of Azure Stack Edge Pro 2.

The following table lists the dimensions of the 2U device enclosure in millimeters and inches.

ENCLOSURE	MILLIMETERS	INCHES
Height	87.0	3.43
Width	482.6	19.00
Depth	430.5	16.95

The following table lists the dimensions of the shipping package in millimeters and inches.

PACKAGE	MILLIMETERS	INCHES
Height	241.3	9.50
Width	768.4	30.25
Depth	616.0	24.25

Enclosure weight

- [Model 642GT](#)
- [Model 128G4T1GPU](#)
- [Model 256G6T2GPU](#)

LINE #	HARDWARE	WEIGHT LBS
1	Model 642GT	21.0
2	Shipping weight, with 4-post mount	35.3
3	Model 642GT install handling, 4-post (without bezel and with inner rails attached)	20.4
4	Shipping weight, with 2-post mount	32.1
5	Model 642GT install handling, 2-post (without bezel and with inner rails attached)	20.4

LINE #	HARDWARE	WEIGHT LBS
6	Shipping weight with wall mount	31.1
7	Model 642GT install handling without bezel	19.8
4	4-post in box	6.28
7	2-post in box	3.08
10	Wallmount as packaged	2.16

Next steps

[Deploy your Azure Stack Edge Pro 2](#)

Clustering on your Azure Stack Edge Pro GPU device

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2

This article provides a brief overview of clustering on your Azure Stack Edge device.

About failover clustering

Azure Stack Edge can be set up as a single standalone device or a two-node cluster. A two-node cluster consists of two independent Azure Stack Edge devices that are connected by physical cables and by software. These nodes when clustered work together as in a Windows failover cluster, provide high availability for applications and services that are running on the cluster.

If one of the clustered nodes fails, the other node begins to provide service (the process is known as failover). The clustered roles are also proactively monitored to make sure that they're working properly. If they aren't working, they're restarted or moved to the second node.

Azure Stack Edge uses Windows Server Failover Clustering for its two-node cluster. For more information, see [Failover clustering in Windows Server](#).

Cluster quorum and witness

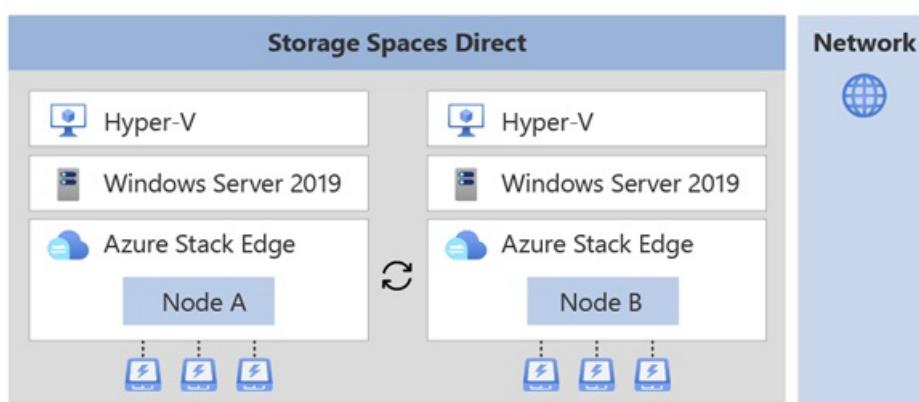
A quorum is always maintained on your Azure Stack Edge cluster to remain online in the event of a failure. If one of the nodes fails, then the majority of the surviving nodes must verify that the cluster remains online. The concept of majority only exists for clusters with an odd number of nodes. For more information on cluster quorum, see [Understand quorum](#).

For an Azure Stack Edge cluster with two nodes, if a node fails, then a cluster witness provides the third vote so that the cluster stays online (since the cluster is left with two out of three votes - a majority). A cluster witness is required on your Azure Stack Edge cluster. You can set up the witness in the cloud or in a local fileshare using the local UI of your device.

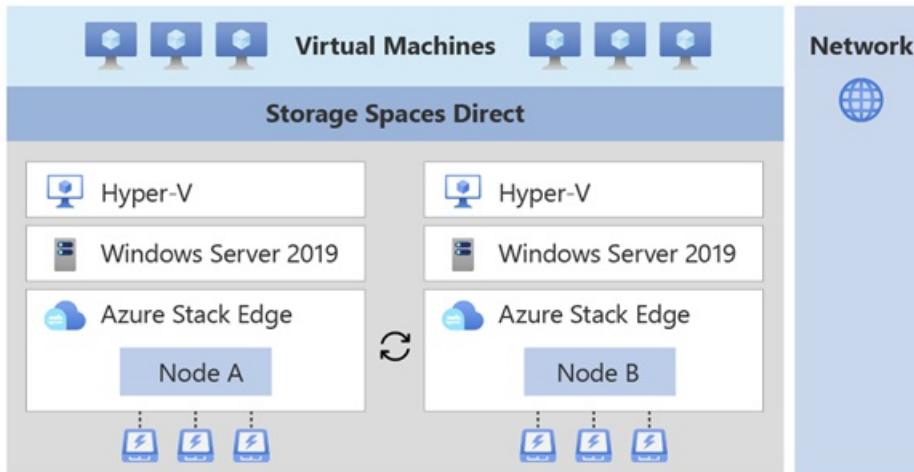
For more information on cluster witness, see [Cluster witness on Azure Stack Edge](#).

Infrastructure cluster

The infrastructure cluster on your device provides persistent storage and is shown in the following diagram:



- The infrastructure cluster consists of the two independent nodes running Windows Server operating system with a Hyper-V layer. The nodes contain physical disks for storage and network interfaces that are connected back-to-back or with switches.
- The disks across the two nodes are used to create a logical storage pool. The storage spaces direct on this pool provides mirroring and parity for the cluster.
- You can deploy your application workloads on top of the infrastructure cluster.
 - Non-containerized workloads such as VMs can be directly deployed on top of the infrastructure cluster.



- Containerized workloads use Kubernetes for workload deployment and management. A Kubernetes cluster that consists of a master VM and two worker VMs (one for each node) is deployed on top of the infrastructure cluster.

The Kubernetes cluster allows for application orchestration whereas the infrastructure cluster provides persistent storage.

Supported networking topologies

Based on the use-case and workloads, you can select how the two Azure Stack Edge device nodes will be connected. The networking topologies available will differ depending on whether you use an Azure Stack Edge Pro GPU device or an Azure Stack Edge Pro 2 device.

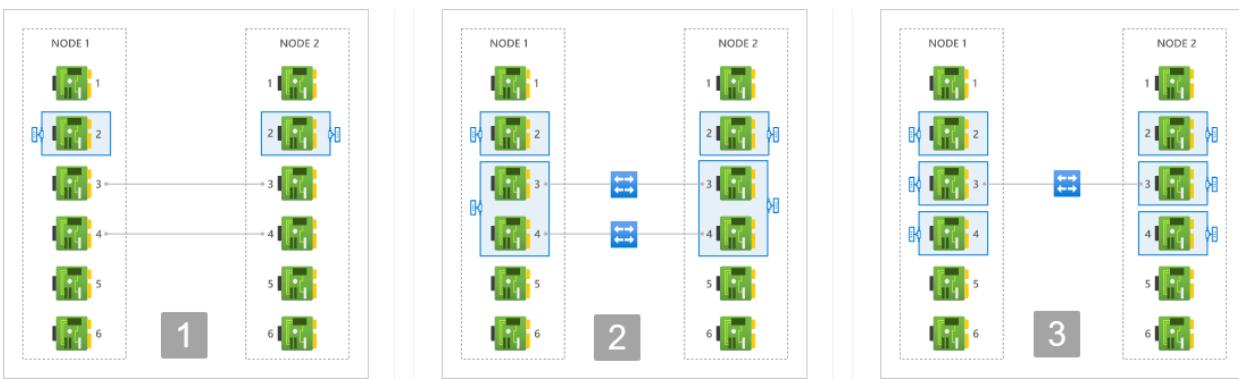
The supported network topologies for each of the device types are described here.

- [Azure Stack Edge Pro GPU](#)
- [Azure Stack Edge Pro 2](#)

On your Azure Stack Edge Pro GPU device node:

- Port 2 is used for management traffic.
- Port 3 and Port 4 are used for storage and cluster traffic. This traffic includes that needed for storage mirroring and Azure Stack Edge cluster heartbeat traffic that is required for the cluster to be online.

The following network topologies are available:



- Switchless** - Use this option when you don't have high speed switches available in the environment for storage and cluster traffic.

In this option, Port 3 and Port 4 are connected back-to-back without a switch. These ports are dedicated to storage and Azure Stack Edge cluster traffic and aren't available for workload traffic. Optionally you can also provide IP addresses for these ports.

- Using switches and NIC teaming** - Use this option when you have high speed switches available for use with your device nodes for storage and cluster traffic.

Each of ports 3 and 4 of the two nodes of your device are connected via an external switch. The Port 3 and Port 4 are teamed on each node and a virtual switch and two virtual NICs are created that allow for port-level redundancy for storage and cluster traffic. These ports can be used for workload traffic as well.

- Using switches and without NIC teaming** - Use this option when you need an extra dedicated port for workload traffic and port-level redundancy isn't required for storage and cluster traffic.

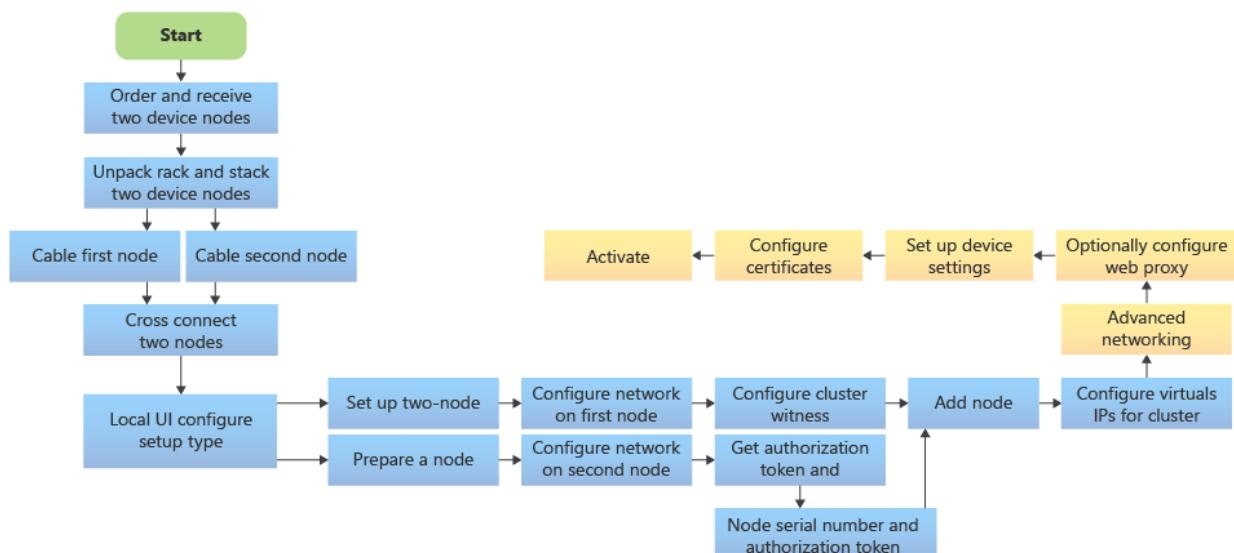
Port 3 on each node is connected via an external switch. If Port 3 fails, the cluster may go offline. Separate virtual switches are created on Port 3 and Port 4.

For more information, see how to [Choose a network topology for your device node](#).

Cluster deployment

- [Azure Stack Edge Pro GPU](#)
- [Azure Stack Edge Pro 2](#)

Before you configure clustering on your device, you must cable the devices as per one of the supported network topologies that you intend to configure. To deploy a two-node infrastructure cluster on your Azure Stack Edge devices, follow these high-level steps:



1. Order two independent Azure Stack Edge devices. For more information, see [Order an Azure Stack Edge device](#).
2. Cable each node independently as you would for a single node device. Based on the workloads that you intend to deploy, cross connect the network interfaces on these devices via cables, and with or without switches. For detailed instructions, see [Cable your two-node cluster device](#).
3. Start cluster creation on the first node. Choose the network topology that conforms to the cabling across the two nodes. The chosen topology would dictate the storage and clustering traffic between the nodes. See detailed steps in [Configure network and web proxy on your device](#).
4. Prepare the second node. Configure the network on the second node the same way you configured it on the first node. Get the authentication token on this node.
5. Use the authentication token from the prepared node and join this node to the first node to form a cluster.
6. Set up a cloud witness using an Azure Storage account or a local witness on an SMB fileshare.
7. Assign a virtual IP to provide an endpoint for Azure Consistent Services or when using NFS.
8. Assign compute or management intents to the virtual switches created on the network interfaces. You may also configure Kubernetes node IPs and Kubernetes service IPs here for the network interface enabled for compute.
9. Optionally configure web proxy, set up device settings, configure certificates and then finally, activate the device.

For more information, see the two-node device deployment tutorials starting with [Get deployment configuration checklist](#).

Clustering workloads

On your two-node cluster, you can deploy non-containerized workloads or containerized workloads.

- **Non-containerized workloads such as VMs:** The two-node cluster will ensure high availability of the virtual machines that are deployed on the device cluster. Live migration of VMs isn't supported.
- **Containerized workloads such as Kubernetes or IoT Edge:** The Kubernetes cluster deployed on top of the device cluster consists of one Kubernetes master VM and two Kubernetes worker VMs. Each Kubernetes node has a worker VM that is pinned to each Azure Stack Edge node. Failover results in the failover of Kubernetes master VM (if needed) and Kubernetes-based rebalancing of pods on the surviving worker VM.

For more information, see [Kubernetes on a clustered Azure Stack Edge device](#).

Cluster management

You can manage the Azure Stack Edge cluster via the PowerShell interface of the device, or through the local UI. Some typical management tasks are:

- [Undo node preparation](#)
- [Configure cloud witness](#)
- [Set up a local witness](#)
- [Configure virtual IP settings](#)
- [Remove the cluster](#)

Cluster updates

A two-node clustered device upgrade will first apply the device updates followed by the Kubernetes cluster updates. Rolling updates to device nodes ensure minimal downtime of workloads.

When you apply these updates via the Azure portal, you only have to start the process on one node and both

the nodes are updated. For step-by-step instructions, see [Apply updates to your two-node Azure Stack Edge device](#).

Billing

If you deploy an Azure Stack Edge two-node cluster, each node is billed separately. For more information, see [Pricing page for Azure Stack Edge](#).

Next steps

- Learn about [Cluster witness for your Azure Stack Edge](#).
- See [Kubernetes for your Azure Stack Edge](#)
- Understand [Cluster failover scenarios](#)

Cluster witness on your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2

This article provides a brief overview of cluster witness on your Azure Stack Edge device including cluster witness requirements, setup, and management.

About cluster quorum and witness

In Windows Server Failover Clustering, quorum needs to be maintained in order for the Windows Server cluster to remain online in the event of a failure. When nodes in a Windows Server cluster fail, surviving nodes need to verify that they constitute the majority of the cluster to remain online.

However, the concept of majority only exists for clusters with an odd number of nodes. When the number of nodes in a cluster is even, the system requires a way to make the total number of votes odd. This is where the role of cluster witness is important. The cluster witness is given a vote, so that in the event of a failure, the total number of votes in the cluster (which originally had an even number of nodes) is odd.

For more information on cluster quorum, see [Understand cluster quorum](#).

Cluster quorum and witness on Azure Stack Edge

Windows Server Failover Clustering is implemented on a two-node Azure Stack Edge device. A quorum is always maintained on your Azure Stack Edge cluster so that the device can remain online in the event of a failure. If one of the nodes fails, then the majority of the surviving nodes must verify that the cluster remains online. The concept of majority only exists for clusters with an odd number of nodes.

For an Azure Stack Edge cluster with two nodes, if a node fails, then a cluster witness provides the third vote so that the cluster stays online (since the cluster is left with 2/3 votes - a majority).

Cluster witness on Azure Stack Edge

A two-node Azure Stack Edge cluster requires a cluster witness, so that if one of the Azure Stack Edge nodes fails, the cluster witness accounts for the third vote, and the cluster stays online (since the cluster is left with 2/3 votes - a majority). On the other hand, if both the device nodes fail simultaneously, or a second Azure Stack Edge node fails after the first has failed, there is no majority vote, and the cluster goes offline.

This system requires both Azure Stack Edge nodes to have connectivity to each other and the cluster witness. If the cluster witness were to go offline or lose connectivity with either of the device nodes, the total number of votes in the event of a single Azure Stack Edge node failure would be even. In this case, Windows Server Failover Clustering will try to remediate this by arbitrarily picking a device node that will not get to vote (in order to make the total number of votes odd). In this case, if the Azure Stack Edge node that failed happened to be the one that got the single vote in the Azure Stack Edge cluster, there will be no majority vote and the cluster will go offline. This is why, in order to prevent the Azure Stack Edge cluster from going offline in the event of a single device node failure, it is important for the cluster witness to be online and have connectivity to both the device nodes.

Witness requirements

Cluster witness can be in the cloud or live locally. In each case, there are certain requirements that the witness

must meet.

- **Cloud witness requirements**

- Both the device nodes in the cluster should have a reliable internet connection.
- Make sure that the HTTPS default port 443 is open on your device as cloud witness uses this port to establish outbound communication with the Azure blob service.

- **Local witness requirements**

- SMB 2.0 File share is created on-premises but not on the nodes of your device.
- A minimum of 5 MB of free space exists on the file share.
- Your device can access the file share over the network.

Cluster witness setup and configuration

In order for the witness to have an independent vote, it must always be hosted outside of the Azure Stack Edge nodes in the device cluster. The witness can be deployed in either of the following ways.

- **Cloud witness** - Use the cloud witness when both the nodes on your Azure Stack Edge cluster are connected to Azure. To set up a cloud witness, use an Azure Storage account in the cloud and configure the witness via the local UI of the device.

We recommend that you deploy the cloud witness with redundant connections so that the witness is highly available. For more information, see [Set up cloud witness via the local UI](#).

- **Local witness** - Use the local witness when both the nodes are not connected to Azure or have sporadic connectivity. If you're in an IT environment with other machines and file shares, use a file share witness. To set up a local witness, you can use an SMB fileshare on a local server in the network where the device is deployed and configure the fileshare path to the server via the local UI.

We recommend that you deploy the witness in a way that it is highly available. For example, a switch running a file server could be used to host a file share. For more information, see [Set up local witness via the local UI](#).

Next steps

- Learn how to [Configure cloud witness for Azure Stack Edge Pro GPU](#).
- Learn how to [Set up local witness for Azure Stack Edge Pro GPU](#).

Kubernetes failover scenarios on a clustered Azure Stack Edge device

9/21/2022 • 4 minutes to read • [Edit Online](#)

Kubernetes cluster is deployed as a popular open-source platform to orchestrate containerized applications. This article describes how Kubernetes works on your 2-node Azure Stack Edge device including the failure modes and the corresponding device responses.

About Kubernetes on Azure Stack Edge

On your Azure Stack Edge device, you can create a Kubernetes cluster by configuring the compute. When the compute role is configured, the Kubernetes cluster including the master and worker nodes are all deployed and configured for you. This cluster is then used for workload deployment via `kubectl`, IoT Edge, or Azure Arc.

The Azure Stack Edge device is available as a 1-node configuration or a 2-node configuration that constitutes the infrastructure cluster. The Kubernetes cluster is separate from the infrastructure cluster and is deployed on top of the infrastructure cluster. The infrastructure cluster provides the persistent storage for your Azure Stack Edge device while the Kubernetes cluster is responsible solely for application orchestration.

The Kubernetes cluster comprises a master node and worker nodes. The Kubernetes nodes in a cluster are virtual machines that run your applications and cloud workflows.

- The Kubernetes master node is responsible for maintaining the desired state for your cluster. The master node also controls the worker node.
- The worker nodes run the containerized applications.

Kubernetes cluster on two-node device

The Kubernetes cluster on the 2-node device has one master node and two worker nodes. The 2-node device is highly available, and if one of the nodes fails, both the device and the Kubernetes cluster keep running. For more information on the Kubernetes cluster architecture, go to [Kubernetes core concepts](#).

On a 2-node Azure Stack Edge device, the Kubernetes master VM and a Kubernetes worker VM are running on node A of your device. On the node B, a single Kubernetes worker VM is running.

Each worker VM in the Kubernetes cluster is a pinned Hyper-V VM. A pinned VM is tied to the specific node it is running on. If the node A on the device fails, the master VM fails over to node B. But the worker VM on node A which is a pinned VM does not fail over to node B and vice-versa. Instead, the pods from the worker VM on node A are rebalanced onto node B.

In order for the rebalanced pods to have enough capacity to run on the device node B, the system enforces that no more than 50% of each ASE node's capacity be used during regular 2-node Azure Stack Edge cluster operations. This capacity usage is done on a best effort basis and there are circumstances (for example, workloads requiring unavailable GPU resources when they are rebalanced to ASE Node B) in which rebalanced pods may not have sufficient resources to run.

These scenarios are covered in detail in the next section on [Failure Modes and Behavior](#).

Failure modes and behavior

The Azure Stack Edge device nodes may fail under certain conditions. The various failure modes and the corresponding device responses are tabulated in this section.

Azure Stack Edge node failures or reboots

NODE	FAILURES	RESPONSES
Node A has failures (Node B has no failures)	<p>Following possible failures can occur:</p> <ul style="list-style-type: none"> • Both PSUs fail • One or both Port 3, Port 4 fail • Core component fails, includes motherboard, DIMM, OS disk • Entire node fails 	<p>Following responses are seen for each of these failures:</p> <ul style="list-style-type: none"> • Kubernetes master VM fails over from node A to node B • Master VM takes few minutes to come up on node B • Pods from node A are rebalanced on node B • GPU workloads keep running if GPU is available on node B
Node A reboots (Node B has no failures)	Node reboots	After node A completes rebooting and the worker VM is available, master VM will rebalance the pods from node B.
Node B has failures (Node A has no failures)	<p>Following possible failures can occur:</p> <ul style="list-style-type: none"> • Both PSUs fail • One or both Port 3, Port 4 fail • Core component fails, includes motherboard, DIMM, OS disk • Entire node fails 	<p>Following responses are seen for each of these failures:</p> <ul style="list-style-type: none"> • Kubernetes master VM rebalances pods from node B. This could take a few minutes.
Node B reboots (Node A has no failures)	Node reboots	After node B completes rebooting and the worker VM is available, master VM will rebalance the pods from node B.

Azure Stack Edge node updates

UPDATE TYPE	RESPONSES
Device node update	Rolling updates are applied to device nodes and the nodes will reboot.
Kubernetes service update	<p>Kubernetes service update includes:</p> <ul style="list-style-type: none"> • A failover of the Kubernetes master VM from device node A to device node B • A Kubernetes master update. • Kubernetes worker node updates (not necessarily in that order). <p>The entire update process could take 30 minutes or more, and during this window the Kubernetes cluster is available for any management operations (like deploying a new workload). Although pods will be drained from the device node while it is being updated, workloads may be offline for several seconds during this process.</p>

Next steps

- Learn more about Kubernetes storage on [Azure Stack Edge device](#).
- Understand the Kubernetes networking model on [Azure Stack Edge device](#).
- Deploy [Azure Stack Edge](#) in Azure portal.

Tutorial: Rack the Azure Stack Edge Pro 2 using a two-post mount

9/21/2022 • 2 minutes to read • [Edit Online](#)

Azure Stack Edge Pro 2 is the next generation of an AI-enabled edge computing device that can transfer data over the network. This device is a part of the Hardware-as-a-service solution offered by Microsoft.

The device must be installed on a standard 19-inch rack. Use the following procedure to rack mount your device on a standard 19-inch rack using a two-post mount.

Prerequisites

- Before you begin, read the safety instructions in your Safety, Environmental, and Regulatory Information booklet. This booklet was shipped with the device.
- Begin installing the rails in the allotted space that is closest to the bottom of the rack enclosure.
- For the rack mounting configuration, you need to supply:
 - A Phillips-head screwdriver

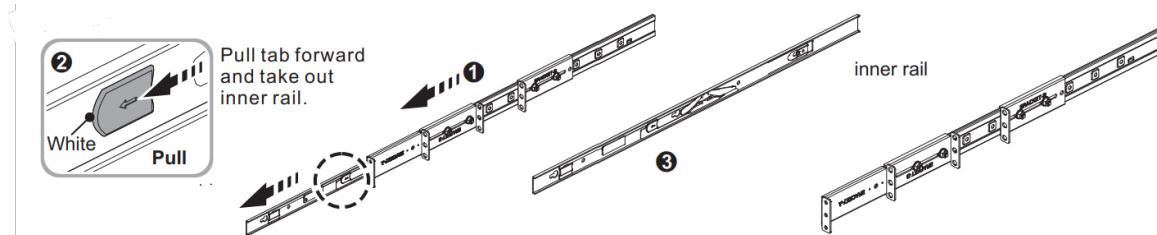
Identify the rail kit contents

- Inner rail
- Chassis
- The following screws and nuts:

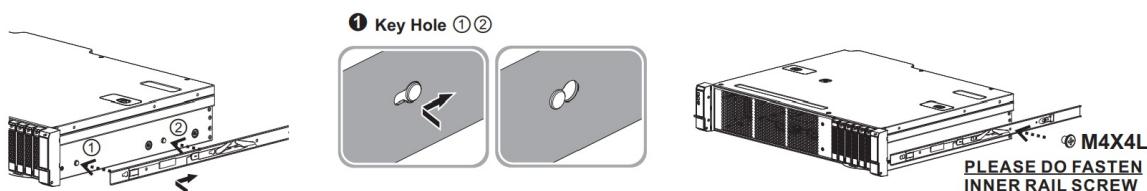
RACK TYPE	SCREWS	NUTS
Square hole	● M6X13 (8)	● M6 (8)
Round hole	● M5X13 (8)	● M5 (8)

Install and remove rails

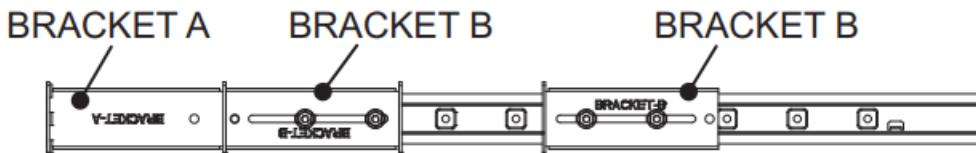
- Remove the inner rail. Pull the tab forward and take out the inner rail.



- Install the inner rail onto the chassis. Make sure to fasten the inner rail screw.

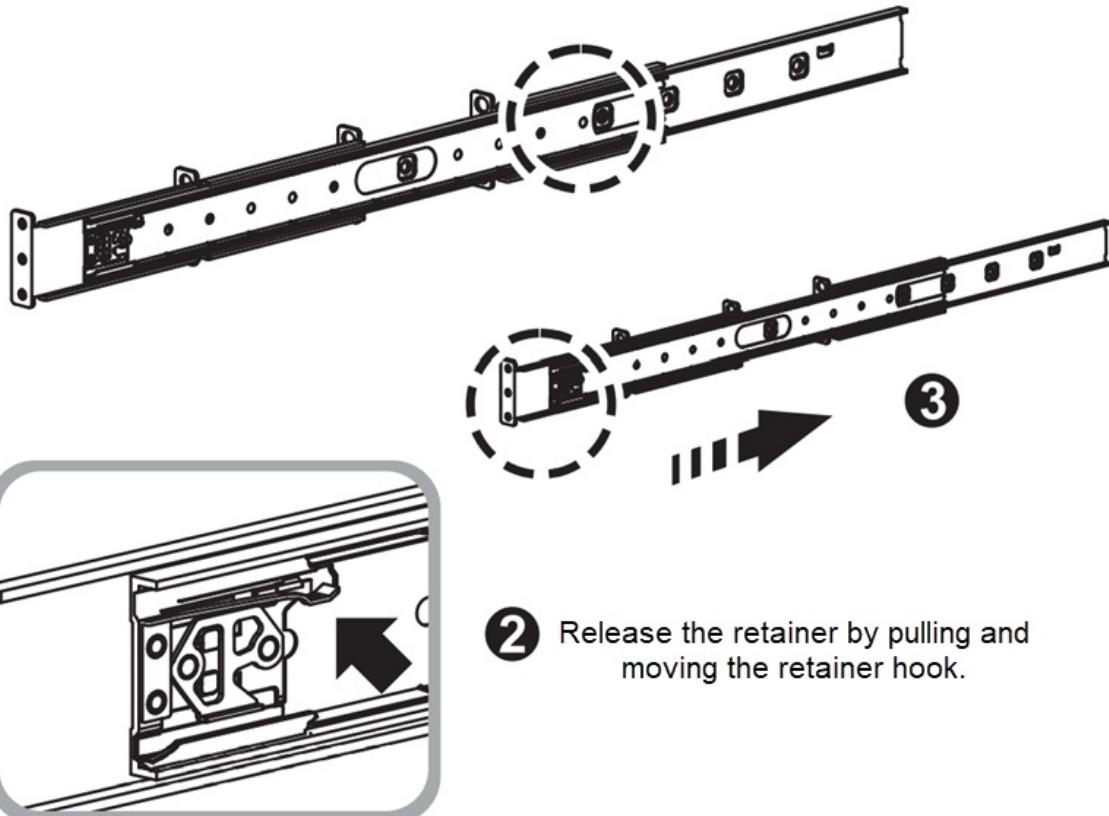


3. Identify Bracket B:



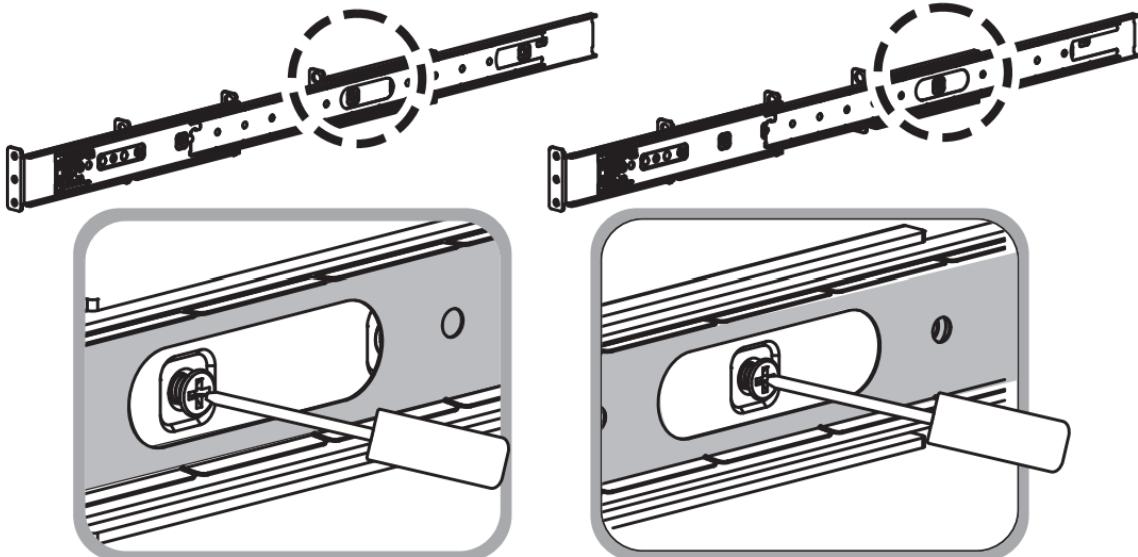
Adjust the fastening position of Bracket B. Release the retainer by pulling and moving the retainer hook.

1 Adjust the fastening position of bracket B.

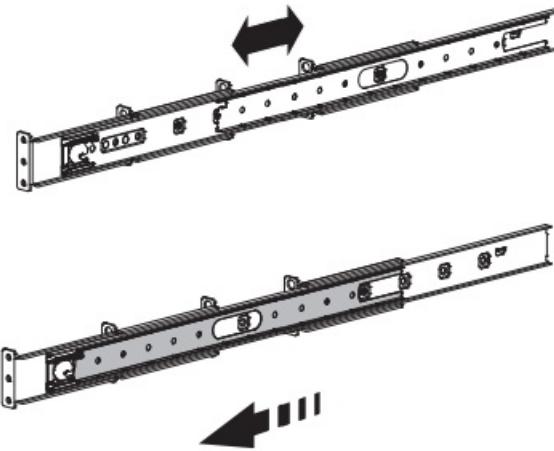


4. Moving the retainer, loosen the screw by the oval holes on the retainer (no need to detach the screw).

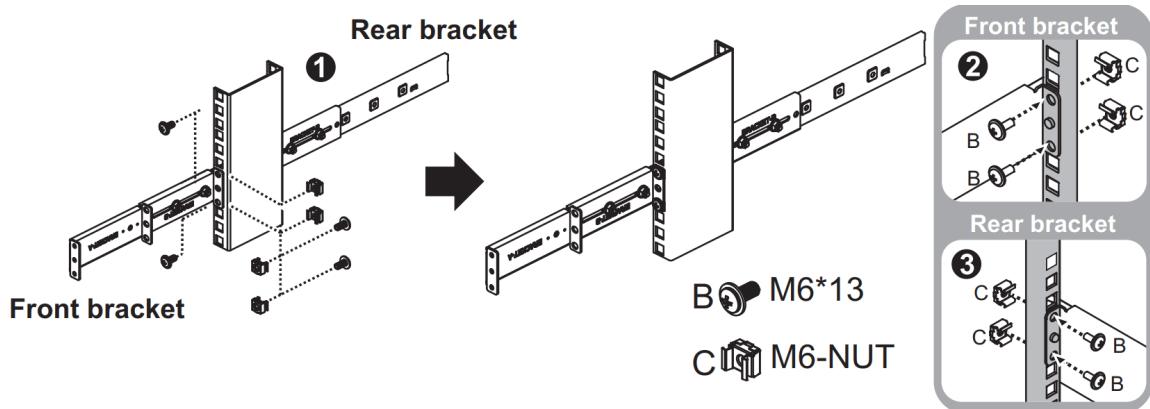
When fastening the rear bracket, use the oval hole on the retainer. Don't use other holes on the retainer.



5. Move Bracket B to the needed position and fasten the screw.

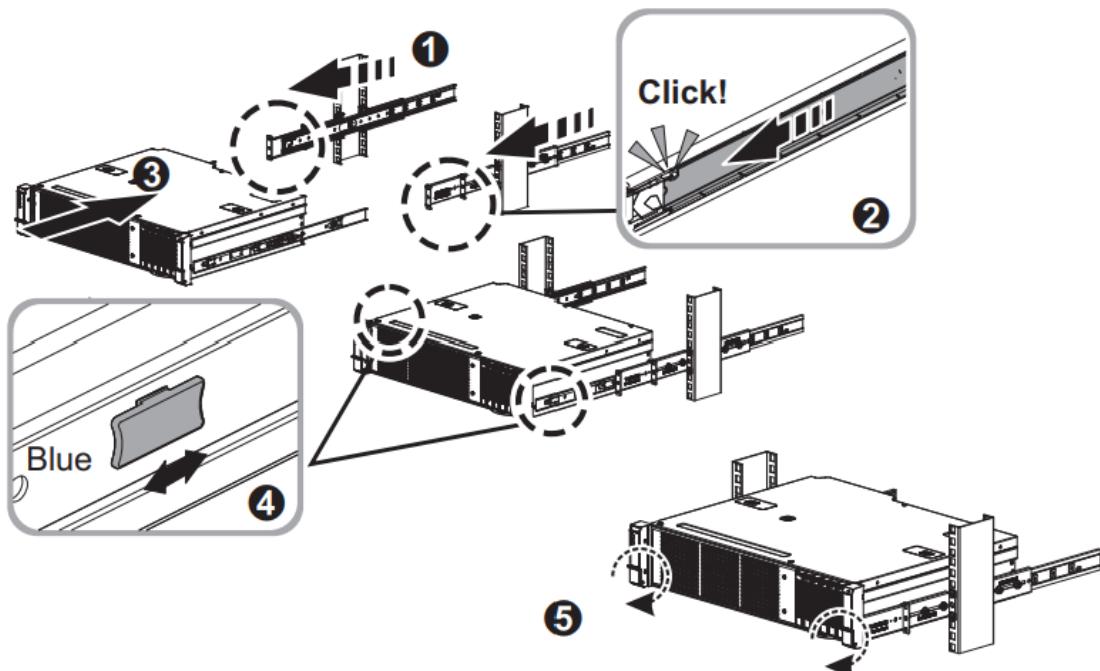


6. Move and hook the retainer back to the front.



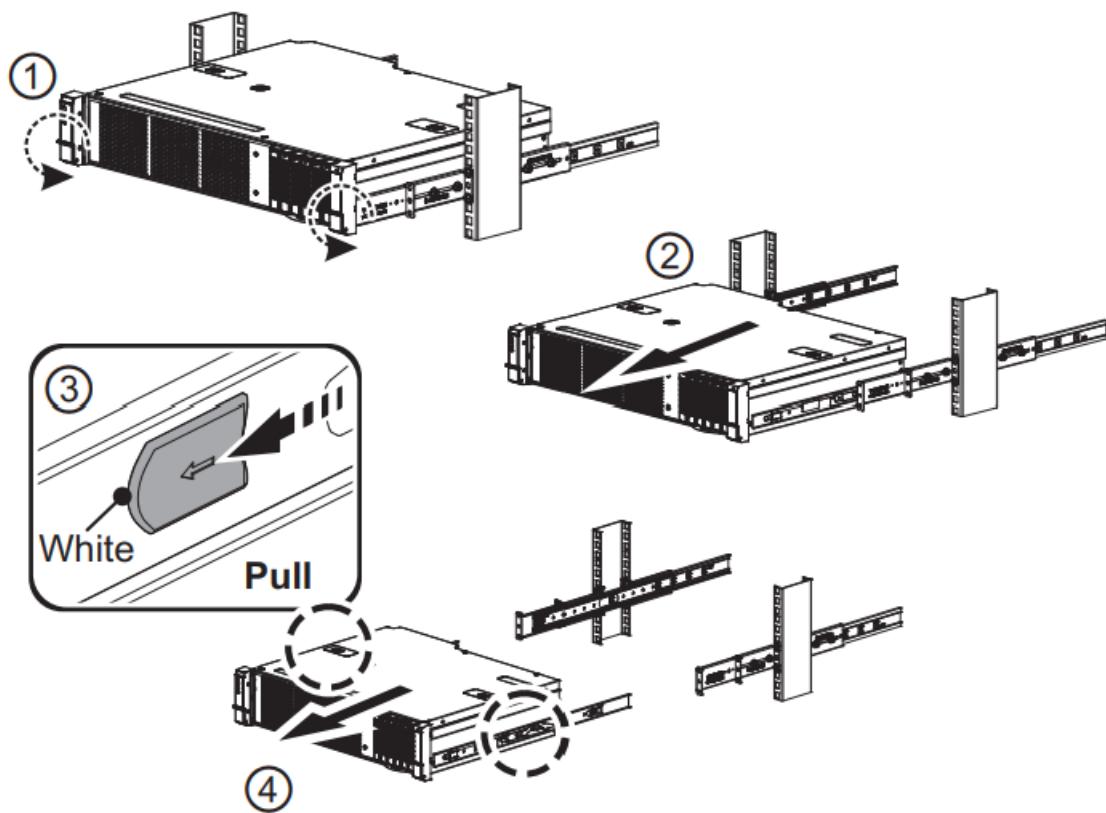
7. Insert the chassis to complete the installation.

- Ensure the ball bearing retainer is located at the front of the middle rail (reference diagram 1 and 2).
- Insert the chassis into the middle-outer rails (reference diagram 3).
- When you hit a stop, pull/push the blue release tab on the inner rails (reference diagram 4).
- Tighten the M5 screws of the chassis to the rail once the server is seated (reference diagram 5).



Remove the chassis

1. Loosen the M5 screws of the chassis.
2. Pull out the chassis.
3. Press the disconnect tab forward to remove the chassis.



Safety instructions for your Azure Stack Edge Pro 2

9/21/2022 • 12 minutes to read • [Edit Online](#)



To reduce the risk of bodily injury, electrical shock, fire, and equipment damage, read the following safety instructions and observe all warnings and precautions in this article before unpacking, installing, or maintaining this device.

Safety icon conventions

The signal words for hazard alerting signs are:

ICON	DESCRIPTION
	DANGER: Indicates a hazardous situation that, if not avoided, will result in death or serious injury.
	WARNING: Indicates a hazardous situation that, if not avoided, could result in death or serious injury.
	CAUTION: Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

Hazard symbols identified in the manual are:

ICON	DESCRIPTION
	Read all instructions first
	Indicates information considered important, but not hazard-related.
	Hazard symbol
	Tip hazard
	Overload tip hazard

ICON	DESCRIPTION
	Electric shock hazard
	No user serviceable parts. Do not access unless properly trained.
	Crush or pinching hazard
	Hot surface. Do not touch. Allow to cool before servicing.
	Moving parts hazard

Installation and handling precautions



DANGER:

- Before you begin to unpack the equipment, to prevent hazardous situations resulting in death, serious injury and/or property damage, read, and follow all warnings and instructions.
- Inspect the as-received equipment for damages. If the equipment enclosure is damaged, [contact Microsoft Support](#) to obtain a replacement. Don't attempt to operate the device.



CAUTION:

- If you suspect the device is malfunctioning, [contact Microsoft Support](#) to obtain a replacement. Don't attempt to service the equipment.
- Always wear the appropriate clothing to protect skin from sharp metal edges and avoid sliding any metal edges against skin. Always wear appropriate eye protection to avoid injury from objects that may become airborne.
- Laser peripherals or devices may be present. To avoid risk or radiation exposure and/or personal injury, don't open the enclosure of any laser peripheral or device. Laser peripherals or devices aren't serviceable. Only use certified and rated Laser Class I for optical transceiver products.



WARNING:

- When installing into an equipment rack, the rack must be anchored to an unmovable support to prevent it from tipping before the rack-mounted equipment is installed or extended from it. The equipment rack must be installed according to the rack manufacturer's instructions.
- When using an equipment rack, the rack may tip over causing serious personal injury. Verify the equipment rack is anchored to the floor and/or bayed to its adjacent equipment racks before installing, extending, or removing equipment. Failure to do so could allow the rack system to tip over leading to death, injury, or damage.

- When installed into an equipment rack, don't extend more than one equipment (for example, storage or server) from the rack at one time to prevent the equipment rack from becoming dangerously unstable.



WARNING:

- This equipment is not to be used as shelves or work spaces. Do not place objects on top of the equipment. Adding any type of load to a rack or wall mounted equipment can create a potential tip or crush hazard which could lead to injury, death, or product damage.



CAUTION:

- Parts enclosed within panels containing this symbol contain no user-serviceable parts. Hazardous voltage, current, and energy levels are present inside. Don't open. Return to manufacturer for servicing. Open a ticket with [Microsoft Support](#).
- The equipment contains coin cell batteries. There's a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.



CAUTION:

- If the equipment has been running, any installed component, processor(s), and heat sink(s) may be hot. Allow the equipment to cool before opening the cover to avoid the possibility of coming into contact with hot component(s). Ensure that you're wearing proper personal protective equipment (PPE) with suitable thermal insulation when hot-swapping any components.



CAUTION:

- CAUTION: Avoid wearing loose clothing items, jewelry, or loose long hair when working near an actively spinning fan.



WARNING:

- The system is designed to operate in a controlled environment. Choose a site that is:
 - Indoors, not exposed to moisture or rain.
 - Well ventilated and away from sources of heat including direct sunlight and radiators.
 - Located in a space that minimizes vibration and physical shock.
 - Isolated from strong electromagnetic fields produced by electrical devices.
 - Provided with properly grounded outlets.
 - Provided with sufficient space to access the power supply cord, because it serves as the product's main power disconnect.
- To reduce the risk of fire or electric shock, install the equipment/system in a temperature-controlled indoor area free of conductive contaminants. Don't place the equipment near liquids or in an excessively humid environment.
- Don't allow any liquid or any foreign object to enter the device. Don't place beverages or any other liquid containers on or near the device.



CAUTION:

- Elevated operating ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma} is 45°C) specified by the manufacturer.
- Reduced air flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment isn't compromised. Carefully route cables as directed to minimize airflow blockage and cooling problems.
- Don't use equipment if rails require excessive force when sliding the inner drawer assembly.



WARNING:

- This equipment has only been certified for use with mounting accessories provided with the equipment. The use of any other mounting device that hasn't been certified for use with this equipment may cause severe injuries.
- When provided with the equipment, carefully follow all instructions provided with the Wall Mount Equipment Bracket or the Slide Rail Kits. Failure to install these accessories properly can cause severe injuries.
- The two and four post Slide Rail Kits are only compatible with the rack specifications in Electronic Industries Association (EIA) standard EIA-310-D. Choosing a rack that doesn't comply with the EIA-310-D specifications can cause hazards that can lead to severe injuries.



CAUTION:

- Don't place fingers on the bearing tracks during slide rails installation (read slide rails installation instructions). Sliding of rails over bearings can pose a risk of pinching.

Electrical precautions



WARNING:

- Hazardous voltage, current, or energy levels are present inside this equipment and any component displaying this symbol: Don't service the equipment until all input power is removed, unless directed otherwise by the service instructions in an accompanying document for the component being serviced. To remove all input power, the equipment power cable must be disconnected from the AC electrical mains supply. Don't remove cover or barrier on any component that contains this label: Servicing should only be performed by qualified trained technicians.



WARNING:

- Don't install equipment into a rack or on a wall while they're energized with external cables.
- Ensure power cords aren't crushed or damaged during installation.
- Provide a safe electrical earth connection to the power supply cord. The AC cord has a three-wire grounding plug (a plug that has a grounding contact). This plug fits only a grounded AC outlet. Don't defeat the purpose of the grounding contact.
- Given that the plug on the power supply cord is the main disconnect device, ensure that the socket outlets are located near the equipment and are easily accessible.
- Unplug the power cord (by pulling the plug, not the cord) and disconnect all cables if any of the following conditions exist:
 - The power cord or plug becomes frayed or otherwise damaged
 - You spill something into the device casing

- The device is exposed to rain, excess moisture, or other liquids. The device has been dropped and the device casing is damaged
- You suspect the device needs service or repair
- Permanently unplug the unit before you move it or if you think it has become damaged in any way.
- Provide a suitable power source with electrical overload protection to meet the power specifications shown on the equipment rating label provided with the equipment.
- Don't attempt to modify or use AC power cord(s) other than the ones provided with the equipment.



WARNING:

- To reduce the risk of electrical shock, injury from moving parts, damage, or loss of data, always make sure to disconnect the equipment from the AC electrical source when working inside the equipment. Powering down the system doesn't ensure there's no electrical activity inside the equipment.

Electrostatic precautions

! NOTICE:

- Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD work-station. If one isn't available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground any unpainted metal surface on the equipment when handling parts.
- ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the equipment, place the board component side up on a grounded, static-free surface. Use a conductive foam pad if available but not the board wrapper. Don't slide board over any surface.
- Wear a grounded wrist strap. If none are available, discharge any personal static electricity by touching the bare metal chassis of the server, or the bare metal body of any other grounded device.
- Humid environments tend to have less static electricity than dry environments. A grounding strap is warranted whenever danger of static electricity exists.

! NOTICE:

- Leave all replacement components inside their static-proof packaging until you're ready to use them.

Regulatory information

Regulatory model numbers: DB040 and DB040-W

This equipment is designed for use with NRTL Listed (UL, CSA, ETL, etc.), and IEC/EN 60950-1 or IEC/EN 62368-1 compliant (CE marked) Information Technology equipment.

This equipment is designed to operate in the following environment:

- Temperature specifications
 - Storage: -40°C to 70°C (-40°F to 149°F)
 - Operating: 10°C to 45°C (50°F to 113°F)
- Relative humidity specifications
 - Storage: 5% to 95% relative humidity
 - Operating: 5% to 85% relative humidity
 - For models with GPU(s), derate allowable max operating temperature by 1°C/210m (2.6°F/1000ft) above 950m (3,117ft).
- Maximum altitude specifications

- Operating: 3,050 meters (10,000 feet)
- Storage: 9,150 meters (30,000 feet)

For electrical supply ratings, refer to the equipment rating label provided with the unit.

! NOTICE: Changes or modifications made to the equipment not expressly approved by Microsoft may void the user's authority to operate the equipment.

USA and Canada

Supplier's Declaration of Conformity

Models: DB040, DB040-W

! NOTICE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Tout changement ou modification non expressément approuvé par la partie responsable de la conformité pourrait annuler l'autorité de l'utilisateur d'utiliser cet équipement.

CAN ICES-3(A)/NMB-3(A)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA.

United States: (800) 426-9400

Canada: (800) 933-4750

For model: DB040-W only

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems. Users are advised that high-power radars are allocated as primary users (priority users) of the bands 5250–5350 MHz and 5650–5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux. Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Exposure to Radio Frequency (RF) Energy

This equipment should be installed and operated with a minimum distance of 20 cm (8 inches) between the radiator and your body. This transmitter must not be colocated or operating with any other antenna or transmitter.

This equipment complies with FCC/ISED radiation exposure limits set forth for an uncontrolled environment. Additional information about radiofrequency safety can be found on the FCC website at <https://www.fcc.gov/general/radio-frequency-safety-0> and the Industry Canada website at <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01904.html>

Detachable antenna usage This radio transmitter [IC: 7542A-MT7921] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 7542A-MT7921] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Brand	Model	Antenna Type	Connector	Max Gain (dBi)		Impedance (Ω)
				2.4GHz	5GHz	
Foxconn	ANEP2M1-CZZ02-EH	Dipole	R-SMA	3.0	4.0	50
Inpaq	DAM-D2-H-N0-000-04-02	Dipole	R-SMA	3.5	4.5	50

European Union



WARNING:

- This device is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



For Model: DB040-W only

Hereby, declares that this device is in compliance with EU Directive 2014/53/EU and UK Radio Equipment Regulations 2017 (S.I. 2017/1206). The full text of the EU and UK declaration of conformity are available on the [product webpage](#).

This device may operate in all member states of the EU. Observe national and local regulations where the device is used. This device is restricted to indoor use only when operating in the 5150 - 5350 MHz frequency range in the following countries:

	AT	BE	BG	CH	CY	CZ	DE
	DK	EE	EL	ES	FI	FR	HR
	HU	IE	IS	IT	LI	LT	LU
	LV	MT	NL	NO	PL	PT	RO
	SE	SI	SK	TR	UK(NI)		

In accordance with Article 10.8(a) and 10.8(b) of the Radio Equipment Directive (RED), the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

FREQUENCY BAND (MHZ)	MAXIMUM EIRP (DBM)
2400 - 2483.5	19.74
5150 - 5350	22.56
5470 - 5725	19.68
5725 - 5875	13.83

Notice: This device is a receiver category 1 device under EN 300 440

Disposal of waste batteries and waste electrical and electronic equipment



This symbol on the product, its batteries, or its packaging means that this product and any batteries it contains must not be disposed of with your household waste. It is your responsibility to hand this product over to an applicable collection point for the recycling of batteries and electrical and electronic equipment. This separate collection and recycling will help to conserve natural resources and prevent potential negative consequences for human health and the environment due to the possible presence of hazardous substances in batteries and electrical and electronic equipment, which could be caused by inappropriate disposal. For more information about where to drop off your batteries and waste electrical and electronic equipment (WEEE), contact your local city/municipality office, your household waste disposal service, or the shop where you purchased this product. Contact erecycle@microsoft.com for additional information on WEEE.

This product might contain Lithium-Ion and/or Lithium Metal battery(ies).

Microsoft Ireland Sandyford Ind Est Dublin D18 KX32 IRL

Telephone number: +353 1 295 3826

Fax number: +353 1 706 4110

Japan

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Declarations of conformity

A Declaration of Conformity (DoC) is a document stating that a product meets the legal standards to which it must adhere, such as safety regulations. Here is the declaration of conformity for EU:



EU Declaration of Conformity

We, Microsoft Corporation, declare under our sole responsibility that **Server** model number **DB040-W** is in conformity with the essential requirements and other relevant requirements of the following directive(s) of the European Parliament and European Council:

- *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC*
- *Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment*
- *Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products*

The following harmonized standards and technical specifications have been applied:

- **EN 63000:2018**, Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances
- **EN 300 328 V2.2.2**, Wideband Transmission Systems - Data transmission equipment operating in the 2.4GHz ISM band and using wide band modulation techniques
- **EN 301 893 V2.1.1**, 5 GHz RLAN
- **EN 300 440 V2.1.1**, Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range
- **EN 301 489-1 v.2.2.3**, EMC standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 v.3.2.4**, EMC Standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems
- **EN 62311: 2008**, Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
- **EN 55032:2015/A11:2020**, Electromagnetic compatibility of multimedia equipment, Emission requirements, Class A
- **EN 61000-3-2:2014**, Electromagnetic compatibility (EMC), Part 3-2: Limits, Limits for harmonic current emissions
- **EN 61000-3-3:2013**, Electromagnetic compatibility (EMC), Part 3-3: Limits, Limitation of voltage changes, voltage fluctuations and flicker in public low- voltage supply systems
- **EN 55035:2017/A11:2020**, Information technology equipment, Immunity characteristics, Limits and methods of measurement
- **EN 62368-1:2014/AC:2015**, Audio/video, information and communication technology equipment - Part 1: Safety requirements
- **Commission Regulation (EU) No 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013**

Manufacturer: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States

A handwritten signature in black ink.

Michele Falcon, Director, HW Engineering

February 21, 2022

DoC #: DB040-W_20220221_EU

Here is the declaration of conformity for UK:



UK Declaration of Conformity

We, Microsoft Corporation, declare under our sole responsibility that **Server** model number **DB040-W**, is in conformity with the following essential and relevant UK statutory requirements:

- The Radio Equipment Regulations 2017 (S.I. 2017/1206), as amended by the applicable 'EU Exit' legislation
- The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (UK S.I. 2012/3032) and amendments
- The Ecodesign for Energy-Related Products and Energy Information (S.I. 2010/2617), as amended by the applicable 'EU Exit' legislation

The following relevant designated standards and technical specifications have been applied in relation to which conformity is declared:

- **BS EN 55032:2015/A11:2020**, Electromagnetic compatibility of multimedia equipment, Emission requirements, Class A
- **EN 300 328 V2.2.2**, Wideband Transmission Systems - Data transmission equipment operating in the 2.4GHz ISM band and using wide band modulation techniques
- **EN 301 893 V2.1.1**, 5 GHz RLAN
- **EN 300 440 V2.1.1**, Short Range Devices (SRD); Radio equipment to be used in the 1 GHz to 40 GHz frequency range
- **EN 301 489-1 v.2.2.3**, EMC standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 v.3.2.4**, EMC Standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems
- **EN 62311:2008**, Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
- **BS EN 61000-3-2:2014**, Electromagnetic compatibility (EMC), Part 3-2: Limits, Limits for harmonic current emissions
- **BS EN 61000-3-3:2013**, Electromagnetic compatibility (EMC), Part 3-3: Limits, Limitation of voltage changes, voltage fluctuations and flicker in public low- voltage supply systems
- **BS EN 55035:2017/A11:2020**, Information technology equipment, Immunity characteristics, Limits and methods of measurement
- **BS EN 62368-1:2014/AC:2015**, Audio/video, information and communication technology equipment - Part 1: Safety requirements
- **Commission Regulation (EU) No 2019/424** of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013
- **BS EN IEC 63000:2018**, Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances

Manufacturer: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States

A handwritten signature in black ink.

Michele Falcon, Director, HW Engineering

February 8, 2022

DoC #: DB040-W_20220208_UK

Next steps

- Prepare to deploy Azure Stack Edge Pro 2 device

What is Azure Stack Edge Pro with GPU?

9/21/2022 • 6 minutes to read • [Edit Online](#)

Azure Stack Edge Pro with GPU is an AI-enabled edge computing device with network data transfer capabilities.

This article provides you an overview of the Azure Stack Edge Pro solution, benefits, key capabilities, and scenarios where you can deploy this device. The article also explains the pricing model for your device.

Azure Stack Edge Pro with GPU is a Hardware-as-a-Service solution. Microsoft ships you a cloud-managed device that acts as a network storage gateway. A built-in Graphical Processing Unit (GPU) enables accelerated AI-inferencing.

Use cases

Here are the various scenarios where Azure Stack Edge Pro GPU can be used for rapid Machine Learning (ML) inferencing at the edge and preprocessing data before sending it to Azure.

- **Inference with Azure Machine Learning** - With Azure Stack Edge Pro GPU, you can run ML models to get quick results that can be acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models. For more information, see how to use [Deploy Azure ML hardware accelerated models on Azure Stack Edge Pro GPU](#).
- **Preprocess data** - Transform data before sending it to Azure via compute options such as containerized workloads and Virtual Machines to create a more actionable dataset. Preprocessing can be used to:
 - Aggregate data.
 - Modify data, for example to remove personal data.
 - Subset data to optimize storage and bandwidth, or for further analysis.
 - Analyze and react to IoT Events.
- **Transfer data over network to Azure** - Use Azure Stack Edge Pro GPU to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

Key capabilities

Azure Stack Edge Pro GPU has the following capabilities:

CAPABILITY	DESCRIPTION
Accelerated AI inferencing	Enabled by the built-in GPU (one or two depending on the model). For more information, see GPU sharing on your Azure Stack Edge device .
Edge computing	Supports VM and containerized workloads to allow analysis, processing, and filtering of data. <ul style="list-style-type: none">● For information on VM workloads, see VM overview on Azure Stack Edge.● For containerized workloads, see Kubernetes overview on Azure Stack Edge

CAPABILITY	DESCRIPTION
Data access	Direct data access from Azure Storage Blobs and Azure Files using cloud APIs for additional data processing in the cloud. Local cache on the device is used for fast access of most recently used files.
Cloud-managed	Device and service are managed via the Azure portal.
Offline upload	Disconnected mode supports offline upload scenarios.
Supported file transfer protocols	Support for standard Server Message Block (SMB), Network File System (NFS), and Representational State Transfer (REST) protocols for data ingestion. For more information on supported versions, see Azure Stack Edge Pro GPU system requirements .
Data refresh	Ability to refresh local files with the latest from cloud. For more information, see Refresh a share on your Azure Stack Edge .
Encryption	BitLocker support to locally encrypt data and secure data transfer to cloud over <i>https</i> .
Bandwidth throttling	Throttle to limit bandwidth usage during peak hours. For more information, see Manage bandwidth schedules on your Azure Stack Edge .
Easy ordering	Bulk ordering and tracking of the device via Azure Edge Hardware Center (Preview). For more information, see Order a device via Azure Edge Hardware Center .
Scale out	Devices can be deployed as a single node or a two-node cluster. For more information, see What is clustering on Azure Stack Edge? .
Specialized network functions	Use the Marketplace experience from Azure Network Function Manager to rapidly deploy network functions such as mobile packet core, SD-WAN edge, and VPN services to an Azure Stack Edge device running in your on-premises environment. For more information, see What is Azure Network Function Manager? (Preview) .

Components

The Azure Stack Edge Pro GPU solution includes the Azure Stack Edge resource, Azure Stack Edge Pro GPU physical device, and a local web UI.

- **Azure Stack Edge Pro GPU physical device** - A 1U rack-mounted server supplied by Microsoft that can be configured to send data to Azure.

To procure a device, go to the Azure Edge Hardware Center and place an order. Azure Edge Hardware Center service lets you choose from a variety of Azure Stack Edge SKUs as per your business need. You can order multiple units of a device type, ship multiple devices to different locations, save addresses for future orders, and also track the status of your orders.

Once the order is delivered, you can configure your device and create an Azure Stack Edge resource to manage the device.

For more information, go to [Create an order for your Azure Stack Edge Pro GPU device](#).

The devices can be deployed as a single node or a two-node cluster. For more information, see [What is clustering for Azure Stack Edge?](#) and how to [Deploy a two-node cluster](#).

- **Azure Stack Edge resource** – A resource in the Azure portal that lets you manage an Azure Stack Edge Pro GPU device from a web interface that you can access from different geographical locations. Use the Azure Stack Edge resource to create and manage resources, view, and manage devices and alerts, and manage shares.
- **Azure Stack Edge Pro GPU local web UI** - A browser-based local user interface on your Azure Stack Edge Pro GPU device primarily intended for the initial configuration of the device. Use the local web UI also to run diagnostics, shut down and restart the Azure Stack Edge Pro GPU device, view copy logs, and contact Microsoft Support to file a service request.

The local web UI on the device currently supports the following languages with their corresponding language codes:

LANGUAGE	CODE	LANGUAGE	CODE	LANGUAGE	CODE
English {default}	en	Czech	cs	German	de
Spanish	es	French	fr	Hungarian	hu
Italian	it	Japanese	ja	Korean	ko
Dutch	nl	Polish	pl	Portuguese - Brazil	pt-br
Portuguese - Portugal	pt-pt	Russian	ru	Swedish	sv
Turkish	tr	Chinese - simplified	zh-hans	Chinese - traditional	zh-hant

For information about using the web-based UI, go to [Use the web-based UI to administer your Azure Stack Edge Pro GPU](#).

Region availability

Azure Stack Edge Pro GPU physical device, Azure resource, and target storage account to which you transfer data don't all have to be in the same region.

- **Resource availability** - For this release, the resource is available in East US, West EU, and South East Asia regions.
- **Device availability** - For a list of all the countries/regions where the Azure Stack Edge Pro GPU device is available, go to **Availability** section in the **Azure Stack Edge Pro** tab for [Azure Stack Edge Pro GPU pricing](#).
- **Destination Storage accounts** - The storage accounts that store the data are available in all Azure regions. For best performance, the regions where the storage accounts store Azure Stack Edge Pro GPU data should be close to the device location. A storage account located far from the device results in long latencies and slower performance.

Azure Stack Edge service is a non-regional service. For more information, see [Regions and Availability Zones in Azure](#). Azure Stack Edge service doesn't have dependency on a specific Azure region, making it resilient to zone-wide outages and region-wide outages.

For a discussion of considerations for choosing a region for the Azure Stack Edge service, device, and data storage, see [Choosing a region for Azure Stack Edge](#).

Billing model

The users are charged a monthly, recurring subscription fee for an Azure Stack Edge device. In addition, there's a onetime fee for shipping. There's no on-premises software license for the device although guest virtual machine (VMs) may require their own licenses under Bring Your Own License (BYOL).

Currency conversion and discounts are handled centrally by the Azure Commerce billing platform, and you get one unified, itemized bill at the end of each month.

Billing starts 14 days after a device is marked as **Shipped** and ends when you initiate return of your device.

The billing happens against the order resource. If you activate the device against a different resource, the order and billing details move to the new resource.

For more information, see [FAQ: Billing for Azure Stack Edge Pro GPU](#).

Next steps

- Review the [Azure Stack Edge Pro GPU system requirements](#).
- Understand the [Azure Stack Edge Pro GPU limits](#).
- Deploy [Azure Stack Edge Pro GPU](#) in Azure portal.

Quickstart: Get started with Azure Stack Edge Pro with GPU

9/21/2022 • 4 minutes to read • [Edit Online](#)

This quickstart details the prerequisites and the steps required to deploy your Azure Stack Edge Pro GPU device. The quickstart steps are performed in the Azure portal and on the local web UI of the device.

The total procedure should approximately take 1.5 hours to complete. For detailed step-by-step instructions, go to [Tutorial: Prepare to deploy Azure Stack Edge Pro GPU](#).

Prerequisites

Before you deploy, make sure that following prerequisites are in place:

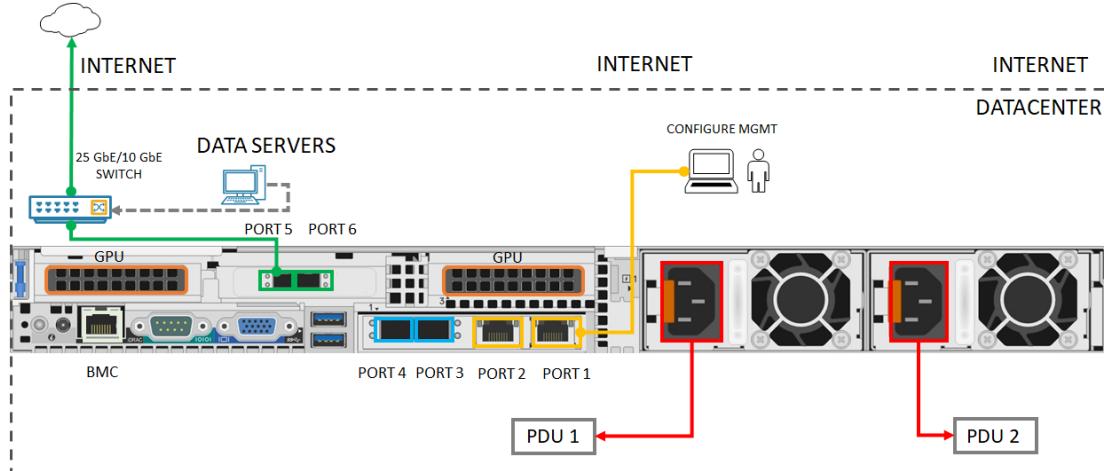
1. The Azure Stack Edge Pro GPU device is delivered to your site, [unpacked](#) and [rack mounted](#).
2. Configure your network such that your device can reach the [listed URL patterns and ports](#).
3. You have owner or contributor access to Azure subscription.
4. In the Azure portal, go to **Home > Subscriptions > Your-subscription > Resource providers**. Search for `Microsoft.DataBoxEdge` and register the resource provider. Repeat to register `Microsoft.Devices` if you'll create an IoT Hub resource to deploy compute workloads.
5. Make sure you have a minimum of 2 free, static, contiguous IPs for Kubernetes nodes and at least 1 static IP for IoT Edge service. For each module or external service that you deploy, you'll need 1 more IP.
6. See the [deployment checklist](#) to get everything you'll need for device configuration.

Deployment steps

1. **Install:** Connect PORT 1 to a client computer via an Ethernet crossover cable or USB Ethernet adapter. Connect at least one other device port for data, preferably 25 GbE, (from PORT 3 to PORT 6) to Internet via SFP+ copper cables or use PORT 2 with RJ45 patch cable. Connect the provided power cords to the Power Supply Units and to separate power distribution outlets. Press the power button on the front panel to turn on the device.

See [Cavium FastlinQ 41000 Series Interoperability Matrix](#) and [Mellanox dual port 25G ConnectX-4 channel network adapter compatible products](#) to get compatible network cables and switches.

Here is the minimum cabling configuration needed to deploy your device:



2. **Connect:** Configure the IPv4 settings on the Ethernet adapter on your computer with a static IP address of 192.168.100.5 and subnet 255.255.255.0. Open your browser, and connect to the local web UI of device at <https://192.168.100.10>. This may take a few minutes. Continue to the webpage when you see the security certificate warning.
3. **Sign in:** Sign into the device with default password *Password1*. Change the device administrator password. The password must contain between 8 to 16 characters, and 3 of the uppercase, lowercase, numeric, and special characters.
4. **Configure network:** Accept the default DHCP configuration for connected data port if you have a DHCP server in your network. If not, provide an IP, DNS server, and default gateway. See more information on [Network settings](#).
5. **Configure compute network:** Create a virtual switch by enabling a port on your device. Enter 2 free, contiguous static IPs for Kubernetes nodes in the same network that you created the switch. Provide at least 1 static IP for IoT Edge Hub service to access compute modules and 1 static IP for each extra service or container that you want to access from outside the Kubernetes cluster.

Kubernetes is required to deploy all containerized workloads. See more information on [Compute network settings](#).
6. **Configure web proxy:** If you use web proxy in your environment, enter web proxy server IP in `http://<web-proxy-server-FQDN>:<port-id>`. Set authentication to **None**. See more information on [Web proxy settings](#).
7. **Configure device:** Enter a device name and DNS domain or accept defaults.
8. **Configure Update server:** Accept the default Microsoft Update server or specify a Windows Server Update Services (WSUS) server and the path to the server.
9. **Configure time settings:** Accept the default time settings or set time zone, primary NTP server, and secondary NTP server on local network or as public servers.
10. **Configure certificates:** If you changed device name and/or DNS domain, then you must generate certificates or add certificates to activate the device.
 - To test non-production workloads, use [Generate certificates option](#).
 - If you bring your own certificates including the signing chain(s), [Add certificates](#) in appropriate format. Make sure to upload the signing chain first. See [Create certificates](#) and [Upload certificates via the local UI](#).
11. **Activate:** To get the activation key
 - a. In the Azure portal, go to your **Azure Stack Edge resource > Overview > Device setup > Activate > Generate key**. Copy the key.
 - b. In the local web UI, go to **Get started > Activate** and provide the activation key. When the key is applied, the device takes a few minutes for activation. Download the `<device-serial-number>.json` file when prompted to safely store device keys needed for a future recovery.
12. **Configure compute:** In the Azure portal, go to **Overview > Device**. Verify that the device is **Online**. In the left-pane, go to **Edge compute > Get started > Configure Edge compute > Compute**. Provide an existing or new IoT Hub service and wait for about 20 minutes for the compute to configure. See more information on [Tutorial: Configure compute on Azure Stack Edge Pro GPU device](#)

You are ready to deploy compute workloads on your device [via IoT Edge via kubectl](#) or [via Azure Arc-enabled Kubernetes!](#) If you experience any issues during the setup, see troubleshooting for [Azure Stack Edge Pro GPU devices](#), [certificate issues](#), or [IoT Edge issues](#).

Next steps

[Install Azure Stack Edge Pro GPU](#)

Deployment checklist for your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

This article describes the information that can be gathered ahead of the actual deployment of your Azure Stack Edge Pro GPU device.

Use the following checklist to ensure you have this information after you've placed an order for an Azure Stack Edge Pro device and before you've received the device.

Deployment checklist

STAGE	PARAMETER	DETAILS
Device management	<ul style="list-style-type: none">Azure subscriptionResource providers registeredAzure Storage account	<ul style="list-style-type: none">Enabled for Azure Stack Edge, owner or contributor access.In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for <code>Microsoft.EdgeOrder</code> and register. Repeat for <code>Microsoft.Devices</code> if deploying IoT workloads.Need access credentials.
Device installation	Power cables in the package. For US, an SVE 18/3 cable rated for 125 V and 15 Amps with a NEMA 5-15P to C13 (input to output) connector is shipped.	For more information, see the list of Supported power cords by country .
	<ul style="list-style-type: none">At least one 1-GbE RJ-45 network cable for Port 1At least one 25/10-GbE SFP+ copper cable for Port 3, Port 4, Port 5, or Port 6	Customer needs to procure these cables. For a full list of supported network cables, switches, and transceivers for device network cards from Cavium, see Cavium FastlinQ 41000 Series Interoperability Matrix . For a full list of supported cables and modules for 25 GbE and 10 GbE from Mellanox, see Mellanox dual port 25G ConnectX-4 channel network adapter compatible products .
Network readiness	Check to see how ready your network is for the deployment of an Azure Stack Edge device.	Use the Azure Stack Network Readiness Checker to test all needed connections.
First-time device connection	Laptop whose IPv4 settings can be changed.	If connecting Port 1 directly to a laptop (without a switch), use an Ethernet crossover cable or a USB to Ethernet adaptor.

Stage	Parameter	Details
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.
Network settings	<p>Device comes with 2 x 1-GbE, 4 x 25-GbE network ports.</p> <ul style="list-style-type: none"> Port 1 is used for initial configuration only. One or more data ports can be connected and configured. At least one data network interface from among Port 2 - Port 6 needs to be connected to the Internet (with connectivity to Azure). DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.
Advanced networking settings	<ul style="list-style-type: none"> Require 2 free, static, contiguous IPs for Kubernetes nodes, and one static IP for IoT Edge service. Require one additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	<ul style="list-style-type: none"> Web proxy server IP/FQDN, port Web proxy username, password 	
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	Configure primary and secondary NTP server on local network. If local server isn't available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public Windows update server is used.
Device settings	<ul style="list-style-type: none"> Device fully qualified domain name (FQDN) DNS domain 	

Stage	Parameter	Details
(Optional) Certificates	To test non-production workloads, use Generate certificates option . If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.	Configure certificates only if you change the device name and/or DNS domain.
Activation	Require activation key from the Azure Stack Edge resource.	Once generated, the key expires in three days.
Stage	Parameter	Details
Device management	<ul style="list-style-type: none"> Azure subscription Resource providers registered Azure Storage account 	<ul style="list-style-type: none"> Enabled for Azure Stack Edge, owner or contributor access. In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for <code>Microsoft.EdgeOrder</code> and register. Repeat for <code>Microsoft.Devices</code> if deploying IoT workloads. Need access credentials.
Device installation	Four power cables for the two device nodes in the package. For US, an SVE 18/3 cable rated for 125 V and 15 Amps with a NEMA 5-15P to C13 (input to output) connector is shipped.	For more information, see the list of Supported power cords by country .
	<ul style="list-style-type: none"> At least two 1-GbE RJ-45 network cables for Port 1 on the two device nodes You would need two 1-GbE RJ-45 network cables to connect Port 2 on each device node to the internet. Depending on the network topology you wish to deploy, you also need SFP+ copper cables to connect Port 3 and Port 4 across the device nodes and also from device nodes to the switches. See the Supported network topologies. 	Customer needs to procure these cables. For a full list of supported network cables, switches, and transceivers for device network cards from Cavium, see Cavium FastLinQ 41000 Series Interoperability Matrix . For a full list of supported cables and modules for 25 GbE and 10 GbE from Mellanox, see Mellanox dual port 25G ConnectX-4 channel network adapter compatible products .
First-time device connection	Laptop whose IPv4 settings can be changed.	This laptop connects to Port 1 via a switch or a USB to Ethernet adaptor.
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.

Stage	Parameter	Details
Network settings	<p>Each device node has 2 x 1-GbE, 4 x 25-GbE network ports.</p> <ul style="list-style-type: none"> Port 1 is used for initial configuration only. Port 2 must be connected to the Internet (with connectivity to Azure). Port 3 and Port 4 must be configured and connected across the two device nodes in accordance with the network topology you intend to deploy. You can choose from one of the three Supported network topologies. DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.
Advanced networking settings	<ul style="list-style-type: none"> Require 2 free, static, contiguous IPs for Kubernetes nodes, and one static IP for IoT Edge service. Require one additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	<ul style="list-style-type: none"> Web proxy server IP/FQDN, port. Web proxy username, password 	
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	Configure primary and secondary NTP server on local network. If local server isn't available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public Windows update server is used.
Device settings	<ul style="list-style-type: none"> Device fully qualified domain name (FQDN) DNS domain 	
(Optional) Certificates	<p>To test non-production workloads, use Generate certificates option.</p> <p>If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.</p>	Configure certificates only if you change the device name and/or DNS domain.

STAGE	PARAMETER	DETAILS
Activation	Require activation key from the Azure Stack Edge resource.	Once generated, the key expires in three days.

Next steps

- Prepare to deploy your [Azure Stack Edge Pro device](#).
- Use the [Azure Stack Edge Network Readiness Tool](#) to verify your network settings.

Tutorial: Prepare to deploy Azure Stack Edge Pro GPU

9/21/2022 • 12 minutes to read • [Edit Online](#)

This tutorial is the first in the series of deployment tutorials that are required to completely deploy Azure Stack Edge Pro GPU. This tutorial describes how to prepare the Azure portal to deploy an Azure Stack Edge resource.

You need administrator privileges to complete the setup and configuration process. The portal preparation takes less than 10 minutes.

In this tutorial, you learn how to:

- Create a new resource
- Get the activation key

Get started

For Azure Stack Edge Pro GPU deployment, you need to first prepare your environment. After the environment is ready, follow the required steps and if needed, optional steps and procedures to fully deploy the device. The step-by-step deployment instructions indicate when you should perform each of these required and optional steps.

STEP	DESCRIPTION
Preparation	These steps must be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information before and during the deployment.
Deployment prerequisites	These prerequisites validate that the environment is ready for deployment.
Deployment tutorials	These tutorials are required to deploy your Azure Stack Edge Pro GPU device in production.
1. Prepare the Azure portal for Azure Stack Edge Pro GPU	Create and configure your Azure Stack Edge resource before you install an Azure Stack Box Edge physical device.
2. Install Azure Stack Edge Pro GPU	Unpack, rack, and cable the Azure Stack Edge Pro GPU physical device.
3. Connect to Azure Stack Edge Pro GPU	Once the device is installed, connect to device local web UI.
4. Configure network settings for Azure Stack Edge Pro GPU	Configure network including the compute network and web proxy settings for your device. If setting up a two-node cluster, advanced networking and cluster configuration is also needed.
5. Configure device settings for Azure Stack Edge Pro GPU	Assign a device name and DNS domain, configure update server and device time.

STEP	DESCRIPTION
6. Configure security settings for Azure Stack Edge Pro GPU	Configure certificates for your device. Use device-generated certificates or bring your own certificates.
7. Activate Azure Stack Edge Pro GPU	Use the activation key from service to activate the device. The device is ready to set up SMB or NFS shares or connect via REST.
8. Configure compute	Configure the compute role on your device. A Kubernetes cluster is also created.
9A. Transfer data with Edge shares	Add shares and connect to shares via SMB or NFS.
9B. Transfer data with Edge storage accounts	Add storage accounts and connect to blob storage via REST APIs.

You can now begin to gather information regarding the software configuration for your Azure Stack Edge Pro GPU device.

Deployment configuration checklist

Before you deploy your device, you need to collect information to configure the software on your Azure Stack Edge Pro GPU device. Preparing some of this information ahead of time helps streamline the process of deploying the device in your environment. Use the [Azure Stack Edge Pro GPU deployment configuration checklist](#) to note down the configuration details as you deploy your device.

Prerequisites

Following are the configuration prerequisites for your Azure Stack Edge resource, your Azure Stack Edge Pro GPU device, and the datacenter network.

For the Azure Stack Edge resource

Before you begin, make sure that:

- Your Microsoft Azure subscription is enabled for an Azure Stack Edge resource. Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#). Pay-as-you-go subscriptions aren't supported. To identify the type of Azure subscription you have, see [What is an Azure offer?](#).
- You have owner or contributor access at resource group level for the Azure Stack Edge, IoT Hub, and Azure Storage resources.
 - To create any Azure Stack Edge resource, you should have permissions as a contributor (or higher) scoped at resource group level.
 - You also need to make sure that the `Microsoft.DataBoxEdge` and `Microsoft.KeyVault` resource providers are registered. To create any IoT Hub resource, `Microsoft.Devices` provider should be registered.
 - To register a resource provider, in the Azure portal, go to **Home > Subscriptions > Your-subscription > Resource providers**.
 - Search for the specific resource provider, for example, `Microsoft.DataBoxEdge`, and register the resource provider.
 - To create a Storage account resource, again you need contributor or higher access scoped at the resource group level. Azure Storage is by default a registered resource provider.

- To create an order in the Azure Edge Hardware Center, you need to make sure that the `Microsoft.EdgeOrder` provider is registered. For information on how to register, go to [Register resource provider](#).
- You have admin or user access to Azure Active Directory Graph API for generating activation key or credential operations such as share creation that uses a storage account. For more information, see [Azure Active Directory Graph API](#).

For the Azure Stack Edge Pro GPU device

Before you deploy a physical device, make sure that:

- You've [run the Azure Stack Network Readiness Checker tool](#) to check network readiness for your Azure Stack Edge device. You can use the tool to check whether your firewall rules are blocking access to any essential URLs for the service and verify custom URLs, among other tests. For more information, see [Check network readiness for your Azure Stack Edge device](#).
- You've reviewed the safety information that was included in the shipment package.
- To rackmount the device in a standard 19* rack in your datacenter, make sure to have:
 - A 1U slot available when deploying a single node device.
 - Two 1U slots available when deploying a two-node cluster.
- You have access to a flat, stable, and level work surface where the device can rest safely.
- The site where you intend to set up the device has standard AC power from an independent source or a rack power distribution unit (PDU) with an uninterruptible power supply (UPS).
- You have access to your device.

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured per the networking requirements for your Azure Stack Edge Pro GPU device. For more information, see [Azure Stack Edge Pro GPU System Requirements](#).
- For normal operating conditions of your Azure Stack Edge Pro GPU, you have:
 - A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
 - A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Create a new resource

In this step, you'll first order a device and then create a management resource to manage the device with the service in the cloud.

Create an order resource

To order a device, use the Azure Edge Hardware Center. [Azure Edge Hardware Center](#) lets you explore and order a variety of hardware from the Azure hybrid portfolio including Azure Stack Edge Pro GPU devices.

If you have an existing device, skip this step and [Create a management resource for your device](#).

When you place an order through the Edge Hardware Center, you can order multiple devices, to be shipped to more than one address, and you can reuse ship to addresses from other orders.

Ordering through Edge Hardware Center will create an Azure resource that will contain all your order-related information. One resource each will be created for each of the units ordered. You'll have to create an Azure Stack Edge resource after you receive the device to activate and manage the devices.

To place an order through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.
2. Select **+ Create a resource**. Search for and select **Azure Edge Hardware Center**. In the Azure Edge Hardware Center, select **Create**.

Azure Edge Hardware Center

Azure Edge Hardware Center
Microsoft
☆☆☆☆ 0.0 (0 ratings)

Create

Overview Plans Usage Information + Support Reviews

Use Azure Edge Hardware Center to order first-party Azure hardware that lets you build and run hybrid apps across datacenters, edge locations, remote offices and the cloud.

Azure Edge Hardware Center lets you choose from a variety of hardware as per your business need and helps you keep track of all the ordered hardware at a single place.

More offers from Microsoft [See All](#)

Workspace Microsoft Virtual Machine Azure Virtual Desktop resource	Microsoft HPC Pack 2012 R2 Microsoft Virtual Machine Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux workloads.	Windows 10 IoT Core Services Microsoft Azure Service Commercialize your project with enterprise-grade security and support	Web App + SQL Microsoft Azure Service Enjoy secure and flexible development, deployment, and scaling options for your web app
--	--	--	---

3. Select a subscription, and then select **Next**.

Get started

1 Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select a subscription

Select a subscription to manage deployed resources and costs.

Subscription

Contoso_USEast

Next

4. To start your order, select **Order** beside the product family that you want to order - for example, **Azure Stack Edge**. If you don't see the product family, you may need to use a different subscription; select **Try**

selecting a different subscription.

The screenshot shows the 'Get started' page of the Azure Edge Hardware Center. At the top, there's a breadcrumb navigation: Home > Azure Edge Hardware Center >. Below it, a header says 'Get started' with a three-dot menu icon and a close button (X). A callout box contains the text: 'Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)'

The main content area is titled 'Select product family' and displays a message: 'Showing 1 product families for selected subscription: ExpressPod BVT (Creates order in BVT env)'. It lists a single product family: 'Azure Stack Edge' (represented by a cloud icon), described as 'Azure managed physical edge compute device'. To the right of the product name is a red-bordered 'Order' button. Below the product listing, a message says: 'Can't see the product family you are looking for? [Try selecting a different subscription.](#)'

5. Select the shipping destination for your order.

The screenshot shows the 'Select shipping destination' page of the Azure Edge Hardware Center. At the top, there's a breadcrumb navigation: Home > Azure Hardware Center | Overview >. Below it, a header says 'Azure Edge Hardware Center' with a three-dot menu icon and a close button (X). A callout box contains the text: 'Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)'

The main content area is titled 'Select shipping destination'. It shows a product summary: 'Azure Stack Edge' (cloud icon) and 'Order to be billed against subscription: Contoso_USWest ([Change](#))'. Below this, a message says: 'Select the country/region where you would like your device to be shipped. *'. A dropdown menu is shown with 'United States' selected, also red-bordered. At the bottom is a red-bordered 'Next' button.

6. On the **Select Hardware** page, use the **Select** button to select the hardware product to order. For example, here **Azure Stack Edge Pro - GPU** was selected.

 Select Hardware ... X

Hardware family: Azure Stack Edge ([Change](#)) Subscription: Contoso_USWest Ship to country/region: United States

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Device specifications	<ul style="list-style-type: none"> • 1U rack mount device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Azure Private Edge Zones enabled 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Pro R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Portable, server class device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Specialized rugged casing tailored for harsh environments 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Mini R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Ultra-portable, WiFi enabled device with battery • Hardware accelerated ML using VPU • Specialized rugged casing tailored for harsh environments 	\$\$\$ USD	Select

After you select a hardware product, you'll select the device configuration to order. For example, if you chose Azure Stack Edge Pro - GPU, you can choose from Azure Stack Edge Pro - 1 GPU and Azure Stack Edge Pro - 2 GPU models.

7. Select the device configuration, and then choose **Select**. The available configurations depend on the hardware you selected. The screen below shows available configurations for Azure Stack Edge Pro - GPU devices.

If you're ordering Azure Stack Edge Mini R devices, which all have the same configuration, you won't see this screen.

Home >
Select Hardware ...

Hardware family: Azure Stack Edge ([Change](#)) Azure managed physical edge compute device

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Hardware specifications	<p>Azure Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. The device is powered with NVIDIA T4 GPUs to provide accelerated AI inferencing at the edge. You can choose from the available configurations with one or two GPUs basis your business need</p> <p>Select a configuration</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Usable compute</th> <th>Usable memory</th> <th>Usable storage</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> <tr> <td><input type="radio"/> Azure Stack Edge Pro - 2 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> </tbody> </table> <p>Learn more Azure Stack Edge Pro - GPU documentation</p>				Model	Usable compute	Usable memory	Usable storage	<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB	<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB
Model	Usable compute	Usable memory	Usable storage													
<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB													
<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB													

[Select](#)

The **Create order** wizard opens.

8. On the **Basics** tab, provide an **Order name**, **Resource group**, and **Region**. Then select **Next: Shipping + quantity >**.

Create order

X

Basics Shipping + quantity Notifications Tags Review + create

Hardware details

 Azure Stack Edge Pro - 1 GPU

Usable compute : 40 vCPU Usable memory : 102 GB

Usable storage : 4.2 TB

Order details

Order name *

Pro1GPUdevices

The selected subscription will be used to manage deployed resources and billing. Select or create a new resource group to organize and manage all your resources.

Subscription *

Contoso_USEast

Resource group *

USEast_ASE



[Create new](#)

Region *

East US



Review + create

< Previous

Next : Shipping + quantity >

Next, you'll add each ship to address you want to send devices to and then specify how many devices to send to each address. You can order up to 20 units (devices) per order.

9. On the **Shipping + quantity** tab, add each ship to address to send devices to:

- To add a new ship to address, select **Add a new address**.

A required **Address alias** field on the **New address** screen identifies the address for later use. Select **Add** when you finish filling in the address fields. Then use **Select address(es)** to add the address to your order.

- To use a ship to address from a previous order, or to use an address that you just added, choose **Select address(es)**. Then, on the **Select address(es)** screen, select one or more addresses, and choose **Select**.

<input type="checkbox"/>	Contact person	Address
<input checked="" type="checkbox"/>	Gus Poland 4255555555 gusp@contoso.com Contoso LE	contoso-redmond One Microsoft Way Building 52 Redmond WA 98152 United States
<input type="checkbox"/>	Gus Poland 4085555555 gusp@contoso.com Contoso LE	contoso-sunnyvale 1020 Enterprise Way Building 2 Sunnyvale CA 94089 United States
<input checked="" type="checkbox"/>	Claudia Olivares 4085555555 gusp@contoso.com Contoso LE	SVBldg2 1020 Enterprise Way Building 2 Sunnyvale

The **Shipping + quantity** tab now has a separate item for each ship to address.

Each order item name includes a name prefix (the order name followed by the address alias), with an item number for each device that is shipped to that address.



Create order

...

Basics **Shipping + quantity**

Notifications

Tags

Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Su CA 94089 US	1	Pro1GPUDevicesSVBldg2-01 Order name Address alias Item #
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01

[Review + create](#) [< Previous](#) [Next : Notifications >](#)

10. For each address, enter the **Quantity** of devices to ship on the **Shipping + quantity** tab.

When you enter a quantity of more than one, a **+n more** label appears after the order item name.



Create order

...

Basics **Shipping + quantity**

Notifications

Tags

Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Sunnyva CA 94089 US	3	Pro1GPUDevicesSVBldg2-... +2 more [Delete]
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01 [Delete]

[Add a new address](#) [Select address\(es\)](#)

11. If you want to change the names of order items, select and click the order item name to open the **Rename order item** pane. If you're shipping more than one item to an address, select **+n more**.

You can make two types of name change:

- To use a different name prefix for all of the order items, edit the **Name prefix** and then select

Apply, as shown on the following screen.

- You can also edit the name of each order item individually.

When you finish, select **Done**.

Select **Next: Notifications** > to continue.

12. If you want to receive status notifications as your order progresses, enter the email address for each recipient on the **Notifications** tab.

To add an email address, enter the address, and select **Add**. You can add up to 20 email addresses.

The screenshot shows the 'Create order' interface. At the top, there's a breadcrumb trail: Home > Select Hardware >. Below it is a title bar with 'Create order' and a close button ('X'). The main area has several tabs: Basics, Shipping + quantity, Notifications (which is highlighted with a red box), Tags, and Review + create. A note below the tabs says: 'We will update you regarding your order progress. You can specify up to 20 email address(es) to receive updates for your order status. Your subscription owner and admin will receive email notifications by default.' Under the 'Email' section, there's a text input field containing 'claudiao@contoso.com' and a red-bordered 'Add' button. Below this, two email addresses are listed: 'gusp@contoso.com' and 'OpsMgmt@contoso.com', each with a 'Remove' link. At the bottom, there are navigation buttons: a red-bordered 'Review + create' button, '< Previous', and 'Next : Tags >'.

When you finish, select **Review + create** to continue.

13. On the **Review + create** tab:

- Review your order. The order is automatically validated when you open this screen. If you see a **Validation failed** banner, you'll have to fix the issues before you create the order.
- Review the **Privacy terms**, and select the check box to agree to them.
- Select **Create**.



Create order



Validation passed.

Basics Shipping + quantity Notifications Tags Review + create

Order name Pro1GPUdevices

Total hardware units 4

Total monthly service fee <Fee>

Total shipping fee <Fee>

Hardware details

Azure Stack Edge Pro - 1 GPU

Usable compute 40 vCPU

Usable memory 102 GB

Usable storage 4.2 TB

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Basics

Subscription Contoso_USEast

Resource Group USEast_ASE

Region East US

Notifications

Emails gusp@contoso.com, OpsMgmt@contoso.com

Shipping + quantity

Total hardware units (4)

Shipping address	Order item name
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-01
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-02
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-03
contoso-sunnyvale, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicescontoso-su-01

Create

< Previous

Next >

During deployment, the order opens in the portal, with the status of each order item displayed. After deployment completes, you may need to click the Down arrow by **Deployment details** to see the status of individual items.

Resource	Type	Status	Operation details
SVBldg2	Microsoft.EdgeOrder/addresses	OK	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	OK	Operation details
Pro1GPUDevicesSunnyvale2-02	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-03	Microsoft.EdgeOrder/orderItems	OK	Operation details

- To view details for an order item, shown below, select the item in the **Resource** column of the deployment details.

Order item information	
Placed on : 8/6/2021	Shipping address 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US
Order name : Pro1GPUDevices	Contact information Claudia Olivares 4085550111, claudiao@contoso.com
View Updates	

Hardware information	
<p>Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage</p> <p>While your hardware arrives, configure your infrastructure. Learn more</p>	

- After a device ships (**Shipped** tag is green), a **Configure hardware** option is added to the item details. Select that option to create a management resource for the device in Azure Stack Edge.

The screenshot shows the Azure Edge Hardware Center interface for an order named 'DemoOrderASAdd1-03'. The 'Overview' tab is selected. Key details shown include:

- Resource group: USEast_ASE
- Location: eastus2euap
- Subscription: Contoso_USEast
- Subscription ID: 1a23bc45-678d-90f1-2ghi-j34klm6n6780
- Order name: Pro1GPUDevices
- Order item name: Pro1GPUDevicesSunnyvale2-02 -03
- Status: Ordered, Shipped (highlighted with a red box), Delivered
- Placed on: 6/24/2021
- Order name: DemoOrderAS
- Shipping address: abc street, xyz city, pqr state 7698798 US
- Contact information: Anam Shaher, 8768789798, ashaheer@hotmail.com
- Hardware information: Azure Stack Edge Pro - 1 GPU: 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage
- Action: Configure hardware

The subscription, resource group, and deployment area are filled in from the order, but you can change them.

The screenshot shows the 'Create management resource' wizard in the Azure Stack Edge portal. The 'Basics' step is active. The 'Device' section shows:

Device	Order resource name	Status
Azure Stack Edge Pro - 1 GPU	DemoOrderASAdd1-03	Delivered

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * ⓘ: Contoso_USEast

Resource group * ⓘ: USEast_ASE

INSTANCE DETAILS

Name * ⓘ: (empty input field)

Deploy Azure resource in * ⓘ: (US) East US

Buttons at the bottom: Review + create, Previous, Next: Tags

After you activate the device, you'll be able to open the management resource from the item, and open the order item from the management resource.

Create a management resource for each device

To create a management resource for a device ordered through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.

2. There are two ways to get started creating a new management resource:

- Through the Azure Edge Hardware Center: Search for and select **Azure Edge Hardware Center**. In the Hardware Center, display **All order items**. Select the item **Name**. In the item **Overview**, select **Configure hardware**.

The **Configure hardware** option appears after a device is shipped.



- In Azure Stack Edge: Search for and select **Azure Stack Edge**. Select **+ Create**. Then select **Create management resource**.



The **Create management resource** wizard opens.

3. On the **Basics** tab, enter the following settings:

SETTING	VALUE
Select a subscription ¹	Select the subscription to use for the management resource.
Resource group ¹	Select the resource group to use for the management resource.
Name	Provide a name for the management resource.
Deploy Azure resource in	Select the country or region where the metadata for the management resource will reside. The metadata can be stored in a different location than the physical device.

¹ An organization may use different subscriptions and resource groups to order devices than they use to manage them.

A screenshot of the "Create management resource" wizard. The "Basics" tab is selected. The "PROJECT DETAILS" section is highlighted with a red box, showing fields for "Select a subscription" (set to "DataBox_Edge_Test") and "Resource group" (set to "myaserg"). The "INSTANCE DETAILS" section is also highlighted with a red box, showing fields for "Name" (set to "myasetestorder") and "Deploy Azure resource in" (set to "(US) East US"). At the bottom, there are "Review + create", "Previous", and "Next: Tags" buttons.

Select **Review + create** to continue.

4. On the **Review + create** tab, review basic settings for the management resource and the terms of use. Then select **Create**.

If you started this procedure by clicking **Configure hardware** for a delivered item in an Azure Edge Hardware Center order, the device, order resource name, and order status are listed at the top of the screen.

Home > Azure Edge Hardware Center > nidhitest1nidhiaddr-04 >

Create management resource

Azure Stack Edge

All validations have passed.

Basics Tags Review + create

Device	Order resource name	Status
Azure Stack Edge Pro - 2 GPU	nidhitest1nidhiaddr-04	Delivered

Terms and conditions
Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Basics

Subscription	ExpressPod BVT (Creates order in BVT env)
Resource group	nidhitest
Name	myNewDevice
Region	(US) East US

Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.

Create Previous Next

The **Create** button isn't available until all validation checks have passed.

5. When the process completes, the **Overview** pane for new resource opens.

Home > Sunnyvale-ASE1GPUdevices-01 | Overview

Deployment

Search (Ctrl+ /) <> Delete Cancel Redeploy Refresh

Overview

We'd love your feedback! →

Your deployment is complete

Deployment name: Sunnyvale-ASE1GPUdevices-01 Start time: 6/29/2021, 6:04:02 PM
Subscription: Azure Data Box testing Correlation ID: bee14110-d803-4ff4-82a5-6f7e1420d216
Resource group: ContosoEastRG

Deployment details (Download)

Resource	Type	Status	Operation details
Sunnyvale-ASE1GPUdevice	Microsoft.DataBoxEdge/...	OK	Operation details

Next steps

Go to resource

Security Center
Secure your apps and infrastructure
[Go to Azure security center >](#)

Free Microsoft tutorials
[Start learning today >](#)

Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.
[Find an Azure expert >](#)

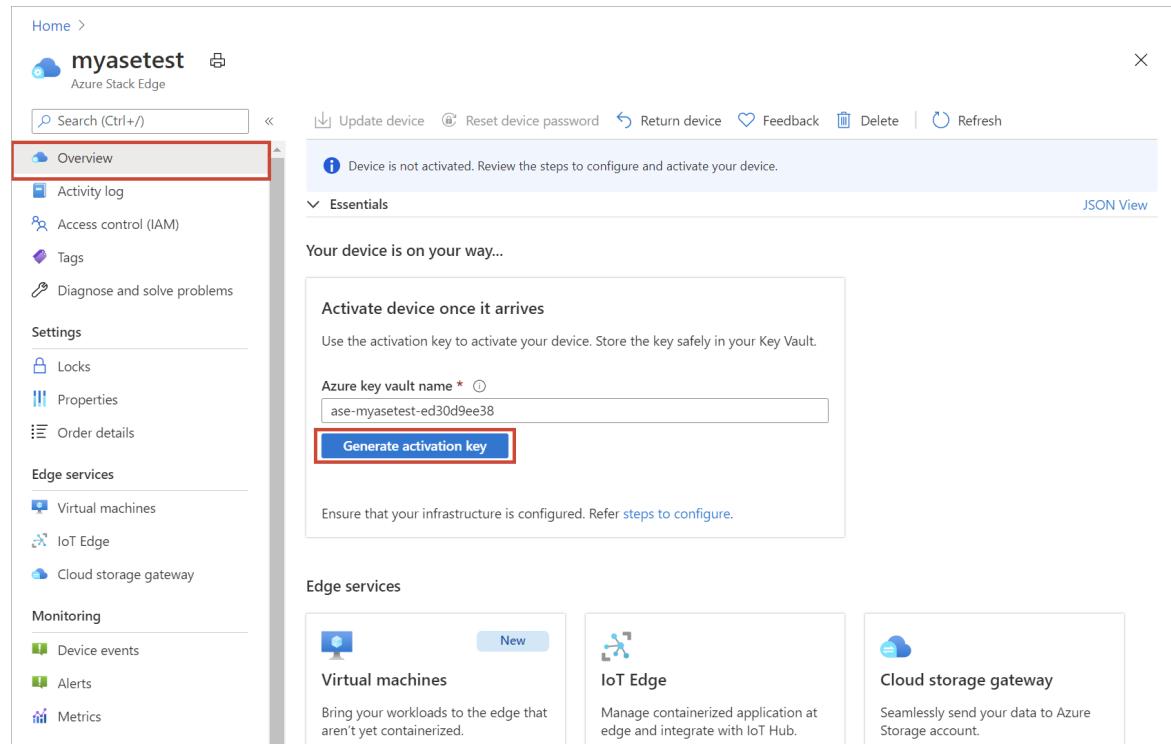
Get the activation key

After the Azure Stack Edge resource is up and running, you'll need to get the activation key. This key is used to activate and connect your Azure Stack Edge Pro GPU device with the resource. You can get this key now while you are in the Azure portal.

1. Select the resource you created, and select **Overview**.
2. In the right pane, enter a name for the Azure Key Vault or accept the default name. The key vault name can be between 3 and 24 characters.

A key vault is created for each Azure Stack Edge resource that is activated with your device. The key vault lets you store and access secrets, for example, the Channel Integrity Key (CIK) for the service is stored in the key vault.

Once you've specified a key vault name, select **Generate key** to create an activation key.



The screenshot shows the Azure Stack Edge Overview page for a resource named "myasetest". The left sidebar lists various sections like Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area has a heading "Your device is on your way..." and a section titled "Activate device once it arrives". It contains a text input field for "Azure key vault name" with the value "ase-myasetest-ed30d9ee38" and a blue button labeled "Generate activation key". Below this, a note says "Ensure that your infrastructure is configured. Refer [steps to configure](#)". At the bottom, there's a "Edge services" section with three cards: "Virtual machines" (New), "IoT Edge", and "Cloud storage gateway".

Wait a few minutes while the key vault and activation key are created. Select the copy icon to copy the key and save it for later use.

IMPORTANT

- The activation key expires three days after it is generated.
- If the key has expired, generate a new key. The older key is not valid.

Next steps

In this tutorial, you learned about Azure Stack Edge articles such as:

- Create a new resource
- Get the activation key

Advance to the next tutorial to learn how to install Azure Stack Edge.

[Install Azure Stack Edge Pro GPU](#)

Tutorial: Install Azure Stack Edge Pro with GPU

9/21/2022 • 12 minutes to read • [Edit Online](#)

This tutorial describes how to install an Azure Stack Edge Pro physical device with a GPU. The installation procedure involves unpacking, rack mounting, and cabling the device.

The installation can take around two hours to complete.

This tutorial describes how to install a two-node Azure Stack Edge Pro GPU cluster. The installation procedure involves unpacking, rack mounting, and cabling the device.

The installation can take around 2.5 hours to complete.

In this tutorial, you learn how to:

- Unpack the device
- Rack mount the device
- Cable the device

Prerequisites

The prerequisites for installing a physical device as follows:

For the Azure Stack Edge resource

Before you begin, make sure that:

- You've completed all the steps in [Prepare to deploy Azure Stack Edge Pro with GPU](#).
 - You've created an Azure Stack Edge resource to deploy your device.
 - You've generated the activation key to activate your device with the Azure Stack Edge resource.

For the Azure Stack Edge Pro physical device

Before you deploy a device:

- Make sure that the device rests safely on a flat, stable, and level work surface.
- Verify that the site where you intend to set up has:
 - Standard AC power from an independent source.

-OR-

- A rack power distribution unit (PDU) with an uninterruptible power supply (UPS).
- An available 1U slot on the rack on which you intend to mount the device.

For the network in the datacenter

Before you begin:

- Review the networking requirements for deploying Azure Stack Edge Pro, and configure the datacenter network per the requirements. For more information, see [Azure Stack Edge Pro networking requirements](#).
- Make sure that the minimum Internet bandwidth is 20 Mbps for optimal functioning of the device.

Unpack the device

This device is shipped in a single box. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, don't open it. Contact Microsoft Support to help you assess whether the device is in good working order.
3. Unpack the box. After unpacking the box, make sure that you have:
 - One single enclosure Azure Stack Edge Pro device
 - Two power cords
 - One rail kit assembly
 - A Safety, Environmental, and Regulatory Information booklet

This device is shipped in a two boxes. Complete the following steps to unpack your device.

1. Place the boxes on a flat, level surface.
2. Inspect the boxes and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the box or packaging is severely damaged, don't open it. Contact Microsoft Support to help you assess whether the devices are in good working order.
3. Unpack each box. After unpacking the box, make sure that you have the following in each box:
 - One single enclosure Azure Stack Edge devices
 - Two power cords
 - One rail kit assembly
 - A Safety, Environmental, and Regulatory Information booklet

If you didn't receive all of the items listed here, [Contact Microsoft Support](#). The next step is to rack mount your device.

Rack the device

The device must be installed on a standard 19-inch rack. Use the following procedure to rack mount your device on a standard 19-inch rack.

IMPORTANT

Azure Stack Edge Pro devices must be rack-mounted for proper operation.

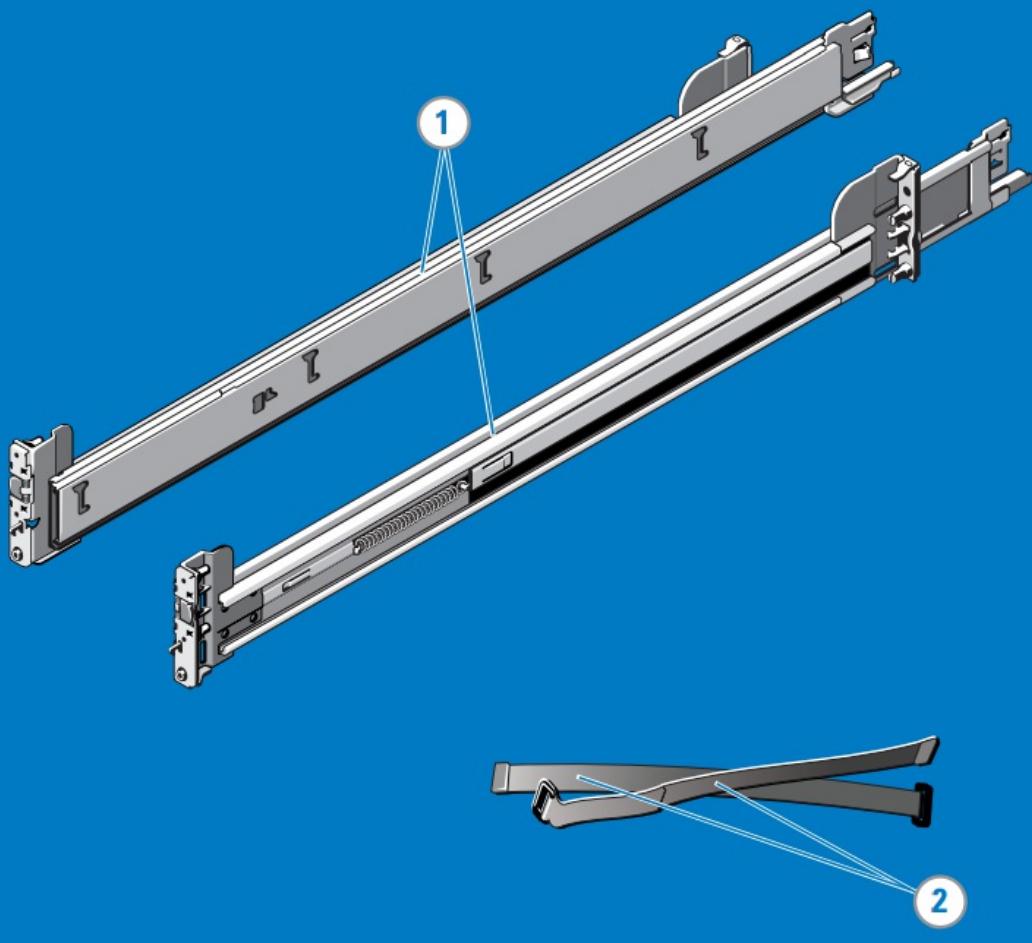
Prerequisites

- Before you begin, read the safety instructions in your Safety, Environmental, and Regulatory Information booklet. This booklet was shipped with the device.
- Begin installing the rails in the allotted space that is closest to the bottom of the rack enclosure.
- For the toolless rail mounting configuration:
 - You need to supply eight screws: #10-32, #12-24, #M5, or #M6. The head diameter of the screws must be less than 10 mm (0.4").
 - You need a flat-tipped screwdriver.

Identify the rail kit contents

Locate the components for installing the rail kit assembly:

- Two A7 Dell ReadyRails II sliding rail assemblies
- Two hook and loop straps

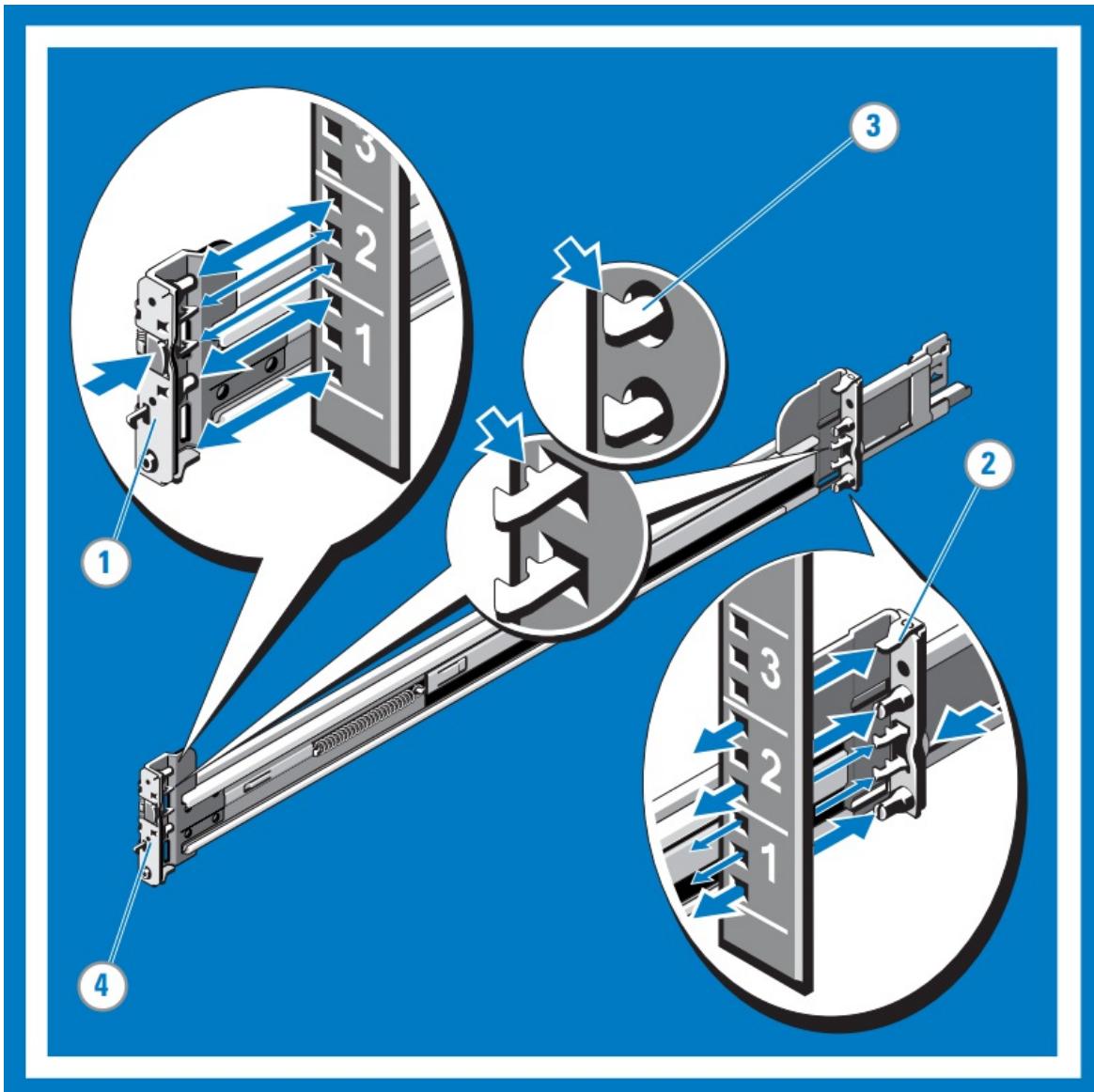


Install and remove tool-less rails (Square hole or round hole racks)

TIP

This option is tool-less because it does not require tools to install and remove the rails into the unthreaded square or round holes in the racks.

1. Position the left and right rail end pieces labeled **FRONT** facing inward and orient each end piece to seat in the holes on the front side of the vertical rack flanges.
2. Align each end piece in the bottom and top holes of the desired U spaces.
3. Engage the back end of the rail until it fully seats on the vertical rack flange and the latch clicks into place. Repeat these steps to position and seat the front-end piece on the vertical rack flange.
4. To remove the rails, pull the latch release button on the end piece midpoint and unseat each rail.

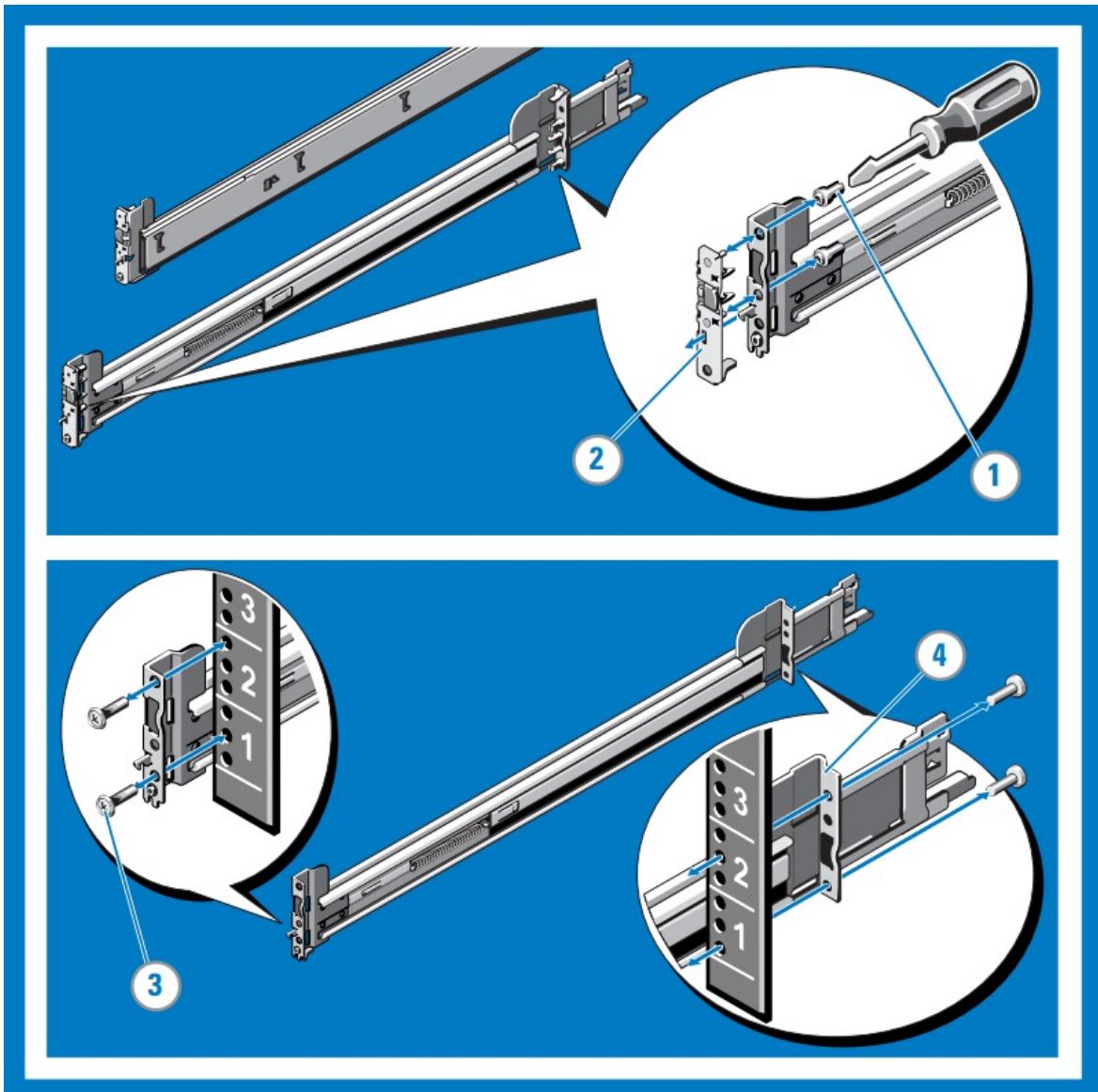


Install and remove tooled rails (Threaded hole racks)

TIP

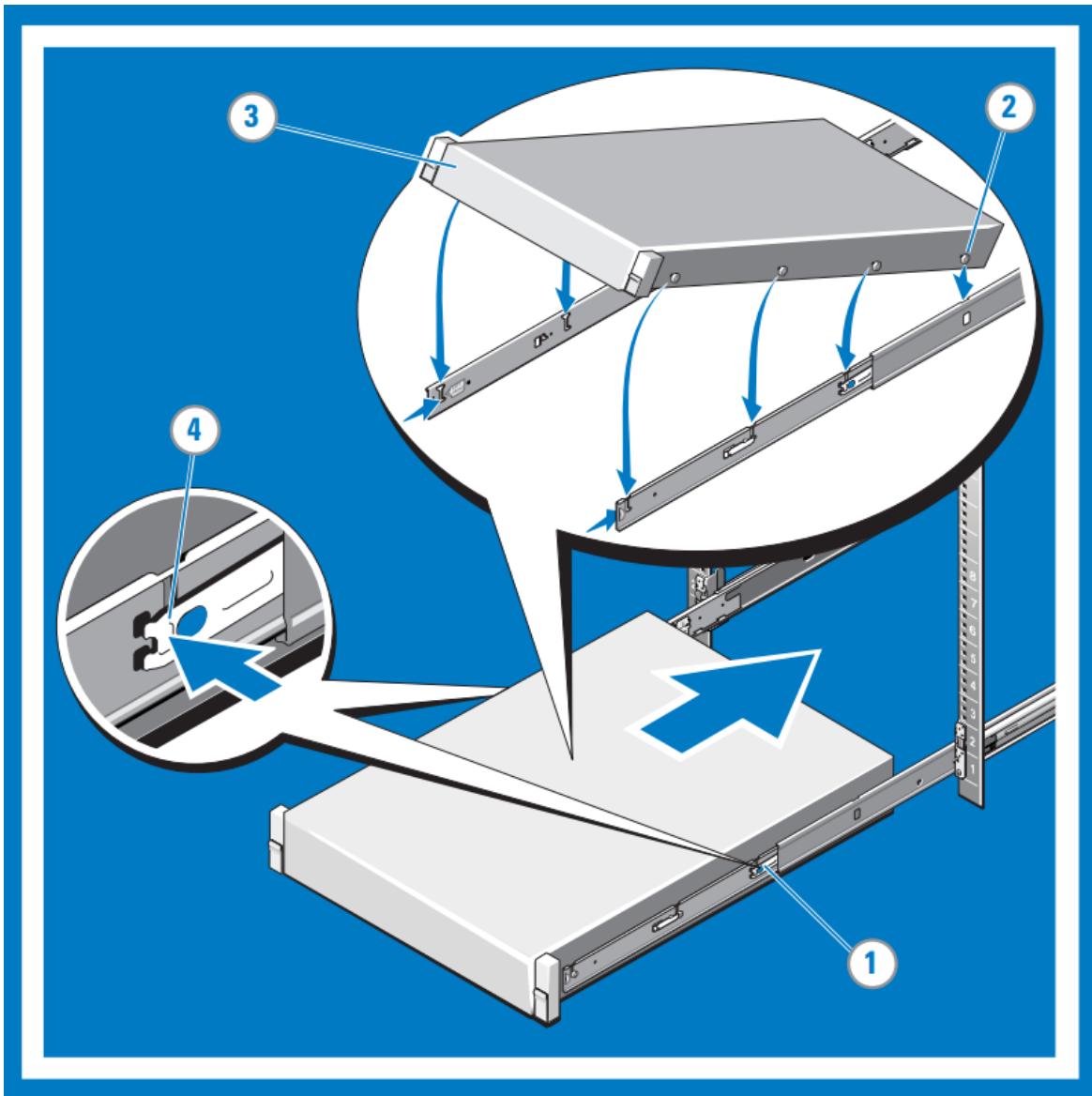
This option is tooled because it requires a tool (*a flat-tipped screwdriver*) to install and remove the rails into the threaded round holes in the racks.

1. Remove the pins from the front and rear mounting brackets using a flat-tipped screwdriver.
2. Pull and rotate the rail latch subassemblies to remove them from the mounting brackets.
3. Attach the left and right mounting rails to the front vertical rack flanges using two pairs of screws.
4. Slide the left and right back brackets forward against the rear vertical rack flanges and attach them using two pairs of screws.



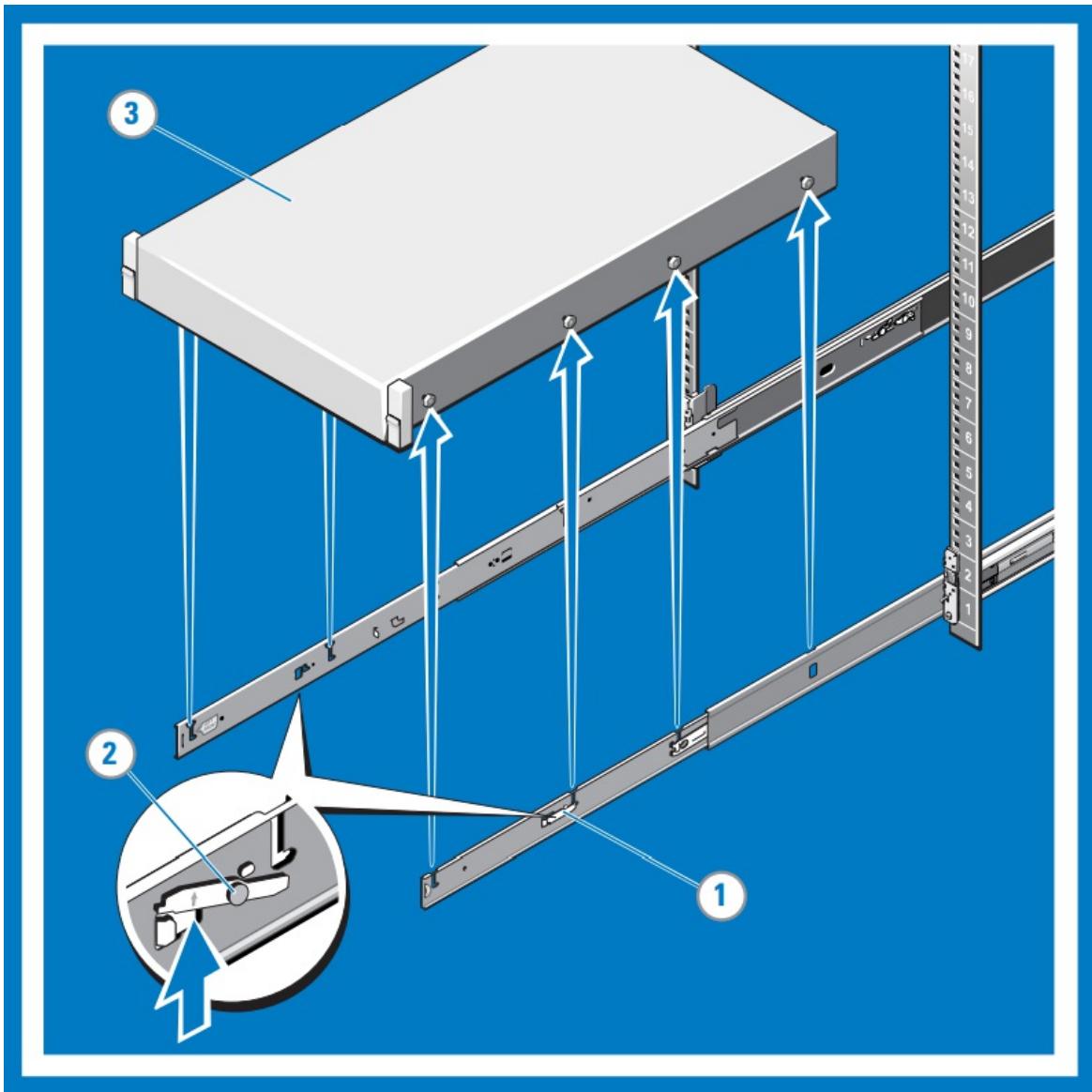
Install the system in a rack

1. Pull the inner slide rails out of the rack until they lock into place.
2. Locate the rear rail standoff on each side of the system and lower them into the rear J-slots on the slide assemblies. Rotate the system downward until all the rail standoffs are seated in the J-slots.
3. Push the system inward until the lock levers click into place.
4. Press the slide-release lock buttons on both rails and slide the system into the rack.



Remove the system from the rack

1. Locate the lock levers on the sides of the inner rails.
2. Unlock each lever by rotating it up to its release position.
3. Grasp the sides of the system firmly and pull it forward until the rail standoffs are at the front of the J-slots. Lift the system up and away from the rack and place it on a level surface.

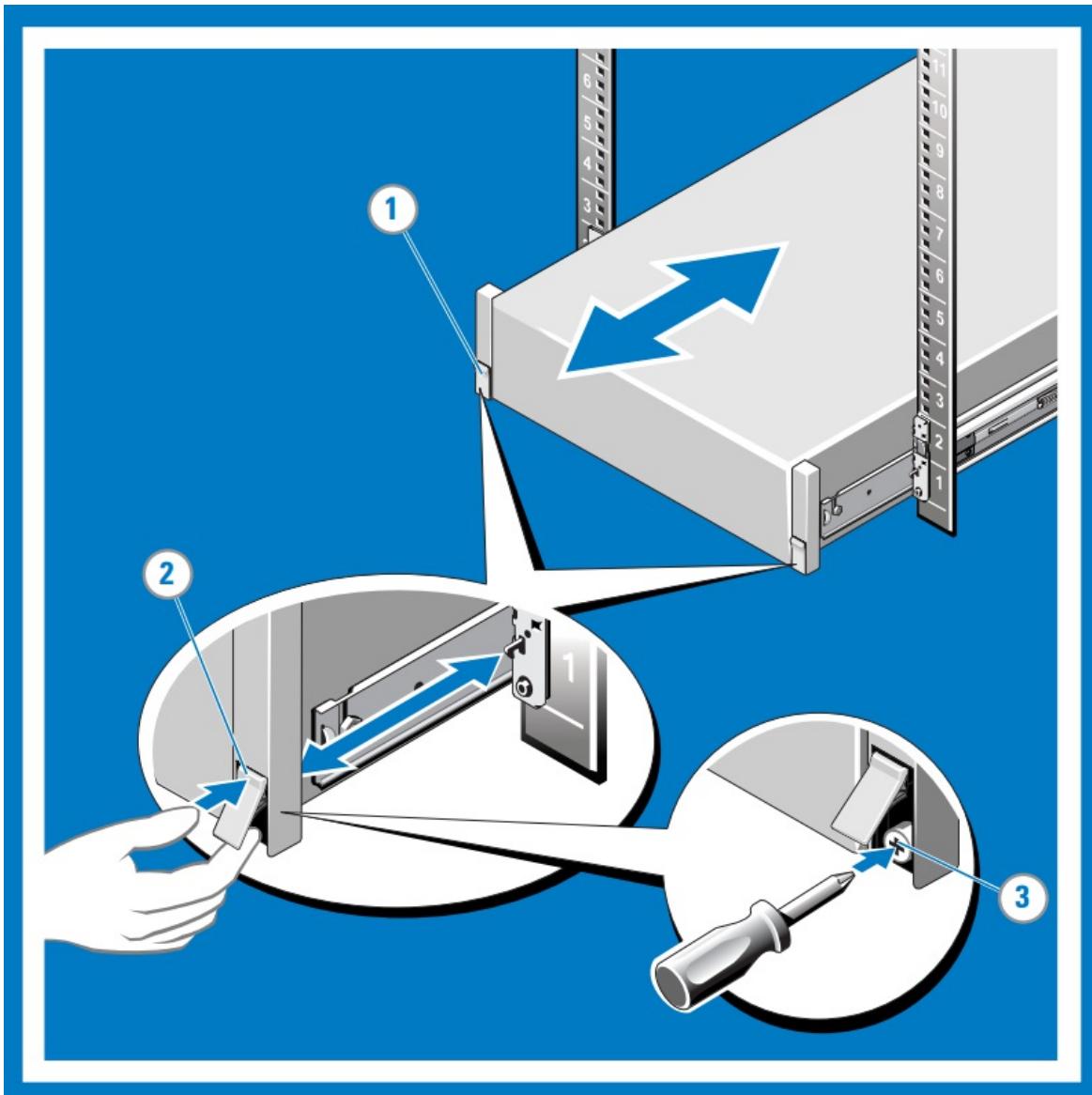


Engage and release the slam latch

NOTE

For systems not equipped with slam latches, secure the system using screws, as described in step 3 of this procedure.

1. Facing the front, locate the slam latch on either side of the system.
2. The latches engage automatically as the system is pushed into the rack and are released by pulling up on the latches.
3. To secure the system for shipment in the rack or for other unstable environments, locate the hard-mount screw under each latch and tighten each screw with a #2 Phillips screwdriver.



Cable the device

Route the cables and then cable your device. The following procedures explain how to cable your Azure Stack Edge Pro device for power and network.

Cabling checklist

Before you start cabling your device, you need the following things:

- Your Azure Stack Edge Pro physical device, unpacked, and rack mounted.
- Two power cables.
- At least one 1-GbE RJ-45 network cable to connect to the management interface. There are two 1-GbE network interfaces, one management and one data, on the device.
- One 25/10-GbE SFP+ copper cable for each data network interface to be configured. At least one data network interface from among PORT 2, PORT 3, PORT 4, PORT 5, or PORT 6 needs to be connected to the Internet (with connectivity to Azure).
- Access to two power distribution units (recommended).
- At least one 1-GbE network switch to connect a 1-GbE network interface to the Internet for data. The local web UI won't be accessible if the connected switch isn't at least 1 GbE. If using 25/10-GbE interface for data, you'll need a 25-GbE or 10-GbE switch.

NOTE

- If you are connecting only one data network interface, we recommend that you use a 25/10-GbE network interface such as PORT 3, PORT 4, PORT 5, or PORT 6 to send data to Azure.
- For best performance and to handle large volumes of data, consider connecting all the data ports.
- The Azure Stack Edge Pro device should be connected to the datacenter network so that it can ingest data from data source servers.

Before you start cabling your device, you need the following things:

- Both of your Azure Stack Edge physical devices, unpacked, and rack mounted.
- Four power cables, two for each device node.
- At least two 1-GbE RJ-45 network cables to connect Port 1 on each device node for initial configuration.
- At least two 1-GbE RJ-45 network cables to connect Port 2 on each device node to the internet (with connectivity to Azure).
- 25/10-GbE SFP+ copper cables for Port 3 and Port 4 to be configured. Additional 25/10-GbR SFP+ copper cables if you'll also connect Port 5 and Port 6. Port 5 and Port 6 must be connected if you intend to [Deploy network functions on Azure Stack Edge](#).
- 25-GbE or 10-GbE switches if opting for a switched network topology. See [Supported network topologies](#).
- Access to two power distribution units (recommended).

NOTE

- For best performance and to handle large volumes of data, consider connecting all the data ports.
- The Azure Stack Edge Pro device should be connected to the datacenter network so that it can ingest data from data source servers.

Device front panel

The front panel on Azure Stack Edge device:

- Has disk drives and a power button.
 - There are 10 disk slots in the front of your device.
 - Slot 0 has a 240-GB SATA drive used as an operating system disk. Slot 1 is empty and slots 2 to 6 are NVMe SSDs used as data disks. Slots 7 to 9 are also empty.

Device backplane

The backplane of Azure Stack Edge device:

- Includes redundant power supply units (PSUs).
- Has six network interfaces:
 - Two 1-Gbps interfaces.
 - Four 25-Gbps interfaces that can also serve as 10-Gbps interfaces.
 - A baseboard management controller (BMC).
- Has two network cards corresponding to the six ports:
 - **Custom Microsoft QLogic Cavium 25G NDC adapter** - Port 1 through port 4.
 - **Mellanox dual port 25G ConnectX-4 channel network adapter** - Port 5 and port 6.

For a full list of supported cables, switches, and transceivers for these network adapter cards, see:

- [QLogic Cavium 25G NDC adapter interoperability matrix](#).

- 25 GbE and 10 GbE cables and modules in [Mellanox dual port 25G ConnectX-4 channel network adapter compatible products](#).

NOTE

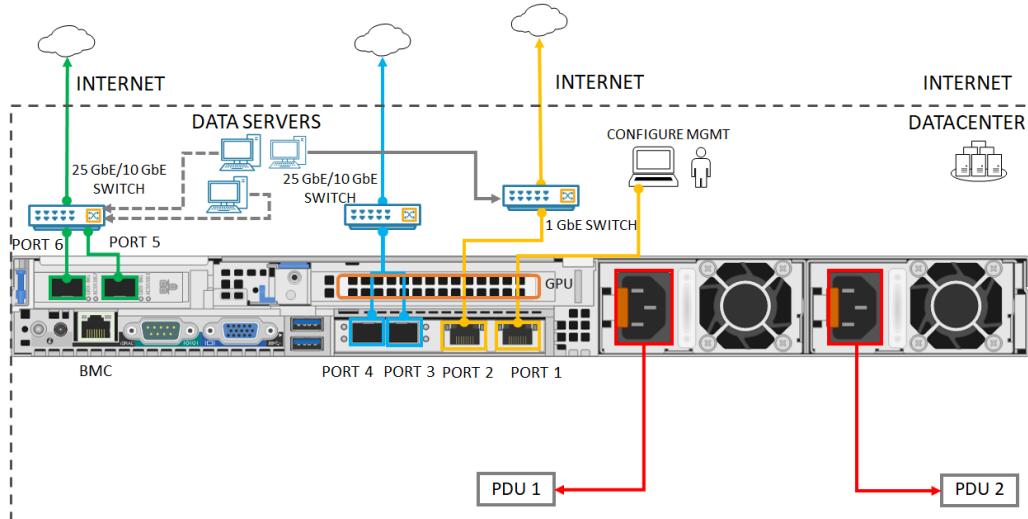
Using USB ports to connect any external device, including keyboards and monitors, is not supported for Azure Stack Edge devices.

Power cabling

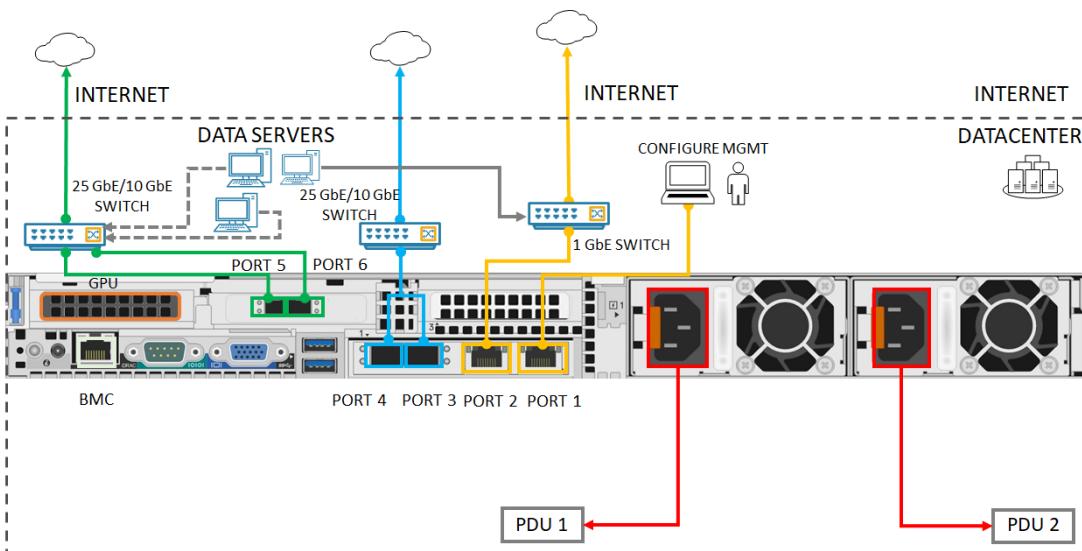
Take the following steps to cable your device for power and network.

1. Identify the various ports on the back plane of your device. You may have received one of the following devices from the factory depending on the number of GPUs in your device.

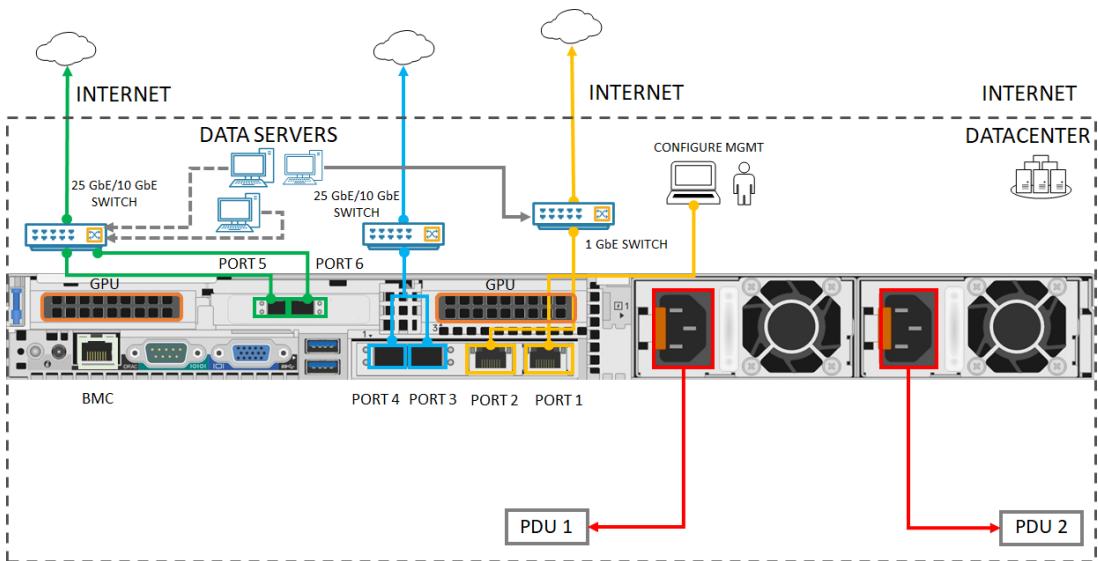
- Device with two Peripheral Component Interconnect (PCI) slots and one GPU



- Device with three PCI slots and one GPU



- Device with three PCI slots and two GPUs



2. Locate the disk slots and the power button on the front of the device.



3. Connect the power cords to each of the PSUs in the enclosure. To ensure high availability, install and connect both PSUs to different power sources.

4. Attach the power cords to the rack power distribution units (PDUs). Make sure that the two PSUs use separate power sources.

5. Press the power button to turn on the device.

6. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. PORT 1 serves as the management interface.

NOTE

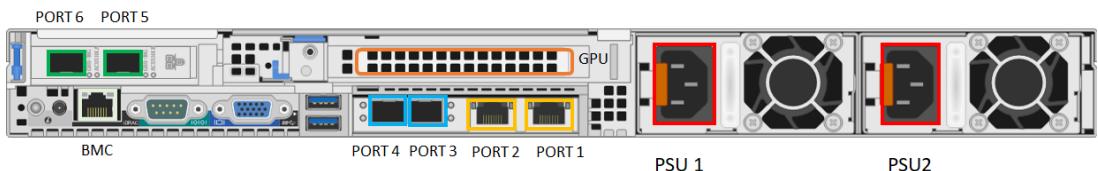
If connecting the computer directly to your device (without going through a switch), use an Ethernet crossover cable or a USB Ethernet adapter.

7. Connect one or more of PORT 2, PORT 3, PORT 4, PORT 5, or PORT 6 to the datacenter network/Internet.

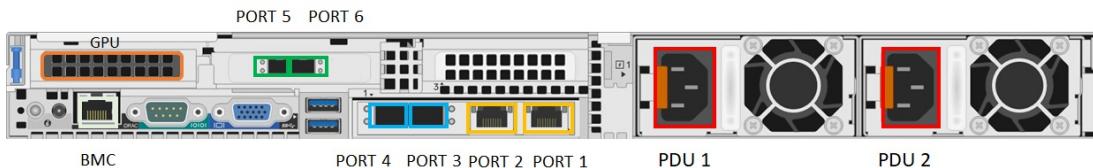
- If connecting PORT 2, use the 1-GbE RJ-45 network cable.
- For the 10/25-GbE network interfaces, use the SFP+ copper cables or fiber. If using fiber, use an optical to SFP adapter.
- For Network Function Manager deployments, make sure that PORT 5 and PORT 6 are connected. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).

1. Identify the various ports on the back plane of your device.

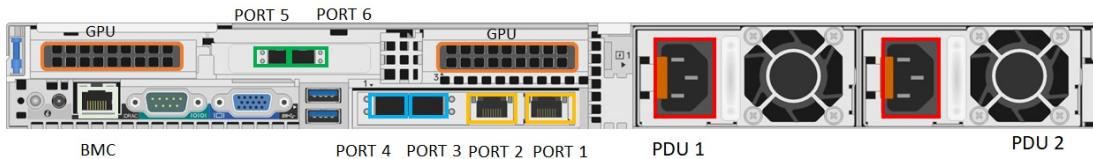
- Device with two Peripheral Component Interconnect (PCI) slots and one GPU



- Device with three PCI slots and one GPU



- Device with three PCI slots and two GPUs

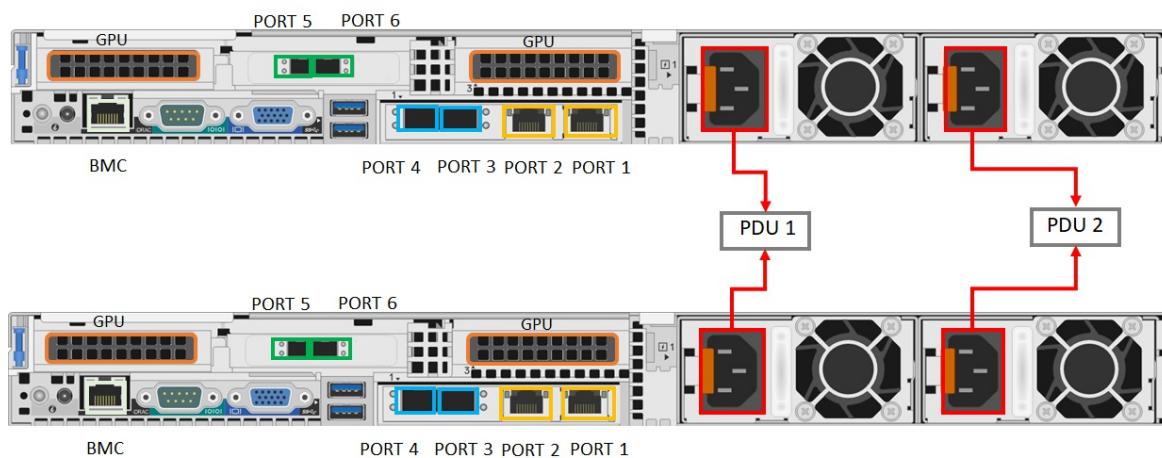


2. Locate the disk slots and the power button on the front of the device.



3. Connect the power cords to each of the PSUs in the enclosure.

4. To ensure high availability, the right power supply of the two devices should be connected to a Power Distribution Unit (PDU) or power source. The left power supply of both the devices should be connected to another PDU or power source.



5. Press the power button in the front panel of the device to turn on the device.

Network cabling

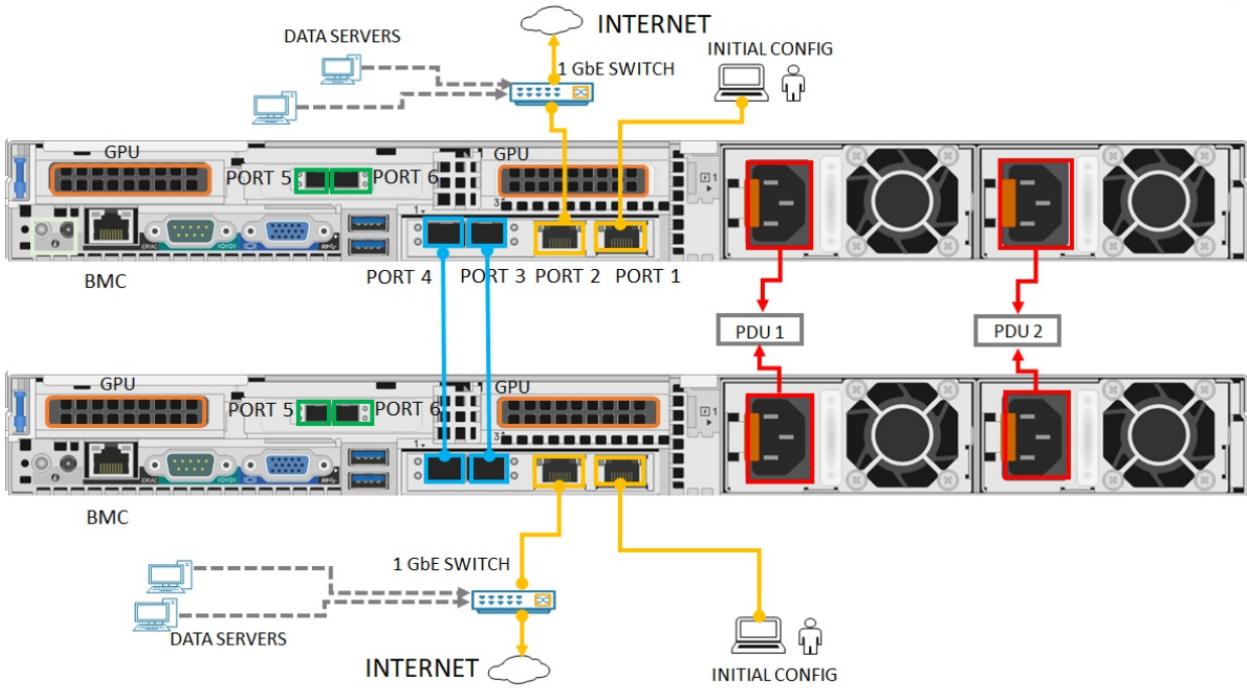
The two-node device can be configured in the following different ways:

- Without switches.
- Connect Port 3 and Port 4 via switches.
- Connect Port 3 via a switch.

Each of these configurations is described in the following sections. For more information on when to use these configurations, see [Supported network topologies](#)

Switchless

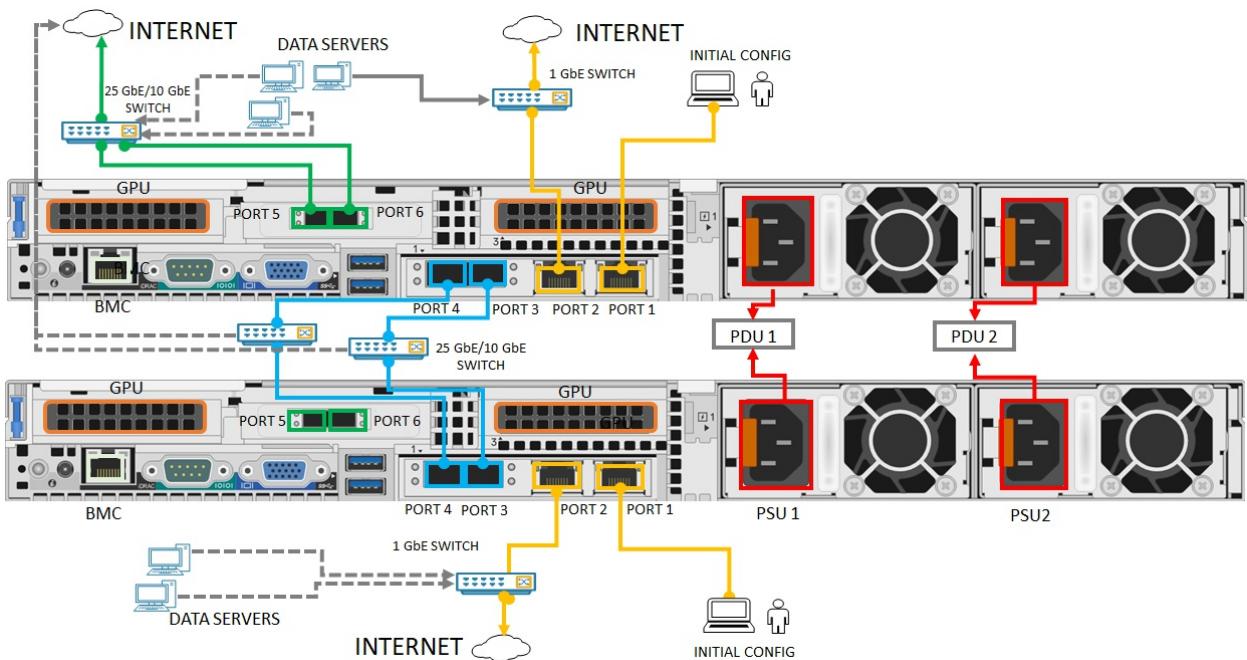
Use this configuration when high speed switches aren't available for storage and clustering traffic.



1. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. If connecting the computer directly to your device (without going through a switch), use an Ethernet crossover cable or a USB Ethernet adapter.
2. Connect PORT 2 to the internet using a 1-GbE RJ-45 network cable.
3. Connect PORT 3 and PORT 4 on both the devices via SFP+ copper cables or fiber. If using fiber, use an optical to SFP adapter.

Connect Port 3 and Port 4 via switches

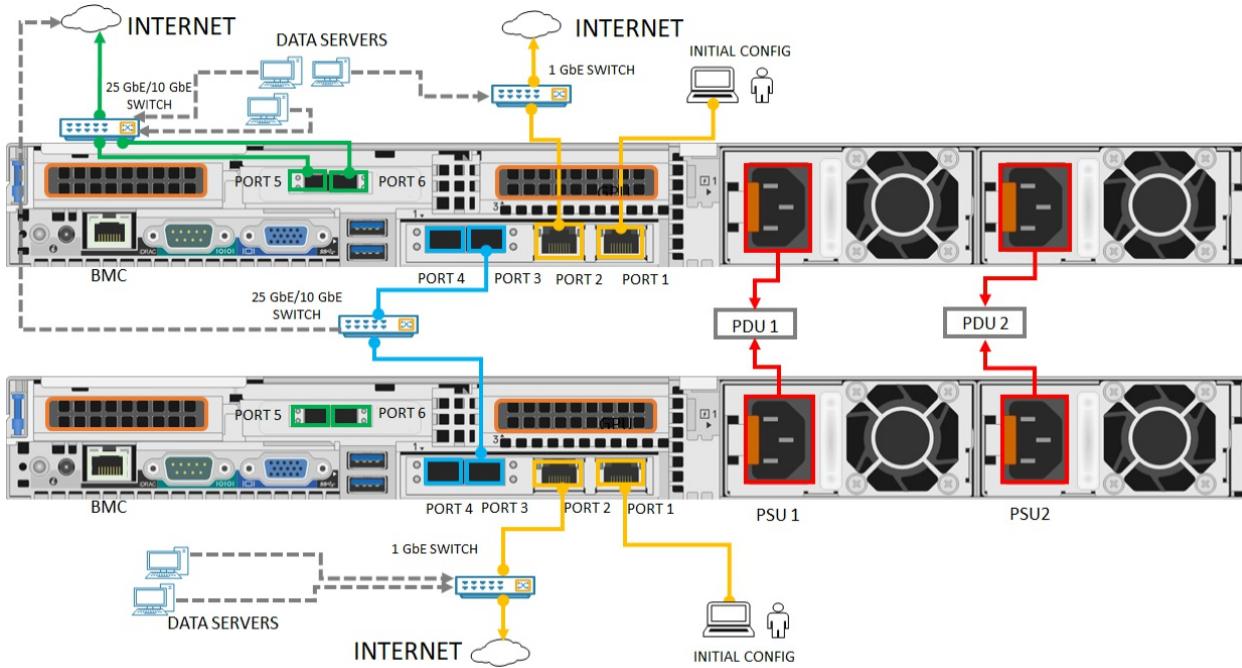
Use this configuration when you need port level redundancy through teaming.



1. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. If connecting the computer directly to your device (without going through a switch), use an Ethernet crossover cable or a USB Ethernet adapter.
2. Connect PORT 2 to the internet using a 1-GbE RJ-45 network cable.
3. Connect PORT 3 and PORT 4 on both the devices via SFP+ copper cables or fiber and using a 10/25 GbE switch. If using fiber, use an optical to SFP adapter.

Connect Port 3 via switch

Use this configuration if you need an extra port for workload traffic and port level redundancy isn't required.



1. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. If connecting the computer directly to your device (without going through a switch), use an Ethernet crossover cable or a USB Ethernet adapter.
2. Connect PORT 2 to the internet using a 1-GbE RJ-45 network cable.
3. Connect PORT 3 on both the devices via SFP+ copper cables or fiber and using a 10/25 GbE switch. If using fiber, use an optical to SFP adapter.

NOTE

For Network Function Manager deployments, make sure that PORT 5 and PORT 6 are connected. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).

Next steps

In this tutorial, you learned about Azure Stack Edge Pro GPU topics such as how to:

- Unpack the device
- Rack the device
- Cable the device

Advance to the next tutorial to learn how to connect to your device.

[Connect Azure Stack Edge Pro](#)

Tutorial: Connect to Azure Stack Edge Pro with GPU

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you can connect to your Azure Stack Edge Pro device with an onboard GPU by using the local web UI.

The connection process can take around 5 minutes to complete.

This tutorial describes how you can connect to the local web UI on the two nodes of your Azure Stack Edge device.

The connection process can take around 10-15 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Connect to a physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Pro GPU device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro](#).
- You've run the Azure Stack Network Readiness Checker tool to verify that your network meets Azure Stack Edge requirements. For instructions, see [Check network readiness for Azure Stack Edge devices](#).

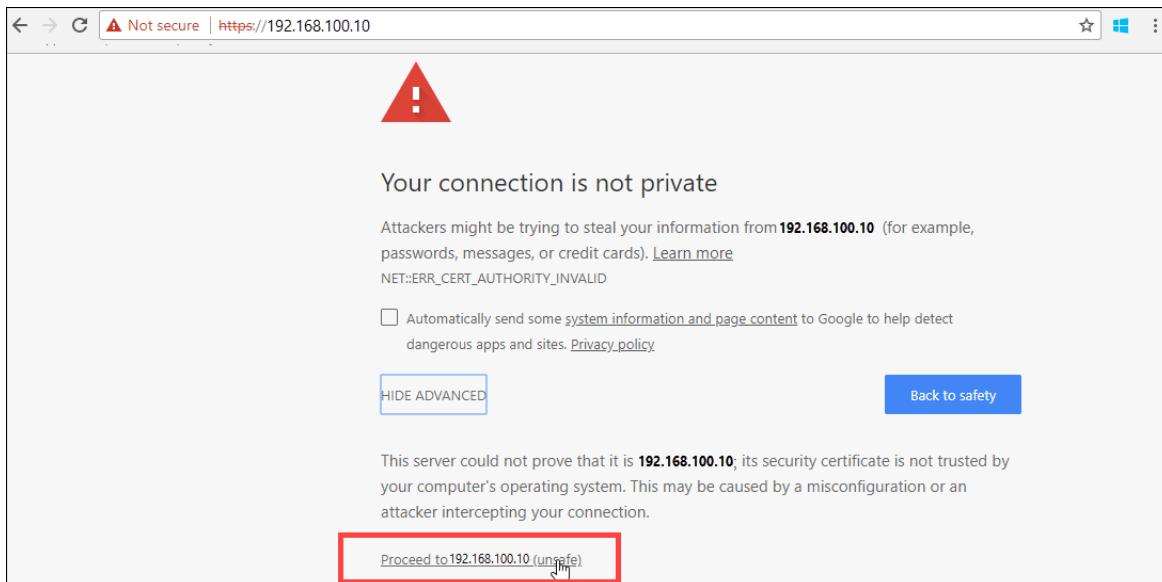
Connect to the local web UI setup

1. Configure the Ethernet adapter on your computer to connect to the Azure Stack Edge Pro device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
2. Connect the computer to PORT 1 on your device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter.

The backplane of the device may look slightly different depending on the exact model you have received. Use the illustrations in [Cable your device](#) to identify Port 1 on your device.

3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>. This action may take a few minutes after you've turned on the device.

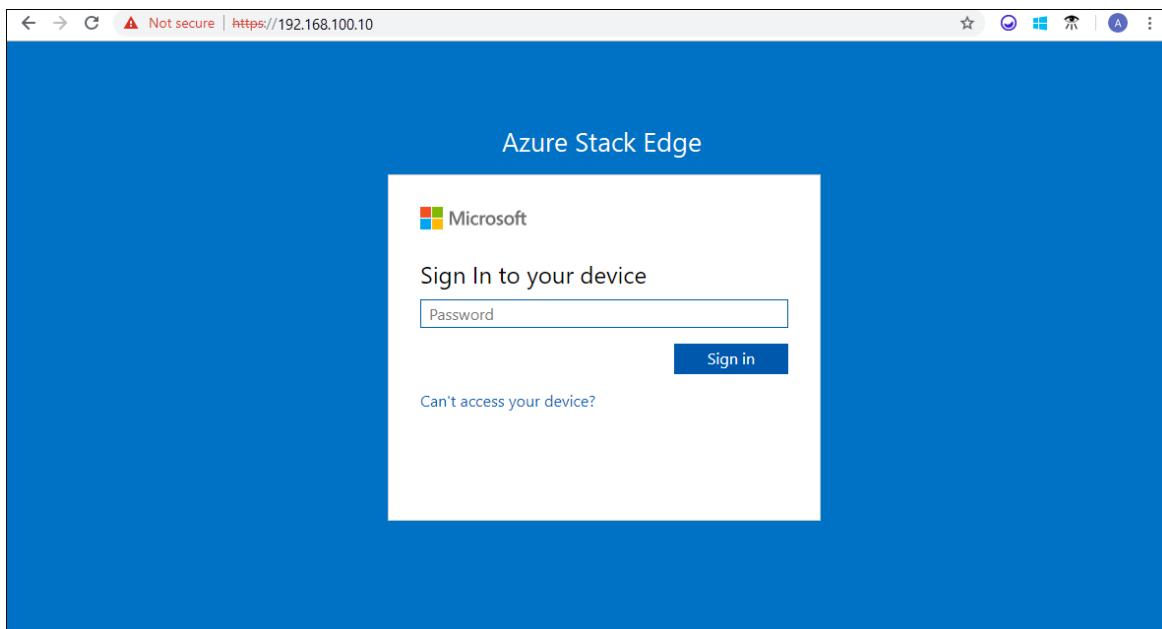
You see an error or a warning indicating that there is a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters.

You're now at the **Overview** page of your device. The next step is to configure the network settings for your device.

1. Configure the Ethernet adapter on your computer to connect to the first node of your Azure Stack Edge device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.

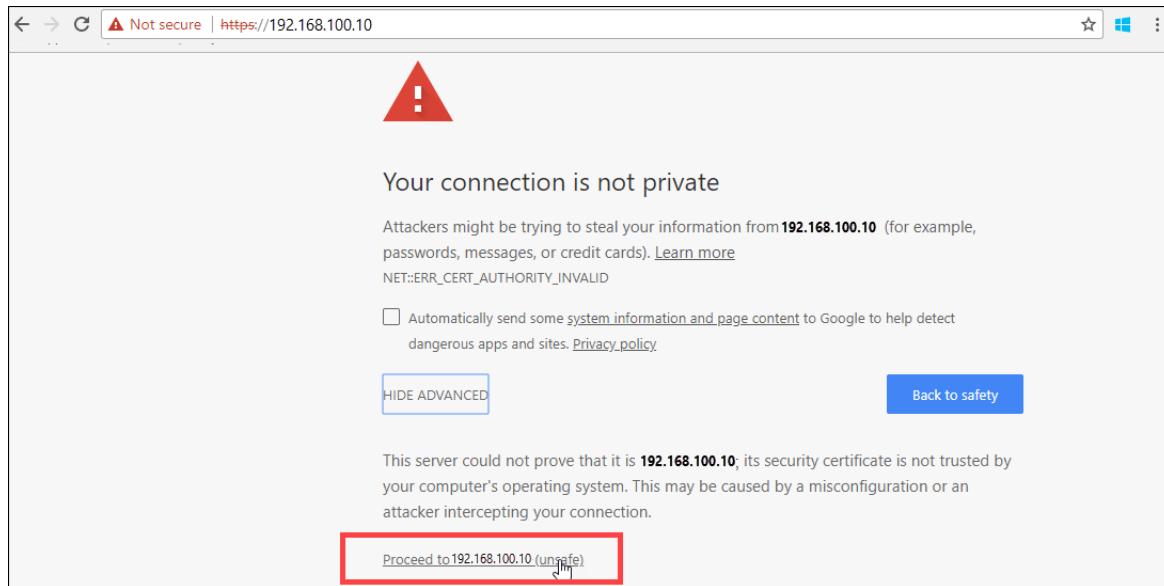
2. Connect the computer to PORT 1 on the first node of your 2-node device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter.

The backplane of the device may look slightly different depending on the exact model you have received. Use the illustrations in [Cable your device](#) to identify Port 1 on your device.

3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>.

This action may take a few minutes after you've turned on the device.

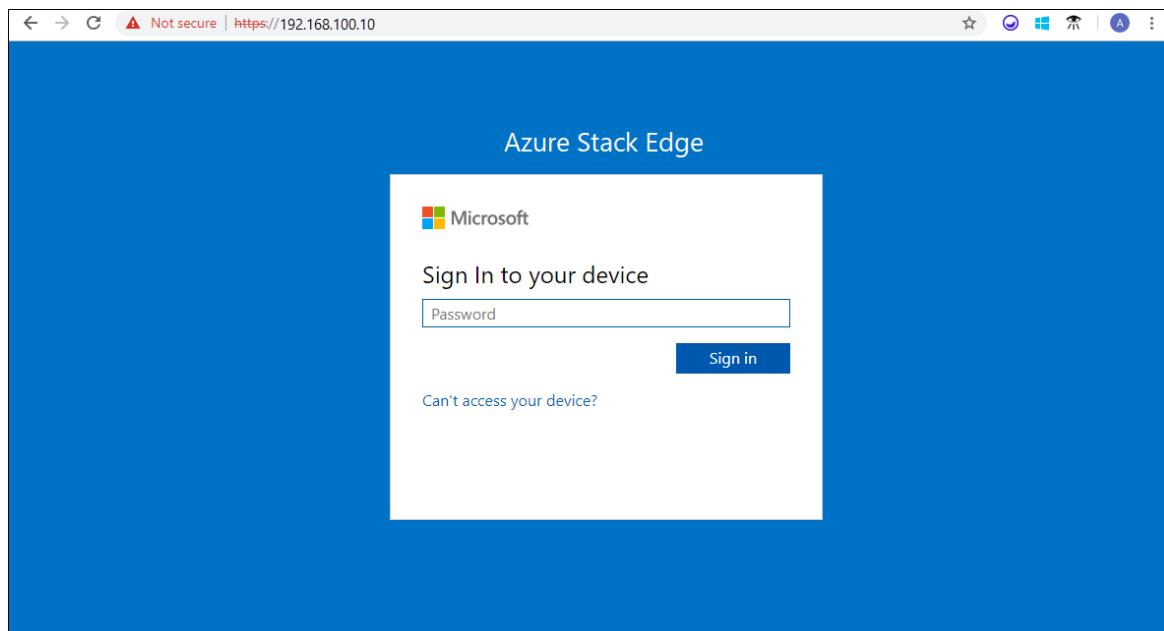
You see an error or a warning indicating that there is a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters. You're now at the **Overview** page in the local web UI of the first node of your 2-node device.

7. Repeat the above steps to connect to the second node of your 2-node device.

The next step is to configure the network settings for your device.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Connect to a physical device

To learn how to configure network settings on your Azure Stack Edge Pro device, see:

[Configure network](#)

Tutorial: Configure network for Azure Stack Edge Pro with GPU

9/21/2022 • 20 minutes to read • [Edit Online](#)

This tutorial describes how to configure network for your Azure Stack Edge Pro device with an onboard GPU by using the local web UI.

The connection process can take around 20 minutes to complete.

This tutorial describes how to configure network for your two-node Azure Stack Edge Pro GPU device by using the local web UI.

The procedure can take around 45 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure network
- Configure advanced networking
- Configure web proxy
- Validate network settings

- Prerequisites
- Select device setup type
- Configure network and network topology on both nodes
- Get authentication token for prepared node
- Configure cluster witness and add prepared node
- Configure virtual IP settings for Azure Consistent Services and NFS
- Configure advanced networking
- Configure web proxy
- Validate network settings

Prerequisites

Before you configure and set up your Azure Stack Edge Pro device with GPU, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro](#).
- You've connected to the local web UI of the device as detailed in [Connect to Azure Stack Edge Pro](#)

Configure setup type

1. Go to the **Get started** page.
2. In the **Set up a single node device** tile, select **Start**.

The screenshot shows the 'Get started' page of the Azure Stack Edge Pro local web interface. The left sidebar contains navigation links for Overview, Configuration (with 'Get started' highlighted), Maintenance, and other device management options. The main content area is titled 'Get started' and displays three configuration tasks:

- Set up a single node device**: Configure a single node device. A 'Start' button is present.
- Set up a 2-node cluster (Preview)**: Set up a node for a 2-node cluster. Recommended for high availability. A 'Start' button is present.
- Prepare a node for clustering (Preview)**: Ready this node if you initiated cluster creation from another node, and want to add this node to that cluster. Recommended for high availability. A 'Start' button is present.

Configure network

Your **Get started** page displays the various settings that are required to configure and activate the physical device with the Azure Stack Edge service.

Follow these steps to configure the network for your device.

1. In the local web UI of your device, go to the **Get started** page.
2. On the **Network** tile, select **Configure**.

The screenshot shows the 'Get started with standalone device setup' page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Get started with standalone device setup' and displays four configuration sections:

- 1 Network**:
 - Network : ⚠ Needs setup
 - Compute network : [Not configured](#)
 - Web proxy : [Not configured](#)
- 2 Device setup**:
 - Device : ⚠ Needs setup
 - Update : [Configured with defaults](#)
 - Time : [Configured with defaults](#)
- 3 Security**:
 - Certificates : [Configured with defaults](#)
- 4 Activation**: Use the activation key from the Azure portal to activate your device. A 'Activate' button is present at the bottom.

[Go back to select setup type](#)

On your physical device, there are six network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3, PORT 4, PORT 5, and PORT 6 are all 25-Gbps network interfaces that can also serve as

10-Gbps network interfaces. PORT 1 is automatically configured as a management-only port, and PORT 2 to PORT 6 are all data ports. For a new device, the **Network** page is as shown below.

The screenshot shows the 'Network' configuration page for an Azure Stack Edge Pro (1 GPU). The left sidebar lists various configuration options: Overview, Get started (selected), Network (highlighted with a red border), Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, and Certificates. The main pane displays the 'Network interfaces' section, which includes a table with columns: Name, IP addresses, Subnet mask, Gateway, and MAC addresses. The table data is as follows:

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	-
Port 2	-	-	-	-
Port 3	-	-	-	-
Port 4	-	-	-	-
Port 5	-	-	-	-
Port 6	-	-	-	-

At the bottom of the main pane, there is a link labeled 'Go back to Get started'.

3. To change the network settings, select a port and in the right pane that appears, modify the IP address, subnet, gateway, primary DNS, and secondary DNS.

- If you select Port 1, you can see that it is preconfigured as static.



Network settings (Port 1)

* Set IP

* IP settings

* Subnet mask

255.255.255.0 ✓

Gateway

Primary DNS

Secondary DNS

Serial number	IP address	MAC address
1CYMHQ2	192.168.100.10 ✓	34-80-0D-05-3A-D7

- If you select Port 2, Port 3, Port 4, or Port 5, all of these ports are configured as DHCP by default.

Network settings (Port 5)

* Set IP

* IP settings

Subnet mask

255.255.0.0

Gateway

Primary DNS

192.168.0.1

Secondary DNS

Serial number	IP address	MAC address
---------------	------------	-------------

1CYMHQ2	192.168.7.66	0C-42-A1-79-41-9D
---------	--------------	-------------------

- By default for all the ports, it is expected that you'll set an IP. If you decide not to set an IP for a network interface on your device, you can set the IP to **No** and then **Modify** the settings.

Network settings (Port 2)

* Set IP

Enable this option if you don't want to specify an IP address for this port.

Serial number	IP address	MAC address
---------------	------------	-------------

1CYMHQ2	<input type="text"/>	34-80-0D-05-3A-D6
---------	----------------------	-------------------

As you configure the network settings, keep in mind:

- Make sure that Port 5 and Port 6 are connected for Network Function Manager deployments. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).
- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.
- If DHCP isn't enabled, you can assign static IPs if needed.
- You can configure your network interface as IPv4.
- Serial number for any port corresponds to the node serial number.

NOTE

If you need to connect to your device from an outside network, see [Enable device access from outside network](#) for additional network settings.

Once the device network is configured, the page updates as shown below.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	F4-E9-D4-7C-47-03
Port 2	10.126.77.42	255.255.248.0	10.126.72.1	F4-E9-D4-7C-47-02
Port 3	192.168.6.10	255.255.0.0	-	F4-E9-D4-7C-47-01
Port 4	192.168.6.9	255.255.0.0	-	F4-E9-D4-7C-47-00
Port 5	192.168.6.4	255.255.0.0	-	0C-42-A1-79-42-6D
Port 6	192.168.6.3	255.255.0.0	-	0C-42-A1-79-42-6C

NOTE

We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has activated with the service, and then change. You can then view the IPs of all the adapters in the [Device properties](#) in the Azure portal for your service.

After you have configured and applied the network settings, select [Next: Advanced networking](#) to configure compute network.

Configure virtual switches

Follow these steps to add or delete virtual switches and virtual networks.

1. In the local UI, go to **Advanced networking** page.
2. In the **Virtual switch** section, you'll add or delete virtual switches. Select **Add virtual switch** to create a new switch.

Name	Network interface	Intent
vsswitch-port2	Port 2	-

Name	Enabled for Kubernetes	Virtual switch	VLAN ID	Network	Gateway	Subnet mask
vsnet		vsswitch-port2				

3. In the **Network settings** blade, if using a new switch, provide the following:

- Provide a name for your virtual switch.
- Choose the network interface on which the virtual switch should be created.
- If deploying 5G workloads, set **Supports accelerated networking** to Yes.
- Select **Apply**. You can see that the specified virtual switch is created.

Name	Network interface	Intent
vsswitch-port2	Port 2	-

Name	Enabled for Kubernetes	Virtual switch	VLAN ID	Network	Gateway	Subnet mask
vsnet		vsswitch-port2				

4. You can create more than one switch by following the steps described earlier.

5. To delete a virtual switch, under the **Virtual switch** section, select **Delete virtual switch**. When a virtual switch is deleted, the associated virtual networks will also be deleted.

You can now create virtual networks and associate with the virtual switches you created.

Configure virtual networks

You can add or delete virtual networks associated with your virtual switches. To add a virtual switch, follow these steps:

- In the local UI on the **Advanced networking** page, under the **Virtual network** section, select **Add virtual network**.
- In the **Add virtual network** blade, input the following information:

- a. Select a virtual switch for which you want to create a virtual network.
- b. Provide a **Name** for your virtual network.
- c. Enter a **VLAN ID** as a unique number in 1-4094 range. The VLAN ID that you provide should be in your trunk configuration. For more information on trunk configuration for your switch, refer to the instructions from your physical switch manufacturer.
- d. Specify the **Subnet mask** and **Gateway** for your virtual LAN network as per the physical network configuration.
- e. Select **Apply**. A virtual network is created on the specified virtual switch.

Add virtual network

Add a virtual network to a specified virtual switch on your device.

* Virtual switch
vSwitch1

* Name
vNet1

* VLAN ID
200

* Subnet mask
255.255.248.0

* Gateway
192.68.100.1

Apply

3. To delete a virtual network, under the **Virtual network** section, select **Delete virtual network** and select the virtual network you want to delete.
4. Select **Next: Kubernetes** > to next configure your compute IPs for Kubernetes.

Configure compute IPs

Follow these steps to configure compute IPs for your Kubernetes workloads.

1. In the local UI, go to the **Kubernetes** page.
2. From the dropdown select a virtual switch that you will use for Kubernetes compute traffic.
3. Assign **Kubernetes node IPs**. These static IP addresses are for the Kubernetes VMs.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. For a 1-node device, provide a minimum of 2 free, contiguous IPv4 addresses.

IMPORTANT

- Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).
- DHCP mode is not supported for Kubernetes node IPs. If you plan to deploy IoT Edge/Kubernetes, you must assign static Kubernetes IPs and then enable IoT role. This will ensure that static IPs are assigned to Kubernetes node VMs.
- If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are on the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

4. Assign **Kubernetes external service IPs**. These are also the load-balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside of the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

5. Select **Apply**.

Compute virtual switch

Specify a virtual switch for Kubernetes compute traffic.

* Virtual switch

vSwitch2 (Port 2)



Compute IPs

For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs

Enter a contiguous range of 2 static IPs for your device.

10.126.77.50 - 10.126.77.51



Kubernetes external service IPs

Specify the static IP range for services exposed outside of Kubernetes cluster.

10.126.77.52 - 10.126.77.53



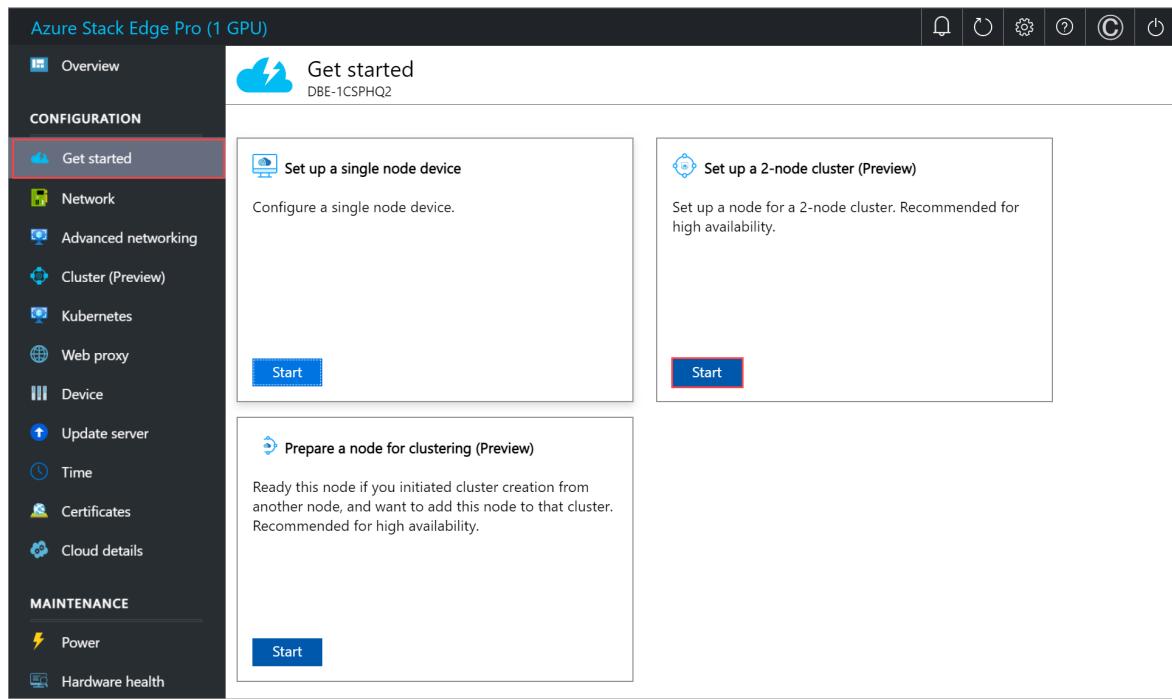
Apply

6. The configuration takes a couple minutes to apply and you may need to refresh the browser.

7. Select **Next: Web proxy** to configure web proxy.

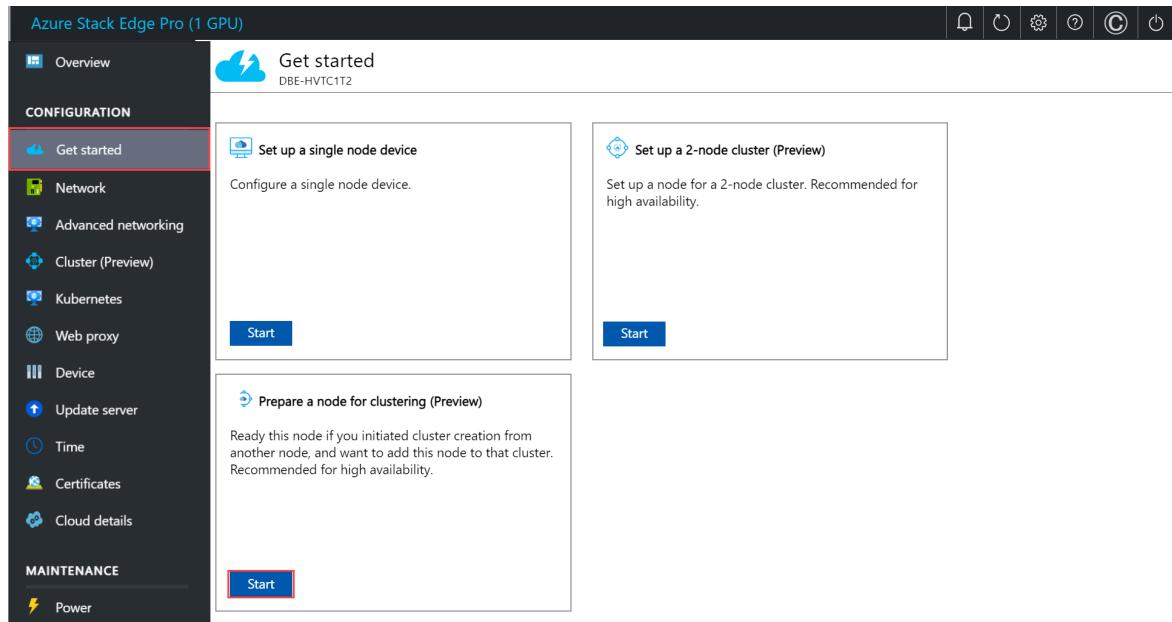
Configure setup type

1. In the local UI for one of the devices, go to the **Get started** page.
2. In the **Set up a 2-node cluster** tile, select **Start**.



3. In the local UI for the second device, go to the **Get started** page.

4. In the **Prepare a node for clustering (Preview)** tile, select **Start**.



Configure network, topology

You'll configure network as well as network topology on both the nodes. These steps can be done in parallel. The cabling on both nodes should be identical and should conform with the network topology you choose.

Configure network on first node

To configure the network for a 2-node device, follow these steps on the first node of the device:

1. In the local UI of the first node, in the **Network** tile, select **Needs setup**.

Get started

Network

Network : **Needs setup**

Network topology : **Needs setup**

Configure cluster

Cluster : **Not configured**

Cluster witness : **Not configured**

Device setup

Compute network : **Not configured**

Web proxy : **Not configured**

Device : **Needs setup**

Update : **Configured with defaults**

Time : **Configured with defaults**

Security

Certificates : **Configured with defaults**

2. In the **Network** page, configure the IP addresses for your network interfaces. On your physical device, there are six network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3, PORT 4, PORT 5, and PORT 6 are all 25-Gbps network interfaces that can also serve as 10-Gbps network interfaces. PORT 1 is automatically configured as a management-only port, and PORT 2 to PORT 6 are all data ports. For a new device, the **Network settings** page is as shown below.

Network

To complete this step, you will need to configure another port.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	34-80-0D-C7-0A-3B
Port2	-	-	-	-	34-80-0D-C7-0A-3A
Port3	-	-	-	-	34-80-0D-C7-0A-39
Port4	-	-	-	-	34-80-0D-C7-0A-38
Port5	-	-	-	-	0C-42-A1-C0-E4-19
Port6	-	-	-	-	0C-42-A1-C0-E4-18

Apply

< Back to Get started | Next: Advanced networking >

To change the network settings, select a port and in the right pane that appears, modify the IP address, subnet, gateway, primary DNS, and secondary DNS. You can configure your network interface as IPv4.

Network settings (Port 2)

* IP settings

DHCP Static **Static**

* Subnet mask
255.255.248.0 ✓

Gateway
10.126.72.1 ✓

Primary DNS
10.50.50.10 ✓

Secondary DNS
10.50.50.100 ✓

Serial number	IP address	MAC address
1CSPHQ2	10.126.72.50 ✓	34-80-0D-C7-0A-3A

Modify

By default for all the ports, it is expected that you'll set an IP. If you decide not to set an IP for a network interface on your device, you can set the IP to **No** and then **Modify** the settings.

Network settings (Port 2)

* Set IP

Yes No **No**

Enable this option if you don't want to specify an IP address for this port.

Serial number	IP address	MAC address
1CYMHQ2		34-80-0D-05-3A-D6

Modify

As you configure the network settings, keep in mind:

- Make sure that Port 5 and Port 6 are connected for Network Function Manager deployments. For more information, see [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).
- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP

address, subnet, gateway, and DNS are automatically assigned. If DHCP isn't enabled, you can assign static IPs if needed.

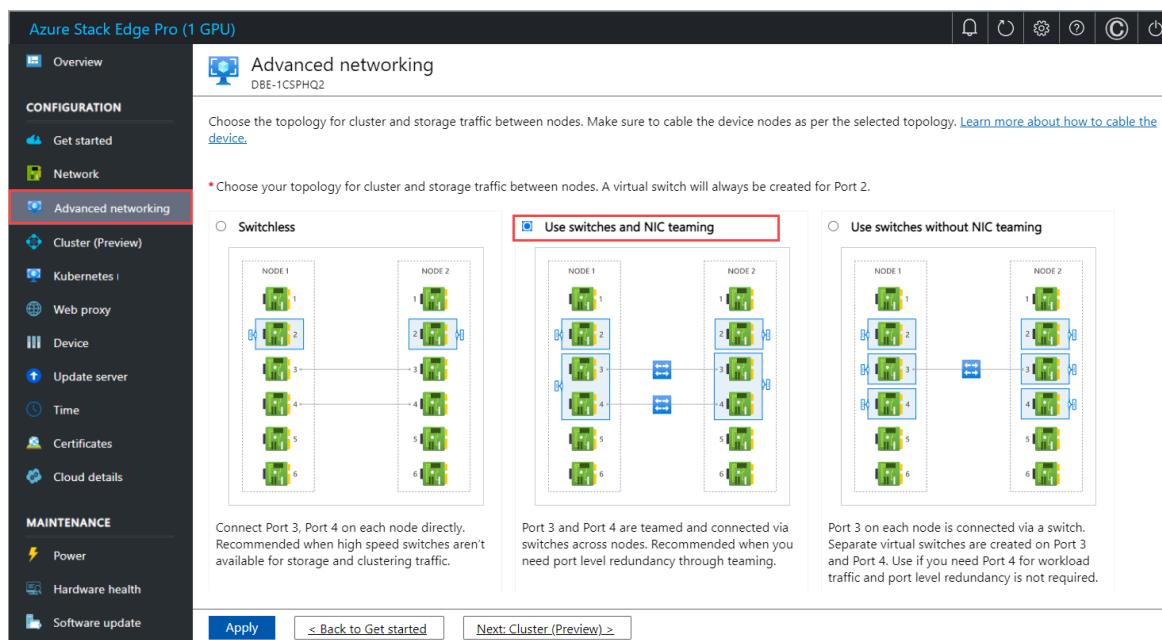
- On 25-Gbps interfaces, you can set the RDMA (Remote Direct Access Memory) mode to iWarp or RoCE (RDMA over Converged Ethernet). Where low latencies are the primary requirement and scalability is not a concern, use RoCE. When latency is a key requirement, but ease-of-use and scalability are also high priorities, iWARP is the best candidate.
- Serial number for any port corresponds to the node serial number.

Once you apply the network settings, select **Next: Advanced networking** > to configure your network topology.

Configure network topology on first node

1. In the **Advanced networking** page, choose the topology for cluster and the storage traffic between nodes from the following options:

- **Switchless.** Use this option when high-speed switches aren't available for storage and clustering traffic.
- **Use switches and NIC teaming.** Use this option when you need port level redundancy through teaming. NIC Teaming allows you to group two physical ports on the device node, Port 3 and Port 4 in this case, into two software-based virtual network interfaces. These teamed network interfaces provide fast performance and fault tolerance in the event of a network interface failure. For more information, see [NIC teaming on Windows Server](#).
- **Use switches without NIC teaming.** Use this option if you need an extra port for workload traffic and port level redundancy is not required.



2. Make sure that your node is cabled as per the selected topology.
3. Select **Apply**.
4. You'll see a **Confirm network setting** dialog. This dialog reminds you to make sure that your node is cabled as per the network topology you selected. Once you choose the network cluster topology, you can't change this topology without a device reset. Select **Yes** to confirm the network topology.

Confirm network setting

Before you proceed, make sure that you've cabled your devices as per the cluster topology. Once you choose the cluster topology, you can't change it without a device reset.

Are you sure you want to continue?

Yes

No

The network topology setting takes a few minutes to apply and you see a notification when the settings are successfully applied.

- Once the network topology is applied, the **Network** page updates. For example, if you selected network topology that uses switches and NIC teaming, you will see that on a device node, a virtual switch **vSwitch1** is created at Port 2 and another virtual switch, **vSwitch2** is created on Port 3 and Port 4. Port 3 and Port 4 are teamed and then on the teamed network interface, two virtual network interfaces are created, **vPort3** and **vPort4**. The same is true for the second device node. The teamed network interfaces are then connected via switches.

The screenshot shows the Network configuration page for the first device node (DBE-1CSPHQ2). It displays a table of network interfaces with columns: Name, Virtual switch, IP addresses, Subnet mask, Gateway, and MAC addresses. The table includes entries for Port1, vEthernet (vSwitch1)vSwitch1 (Port2), vEthernet (vPort3) (Port3, Port4), vEthernet (vPort4) (Port3, Port4), Port5, and Port6. A red box highlights the table area. At the bottom, there are navigation buttons: < Back to Get started and Next: Cluster >.

Name	Virtual switch	IP addresses	Subnet mask	Gateway	MAC addresses
Port1	-	192.168.100.10	255.255.255.0	-	34-80-0D-C7-0A-3B
vEthernet (vSwitch1)vSwitch1 (Port2)	vSwitch1 (Port2)	10.126.77.125	255.255.248.0	10.126.72.1	34-80-0D-C7-0A-3A
vEthernet (vPort3)	vSwitch2 (Port3, Port4)	192.168.1.123	255.255.0.0	-	34-80-0D-C7-0A-39
vEthernet (vPort4)	vSwitch2 (Port3, Port4)	192.168.1.107	255.255.0.0	-	34-80-0D-C7-0A-3B
Port5	-	192.168.6.196	255.255.0.0	-	0C-42-A1-C0-E4-19
Port6	-	192.168.6.160	255.255.0.0	-	0C-42-A1-C0-E4-18

You'll now configure the network and the network topology of the second node.

Configure network on second node

You'll now prepare the second node for clustering. You'll first need to configure the network. Follow these steps in the local UI of the second node:

- On the **Prepare a node for clustering** page, in the **Network** tile, select **Needs setup**.

The screenshot shows the 'Prepare a node for clustering' page. The left sidebar has 'Get started' selected. The main area has two tiles: 'Network' (status: Needs setup) and 'Get authentication token' (description: Get a token to authenticate this node to form a 2-node cluster if you started cluster creation on another node). At the bottom, there is a 'Prepare node' button and a link to 'Go back to select setup type'.

Configure network topology on second node

1. Make sure that the second node is cabled as per the topology you selected for the first node. In the **Network** page, choose and **Apply** the same topology that you selected for the first node.

The screenshot shows the 'Network' configuration page for an Azure Stack Edge Pro (1 GPU). The 'Advanced networking' section is active. It displays three network topology options:

- Switchless:** Shows two nodes connected directly via their respective port 2 and port 3. Recommended when high speed switches aren't available for storage and clustering traffic.
- Use switches and NIC teaming:** (Selected) Shows two nodes connected via a central switch. Port 3 and Port 4 are teamed and connected via switches across nodes. Recommended when you need port level redundancy through teaming.
- Use switches without NIC teaming:** Shows two nodes connected via a central switch. Port 3 on each node is connected via a switch. Separate virtual switches are created on Port 3 and Port 4. Use if you need Port 4 for workload traffic and port level redundancy is not required.

At the bottom, there are 'Apply' and '< Back to Get started' buttons.

2. Select **Back to get started**.

Get authentication token

You'll now get the authentication token that will be needed when adding this node to form a cluster. Follow these steps in the local UI of the second node:

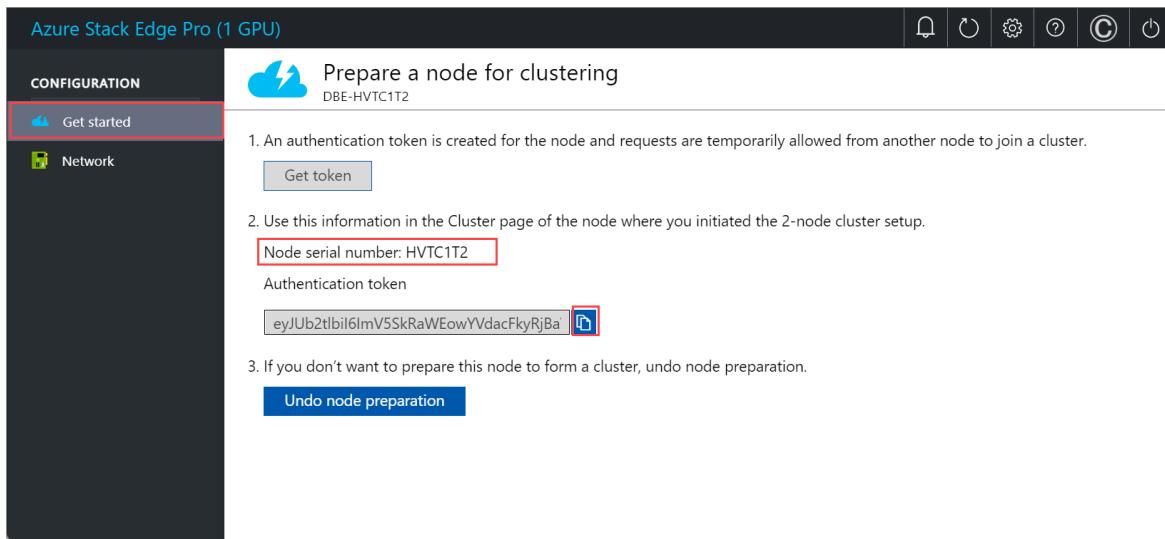
1. On the **Prepare a node for clustering** page, in the **Get authentication token** tile, select **Prepare node**.

The screenshot shows the 'Prepare a node for clustering (Preview)' page. The 'Get started' section is active. It contains two main tiles:

- 1 Network:** Status: Configured. Details: Network and Network topology both configured.
- 2 Get authentication token:** Status: Configured. Description: Get a token to authenticate this node to form a 2-node cluster if you started cluster creation on another node. Contains a 'Prepare node' button.

At the bottom, there is a 'Go back to select setup type' link.

2. Select **Get token**.
3. Copy the node serial number and the authentication token. You will use this information when you add this node to the cluster on the first node.



Configure cluster

To configure the cluster, you'll need to establish a cluster witness and then add a prepared node. You'll also need to configure virtual IP settings so that you can connect to a cluster as opposed to a specific node.

Configure cluster witness

You'll now create a cluster witness. A cluster witness helps establish quorum for a two-node device if a node goes down. To learn about quorum, see [Understanding quorum](#).

A cluster witness can be:

- **Cloud witness** if you use an Azure Storage account to provide a vote on cluster quorum. A cloud witness uses Azure Blob Storage to read or write a blob file and then uses it to arbitrate in split-brain resolution.

Use cloud witness when you have internet access. For more information on cloud witness, see [Deploy a cloud witness for Failover cluster](#).

- **File share witness** if you use a local SMB file share to provide a vote in the cluster quorum. Use a file share witness if all the servers in a cluster have spotty internet connectivity or can't use disk witness as there aren't any shared drives.

Use file share witness if you're in an IT environment with other machines and file shares. For more information on file share witness, see [Deploy a file share witness for Failover cluster](#).

Before you create a cluster witness, make sure that you've reviewed the cluster witness requirements.

Follow these steps to configure the cluster witness.

Configure cloud witness

1. In the local UI of the first node, go to the [Cluster \(Preview\)](#) page. Under **Cluster witness type**, select **Modify**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview) - highlighted with a red box), Kubernetes, Web proxy, Device, Update server, Time, Certificates, and Cloud details. The Maintenance section includes Power, Hardware health, Software update, Password change, and Device reset. The main content area is titled 'Cluster (Preview)' and shows 'DBE-1CSPHQ2'. It has a note about adding prepared nodes or modifying cluster witness. The 'Cluster witness' section is expanded, showing 'Witness type' set to 'None' and a 'Modify' button. Below is the 'Existing nodes' section with an 'Add node' and 'Replace node' button. A table lists one node: Serial number 1CSPHQ2, Version 2.2.1842.4304, and Status Healthy. An 'Apply' button is at the bottom. Navigation buttons at the bottom are '< Back to Get started' and 'Next: Web proxy >'.

2. In the **Modify cluster witness** blade, enter the following inputs.
 - a. Choose the **Witness type** as **Cloud**.
 - b. Enter the **Azure Storage account name**.
 - c. Specify Storage account authentication from Access key or SAS token.
 - d. If you chose Access key as the authentication mechanism, enter the Access key of the Storage account, Azure Storage container where the witness lives, and the service endpoint.
 - e. Select **Apply**.

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

Cloud

* Azure Storage account name

myasestoracca

* Storage account authentication

Access key SAS token

* Access key

<Access key>

Azure Storage container

myasecont

Service endpoint

core.windows.net

Apply

Configure local witness

1. In the local UI of the first node, go to the Cluster page. Under Cluster witness type, select Modify.

The screenshot shows the Azure Stack Edge Pro (1 GPU) management interface. The left sidebar contains navigation links for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Help (Feedback, Report a problem). The main content area is titled "Cluster (Preview)" and shows the cluster name "1CSPHQ2CL". It includes sections for "Cluster witness" (Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share. Witness type: None, Modify button), "Existing nodes" (Add new nodes or view existing nodes, Add node, Replace node buttons, table with one row: Serial number 1CSPHQ2, Version 2.2.1842.4304, Status Healthy, Apply button), and navigation links "< Back to Get started" and "Next: Web proxy >".

2. In the **Modify cluster witness** blade, enter the following inputs.

- a. Choose the **Witness type** as **Local**.
- b. Enter the file share path as **//server/fileshare** format.
- c. Select **Apply**.

X

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

File share

* Share path

//clusterserver/clusterwitnessshare

Credentials required

* Username

mysmbuser1

* Password

Apply

Add prepared node to cluster

You'll now add the prepared node to the first node and form the cluster. Before you add the prepared node, make sure the networking on the incoming node is configured in the same way as that of this node where you initiated cluster creation.

1. In the local UI of the first node, go to the Cluster page. Under Existing nodes, select Add node.

2. In the Add node blade, input the following information for the incoming node:
 - a. Provide the serial number for the incoming node.
 - b. Enter the authentication token for the incoming node.
3. Select Validate & add. This step takes a few minutes.

You see a notification when the node is successfully validated.

- The node is now ready to join the cluster. Select **Apply**. The cluster creation takes several minutes. Once the cluster is created, the page updates to show both the nodes are added.

Configure virtual IPs

For Azure consistent services and NFS, you'll also need to define a virtual IP that allows you to connect to a clustered device as opposed to a specific node. A virtual IP is an available IP in the cluster network and any client connecting to the cluster network on the two-node device should be able to access this IP.

For Azure Consistent Services

For Azure Consistent Services, follow these steps to configure virtual IP.

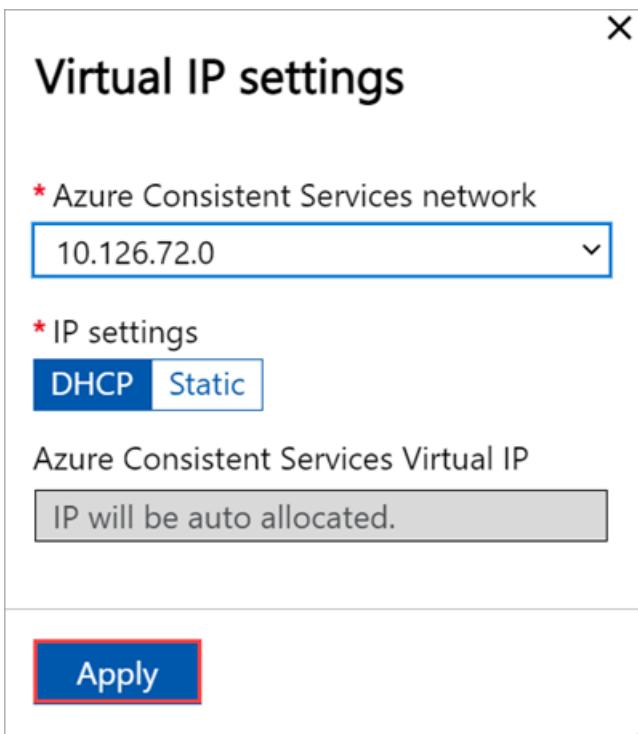
- In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Azure Consistent Services**.

Name	Network	Virtual IP
Azure Consistent Services	-	
Network File System	-	

- In the **Virtual IP settings** blade, input the following.

- From the dropdown list, select the **Azure Consistent Services network**.
- Choose IP settings from **DHCP** or **static**.
- If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the Azure Consistent Services network that you specified. If you selected DHCP, a virtual IP is automatically picked from the Azure Consistent Services network that you selected.

- Select **Apply**.



For Network File System

For clients connecting via NFS protocol to the two-node device, follow these steps to configure virtual IP.

- In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Network File System**.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestoracctalkohli	myasecont	core.windows.net

Serial number	Version	Status
1CSPHQ2	2.2.1842.4304	Healthy
HVTC1T2	2.2.1842.4304	Healthy

Name	Network	Virtual IP
Azure Consistent Services	10.126.72.0	10.126.77.178
Network File System	-	-

- In the **Virtual IP settings** blade, input the following.

- a. From the dropdown list, select the **NFS network**.
 - b. Choose IP settings from **DHCP** or **Static**.
 - c. If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the NFS network that you specified. If you selected DHCP, a virtual IP is automatically picked from the NFS network that you selected.
3. Select **Apply**.

The dialog box has a title 'Virtual IP settings' and an 'X' button in the top right corner. It contains the following fields:

- * Network File System network: A dropdown menu showing '10.126.72.0'.
- * IP settings: A radio button group with 'DHCP' selected and 'Static' as an option.
- Network File System Virtual IP: A note saying 'IP will be auto allocated.'
- Apply: A red-bordered button at the bottom.

NOTE

Virtual IP settings are required. If you do not configure this IP, you will be blocked when configuring the **Device settings** in the next step.

Configure virtual switches

After the cluster is formed and configured, you can now create new virtual switches.

IMPORTANT

On a two-node cluster, compute should only be configured on a virtual switch.

1. In the local UI, go to **Advanced networking** page.
2. In the **Virtual switch** section, add or delete virtual switches. Select **Add virtual switch** to create a new switch.

3. In the **Network settings** blade, if using a new switch, provide the following:

- Provide a name for your virtual switch.
- Choose the network interface on which the virtual switch should be created.
- If deploying 5G workloads, set **Supports accelerated networking** to Yes.
- Select **Apply**.

4. The configuration will take a couple minutes to apply and once the virtual switch is created, the list of virtual switches updates to reflect the newly created switch. You can see that the specified virtual switch is created and enabled for compute.

5. You can create more than one switch by following the steps described earlier.

6. To delete a virtual switch, under the **Virtual switch** section, select **Delete virtual switch**. When a virtual switch is deleted, the associated virtual networks will also be deleted.

You can next create and associate virtual networks with your virtual switches.

Configure virtual network

You can add or delete virtual networks associated with your virtual switches. To add a virtual network, follow these steps:

- In the local UI on the **Advanced networking** page, under the **Virtual network** section, select **Add virtual network**.

2. In the **Add virtual network** blade, input the following information:
 - a. Select a virtual switch for which you want to create a virtual network.
 - b. Provide a **Name** for your virtual network.
 - c. Enter a **VLAN ID** as a unique number in 1-4094 range. The VLAN ID that you provide should be in your trunk configuration. For more information on trunk configuration for your switch, refer to the instructions from your physical switch manufacturer.
 - d. Specify the **Subnet mask** and **Gateway** for your virtual LAN network as per the physical network configuration.
 - e. Select **Apply**.

Add virtual network

Add a virtual network to a specified virtual switch on your device.

*Virtual switch
vSwitch1

*Name
vNet1

*VLAN ID
200

*Subnet mask
255.255.248.0

*Gateway
192.68.100.1

Apply

3. To delete a virtual network, under the **Virtual network** section, select **Delete virtual network** and select the virtual network you want to delete.

Select **Next: Kubernetes** > to next configure your compute IPs for Kubernetes.

Configure compute IPs

After the virtual switches are created, you can enable these switches for Kubernetes compute traffic.

1. In the local UI, go to the **Kubernetes** page.
2. From the dropdown list, select the virtual switch you want to enable for Kubernetes compute traffic.
3. Assign **Kubernetes node IPs**. These static IP addresses are for the Kubernetes VMs.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. For a 1-node device, provide a minimum of 2 free, contiguous IPv4 addresses. For a two-node cluster, provide a minimum of 3 free, contiguous IPv4 addresses.

IMPORTANT

- Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).
- DHCP mode is not supported for Kubernetes node IPs. If you plan to deploy IoT Edge/Kubernetes, you must assign static Kubernetes IPs and then enable IoT role. This will ensure that static IPs are assigned to Kubernetes node VMs.

4. Assign **Kubernetes external service IPs**. These are also the load-balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside of the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

5. Select **Apply**.

Compute virtual switch

Specify a virtual switch for Kubernetes compute traffic.

* Virtual switch

vSwitch2 (Port 2)



Compute IPs

For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs

Enter a contiguous range of 2 static IPs for your device.

10.126.77.50 - 10.126.77.51



Kubernetes external service IPs

Specify the static IP range for services exposed outside of Kubernetes cluster.

10.126.77.52 - 10.126.77.53



Apply

6. The configuration takes a couple minutes to apply and you may need to refresh the browser.

Configure web proxy

This is an optional configuration. Although web proxy configuration is optional, if you use a web proxy, you can configure it on this page only.

IMPORTANT

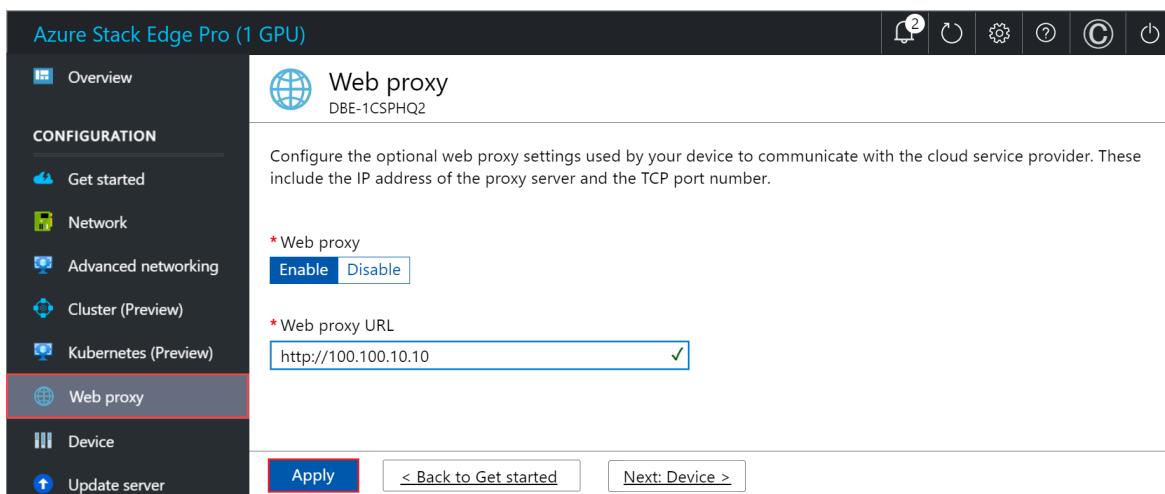
- Proxy-auto config (PAC) files are not supported. A PAC file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.
- Transparent proxies work well with Azure Stack Edge Pro. For non-transparent proxies that intercept and read all the traffic (via their own certificates installed on the proxy server), upload the public key of the proxy's certificate as the signing chain on your Azure Stack Edge Pro device. You can then configure the proxy server settings on your Azure Stack Edge device. For more information, see [Bring your own certificates and upload through the local UI](#).

1. On the **Web proxy settings** page, take the following steps:

a. In the **Web proxy URL** box, enter the URL in this format:

`http://host-IP address or FQDN:Port number`. HTTPS URLs are not supported.

b. To validate and apply the configured web proxy settings, select **Apply**.



Validate network settings

Follow these steps to validate your network settings.

1. Go to the **Diagnostic tests** page and select the tests as shown below.
2. Select **Run test**.

Azure Stack Edge Pro (1 GPU)

Test	Category	Status	Recommended actions
Azure portal connectivity	Azure connectivity	-	-
Azure storage account credentials	Azure connectivity	-	-
Azure container read/write	Azure connectivity	-	-
Azure consistent services health check	Azure consistent services	-	-
Certificates	Certificates	-	-
<input checked="" type="checkbox"/> Azure Edge compute runtime	Edge compute	-	-
Disks	Hardware	-	-
Power Supply Units	Hardware	-	-
<input checked="" type="checkbox"/> Network interfaces	Hardware	-	-
CPUs	Hardware	-	-
Compute acceleration	Hardware	-	-
<input checked="" type="checkbox"/> Network settings	Networking	-	-
<input checked="" type="checkbox"/> Internet connectivity	Networking	-	-
System software	Software	-	-
Time sync	Time	-	-
Software update readiness	Update	-	-

Run test

- Review test results to ensure that status shows **Healthy** for each test that was run.

Azure Stack Edge Pro (1 GPU)

Test	Category	Status	Recommended actions
Azure consistent services health check	Azure consistent services	-	-
Certificates	Certificates	-	-
<input checked="" type="checkbox"/> Azure Edge compute runtime	Edge compute	✓ Healthy	-
Disks	Hardware	-	-
Power Supply Units	Hardware	-	-
<input checked="" type="checkbox"/> Network interfaces	Hardware	✓ Healthy	-
CPUs	Hardware	-	-
Compute acceleration	Hardware	-	-
<input checked="" type="checkbox"/> Network settings	Networking	✓ Healthy	-
<input checked="" type="checkbox"/> Internet connectivity	Networking	✓ Healthy	-
System software	Software	-	-
Time sync	Time	-	-
Software update readiness	Update	-	-

Run test

- If a test fails, select **Recommended actions** on the test results page, implement the recommended change, and then rerun the test. For example, the dialog below shows recommended actions if the Azure Edge compute runtime test fails.

Recommended actions

To resolve the issue(s), complete the following:

- The 'Node' IPs provided for kubernetes cluster '192.168.167.132' are already in use on the network. Provide unused IPs to resolve the issue. If the problem persists, contact Microsoft Support.
- The 'Service' IPs provided for kubernetes cluster '192.168.167.128,192.168.167.129,192.168.167.130' are already in use on the network. Provide unused IPs to resolve the issue. If the problem persists, contact Microsoft Support.

OK

5. After network settings are validated and all tests return **Healthy** status, proceed to the device settings page.

Repeat the above steps for the second node of the 2-node device. Make sure to use the same web proxy settings on both the device nodes.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Configure network
- Enable compute network
- Configure web proxy
- Validate network settings
- Prerequisites
- Select device setup type
- Configure network on both nodes
- Get authentication token for prepared node
- Configure cluster witness and add prepared node
- Configure virtual IP settings for Azure Consistent Services and NFS
- Configure advanced networking
- Configure web proxy
- Validate network settings

To learn how to set up your Azure Stack Edge Pro GPU device, see:

[Configure device settings](#)

Tutorial: Configure the device settings for Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how to configure device related settings for your Azure Stack Edge Pro GPU device. You can set up your device name, update server, and time server via the local web UI.

The device settings can take around 5-7 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

Prerequisites

Before you configure device related settings on your Azure Stack Edge Pro device GPU, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro](#).
 - You've configured network and enabled and configured compute network on your device as detailed in [Tutorial: Configure network for Azure Stack Edge Pro with GPU](#).

Configure device settings

Follow these steps to configure device related settings:

1. In the local web UI for your device, go to the **Device** page.
2. Enter a **Name** for your device. The name must contain from 1 to 13 characters and can have letter, numbers, and hyphens.
3. Provide a **DNS domain** for your device. This domain is used to set up the device as a file server.
4. To validate and apply the configured device settings, select **Apply**.

Azure Stack Edge Pro (1 GPU)

Device
DBE-1CSPHQ2

To complete this step, you will need to apply the desired device name and DNS domain.

Device name

Assign a friendly name and DNS domain for the device.

* Name: DBE-1CSPHQ2

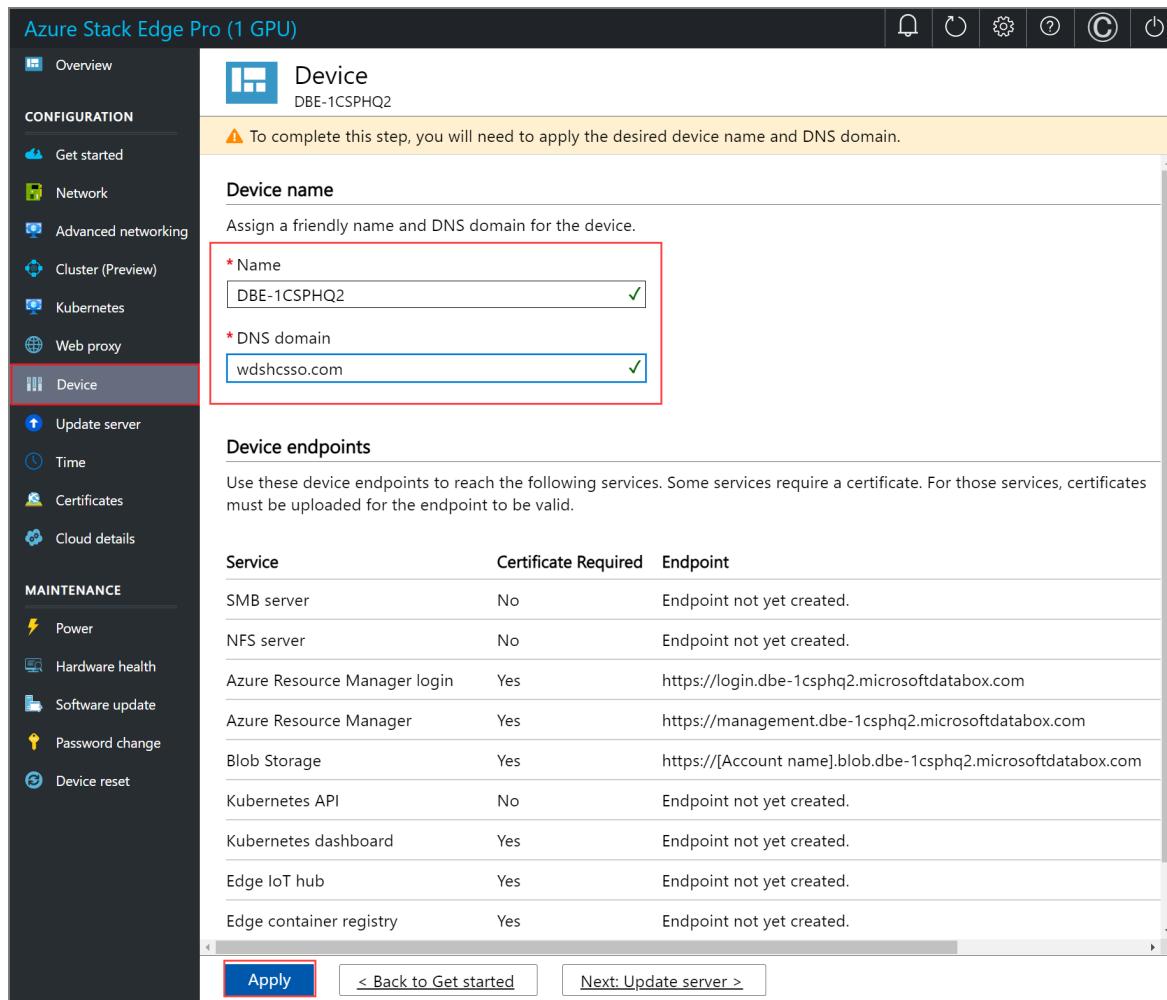
* DNS domain: wdshcsso.com

Device endpoints

Use these device endpoints to reach the following services. Some services require a certificate. For those services, certificates must be uploaded for the endpoint to be valid.

Service	Certificate Required	Endpoint
SMB server	No	Endpoint not yet created.
NFS server	No	Endpoint not yet created.
Azure Resource Manager login	Yes	https://login.dbe-1csphq2.microsoftdatobox.com
Azure Resource Manager	Yes	https://management.dbe-1csphq2.microsoftdatobox.com
Blob Storage	Yes	https://[Account name].blob.dbe-1csphq2.microsoftdatobox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	Yes	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.
Edge container registry	Yes	Endpoint not yet created.

Apply [< Back to Get started](#) [Next: Update server >](#)



When the device name and the DNS domain are changed, the SMB endpoint is created.

If you've changed the device name and the DNS domain, the automatically generated self-signed certificates on the device won't work. You'll need to regenerate device certificates or bring your own certificates.

Warning

If you change the device name or DNS domain, you must upload new certificates for the device to work properly.

Apply

Cancel

5. After the settings are applied, select **Next: Update server**.

The screenshot shows the 'Device' configuration page. On the left sidebar, the 'Device' option is selected and highlighted with a red box. In the main content area, there's a 'Device name' section where 'DBE-1CSPHQ2' is entered in the 'Name' field and 'wdshcsso.com' is entered in the 'DNS domain' field, both with green checkmarks. Below this is a 'Device endpoints' section containing a table of service endpoints. The first row, 'SMB server', has its entire row highlighted with a red box. The table includes columns for Service, Certificate Required, and Endpoint. Other services listed include NFS server, Azure Resource Manager login, Azure Resource Manager, Blob Storage, Kubernetes API, Kubernetes dashboard, Edge IoT hub, and Edge container registry. At the bottom of the page are 'Apply', '< Back to Get started', and 'Next: Update server >' buttons.

Configure update

1. On the **Update** page, you can now configure the location from where to download the updates for your device.

- You can get the updates directly from the **Microsoft Update server**.

The screenshot shows the 'Update server' configuration page. The 'Update server' section title is displayed above a dropdown menu labeled 'Select update server type' which contains 'Microsoft Update (default)'. The left sidebar shows the 'Update server' option selected and highlighted with a red box. At the bottom of the page are 'Apply', '< Back to Get started', and 'Next: Time >' buttons.

You can also choose to deploy updates from the **Windows Server Update services (WSUS)**. Provide the path to the WSUS server.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. The left sidebar has a red box around the 'Update server' tab. The main content area is titled 'Update server' and shows the configuration for a Windows Server Update Services update server. The 'Server URI' field contains 'http://wsusupdate.microsoft.com:8080' with a green checkmark. Buttons at the bottom include 'Apply', '< Back to Get started', and 'Next: Time >'.

NOTE

If a separate Windows Update server is configured and if you choose to connect over *https* (instead of *http*), then signing chain certificates required to connect to the update server are needed. For information on how to create and upload certificates, go to [Manage certificates](#).

2. Select **Apply**.
3. After the update server is configured, select **Next: Time**.

Configure time

Follow these steps to configure time settings on your device.

IMPORTANT

Though the time settings are optional, we strongly recommend that you configure a primary NTP and a secondary NTP server on the local network for your device. If local server is not available, public NTP servers can be configured.

NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

1. On the **Time** page, you can select the time zone, and the primary and secondary NTP servers for your device.
 - a. In the **Time zone** drop-down list, select the time zone that corresponds to the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. In the **Primary NTP server** box, enter the primary server for your device or accept the default value of time.windows.com.
Ensure that your network allows NTP traffic to pass from your datacenter to the internet.
 - c. Optionally, in the **Secondary NTP server** box, enter a secondary server for your device.
 - d. To validate and apply the configured time settings, select **Apply**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. The left sidebar has a red box around the 'Time' option under the 'CONFIGURATION' section. The main content area is titled 'Time' and shows the device's current time as '2/15/2022 10:30:26 AM'. It includes fields for 'Time zone' (set to '(UTC-08:00) Pacific Time (US & Canada)'), 'Primary NTP server' (set to 'time.windows.com'), and 'Secondary NTP server' (set to '100.10.10.10'). There are 'Apply' and 'Next: Certificates >' buttons at the bottom.

2. After the settings are applied, select **Next: Certificates**.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

To learn how to configure certificates for your Azure Stack Edge Pro device, see:

[Configure certificates](#)

Tutorial: Configure certificates for your Azure Stack Edge Pro with GPU

9/21/2022 • 8 minutes to read • [Edit Online](#)

This tutorial describes how you can configure certificates for your Azure Stack Edge Pro device with an onboard GPU by using the local web UI.

This tutorial describes how you can configure certificates for your 2-node Azure Stack Edge Pro GPU device by using the local web UI.

The time taken for this step can vary depending on the specific option you choose and how the certificate flow is established in your environment.

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Pro device with GPU, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro GPU](#).
- If you plan to bring your own certificates:
 - You should have your certificates ready in the appropriate format including the signing chain certificate. For details on certificate, go to [Manage certificates](#)
 - If your device is deployed in Azure Government and not deployed in Azure public cloud, a signing chain certificate is required before you can activate your device. For details on certificate, go to [Manage certificates](#).

Configure certificates for device

1. Open the **Certificates** page in the local web UI of your device. This page will display the certificates available on your device. The device is shipped with self-signed certificates, also referred to as the device certificates. You can also bring your own certificates.
2. If you didn't change the device name or DNS domain when you [configured device settings earlier](#), and you don't want to use your own certificates, you don't need any configuration on this page. You just need to verify that the status of all the certificates shows as valid on this page.

Name	Status	Issued by	Subject	Expiration date	Thumbprint	Download
Signing Chain	⚠ Not present -	-	-	-	-	-
Node (1HWF613)	✓ Active	CN=1hwf613.microsoftdatabox.com	CN=1hwf613.microsoftdatabox.com	6/9/2022	B3DB2E36B410F694FC76565EEADA0D8F3FOA...	Download
Azure Resource Manager	✓ Active	CN=management.dbe-1hwf613.microsoftd...	CN=management.dbe-1hwf613.microsoftd...	6/9/2022	A62299C8DEB213EF11033E133B25D9895EE...	Download
Blob storage	✓ Active	CN=dbe-1hwf613.microsoftdatabox.com	CN=dbe-1hwf613.microsoftdatabox.com	6/9/2022	CF5D93B6FB16C1312DCF0D3E5D0664382B...	Download
Local web UI	✓ Active	CN=dbe-1hwf613.microsoftdatabox.com	CN=dbe-1hwf613.microsoftdatabox.com	6/9/2022	CF5D93B6FB16C1312DCF0D3E5D0664382B...	Download
IoT device root CA	⚠ Not present -	-	-	-	-	-
IoT device CA	⚠ Not present -	-	-	-	-	-
IoT device Key	⚠ Not present -	-	-	-	-	-

Go back to Get started

You're ready to [Activate your device](#) with the existing device certificates.

- Follow these steps only if you've changed the device name or the DNS domain for your device. In these instances, the status of your device certificates will be **Not valid**. That's because the device name and DNS domain in the certificates' `subject name` and `subject alternative` settings are out of date.

Select a certificate to view status details.

Name	Status	Expiration date	Thu
Node (3Q7LHQ2)	⚠ Not valid	9/4/2022	B53
Azure Resource Manager	⚠ Not valid	9/4/2022	3BD
Blob storage	⚠ Not valid	9/4/2022	E55
Local web UI	⚠ Not valid	9/4/2022	E55
IoT device root CA	⚠ Not present	-	-
IoT device CA	⚠ Not present	-	-
IoT device Key	⚠ Not present	-	-

Local web UI has following errors:-
 • Certificate with subject name CN=dbe-3q7lhq2.microsoftdatabox.com does not have the correct subject name or subject alternative names for Appliance Endpoint certificate. Check the certificate you have uploaded and if needed bring in a new certificate.

< Back to Get started | Next: Cloud details >

- If you've changed the device name or DNS domain of your device, and you don't provide new certificates, **activation of the device will be blocked**. To use a new set of certificates on your device, choose one of the following options:

- Generate all the device certificates.** Select this option, and then complete the steps in [Generate device certificates](#), if you plan to use automatically generated device certificates and need to generate new device certificates. You should only use these device certificates for testing, not with production workloads.
- Bring your own certificates.** Select this option, and then do the steps in [Bring your own certificates](#), if you want to use your own signed endpoint certificates and the corresponding signing chains. **We recommend that you always bring your own certificates for production workloads.**
- You can choose to bring some of your own certificates and generate some device certificates. The **Generate all the device certificates** option only regenerates the device certificates.

- When you have a full set of valid certificates for your device, the device is ready for activation. Select [Back to Get started](#) to proceed to the next deployment step, [Activate your device](#).

1. Open the Certificates page in the local web UI of your device. This page will display the certificates available on your device. The device is shipped with self-signed certificates, also referred to as the device certificates. You can also bring your own certificates.
2. If you didn't change the device name or DNS domain when you [configured device settings earlier](#), and you don't want to use your own certificates, you don't need any configuration on this page. You just need to verify that the status of all the certificates shows as valid on this page.

Name	Status	Issued by	Subject	Expiration date	Thumbprint	Download
Signing Chain	Not present -	-	-	-	-	-
Node (1HWF613)	Active	CN=1hwf613.microsoftdatobox.com	CN=1hwf613.microsoftdatobox.com	6/9/2022	B3DB2E36B410F694FC76565EEADA0D8F3F0A...	Download
Azure Resource Manager	Active	CN=management.dbe-1hwf613.microsoftd...	CN=management.dbe-1hwf613.microsoftd...	6/9/2022	A62299C8DEB213EF11033E133825D9895EE...	Download
Blob storage	Active	CN=dbe-1hwf613.microsoftdatobox.com	CN=dbe-1hwf613.microsoftdatobox.com	6/9/2022	CF5D93B6FB16C1312DCF0D3E5D0664382B...	Download
Local web UI	Active	CN=dbe-1hwf613.microsoftdatobox.com	CN=dbe-1hwf613.microsoftdatobox.com	6/9/2022	CF5D93B6FB16C1312DCF0D3E5D0664382B...	Download
IoT device root CA	Not present -	-	-	-	-	-
IoT device CA	Not present -	-	-	-	-	-
IoT device Key	Not present -	-	-	-	-	-

You're ready to [Activate your device](#) with the existing device certificates.

3. Follow these steps only if you've changed the device name or the DNS domain for your device. In these instances, the status of your device certificates will be **Not valid**. That's because the device name and DNS domain in the certificates' `subject name` and `subject alternative` settings are out of date.

Select a certificate to view status details.

Name	Status	Expiration date	Thu
Node (3Q7LHQ2)	Not valid	9/4/2022	B53
Azure Resource Manager	Not valid	9/4/2022	3BD
Blob storage	Not valid	9/4/2022	E55
Local web UI	Not valid	9/4/2022	E55
IoT device root CA	Not present	-	-
IoT device CA	Not present	-	-
IoT device Key	Not present	-	-

4. If you've changed the device name or DNS domain of your device, and you don't provide new certificates, **activation of the device will be blocked**. To use a new set of certificates on your device, choose one of the following options:

- **Generate all the device certificates.** Select this option, and then complete the steps in [Generate device certificates](#), if you plan to use automatically generated device certificates and need to generate new device certificates. You should only use these device certificates for testing, not with production workloads.
- **Bring your own certificates.** Select this option, and then do the steps in [Bring your own certificates](#), if you want to use your own signed endpoint certificates and the corresponding

signing chains. We recommend that you always bring your own certificates for production workloads.

- You can choose to bring some of your own certificates and generate some device certificates. The **Generate all the device certificates** option only regenerates the device certificates.
5. When you have a full set of valid certificates for your device, the device is ready for activation. Select **< Back to Get started** to proceed to the next deployment step, [Activate your device](#).

Generate device certificates

Follow these steps to generate device certificates.

Use these steps to regenerate and download the Azure Stack Edge Pro GPU device certificates:

1. In the local UI of your device, go to **Configuration > Certificates**. Select **Generate certificates**.

Name	Status	Expiration date	Thumbprint
Node (3Q7LHQ2)	⚠️ Not valid	9/4/2022	B534D2434DDCEA51B438B2A15E509080DC8472C
Azure Resource Manager	⚠️ Not valid	9/4/2022	3BDC2519CF5BD346E2F9BD9D2C2D3B657EAB44E5
Blob storage	⚠️ Not valid	9/4/2022	E55E86DB93B96ED98C929A2CC6614B2BE40A5152
Local web UI	⚠️ Not valid	9/4/2022	E55E86DB93B96ED98C929A2CC6614B2BE40A5152
IoT device root CA	⚠️ Not present	-	-
IoT device CA	⚠️ Not present	-	-
IoT device Key	⚠️ Not present	-	-

2. In the **Generate device certificates**, select **Generate**.

Generate certificates

Use device generated certificates only for testing purposes. For production workload, use signed certificates issued by your certificate authority.

To regenerate and apply device certificates, select 'Generate'. After the operation is complete, close and restart the browser to avoid any cache issues.

Generate

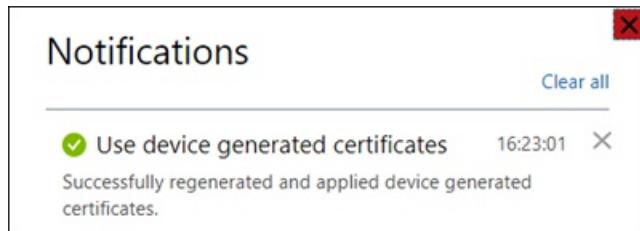
The device certificates are now generated and applied. It takes a few minutes to generate and apply the certificates.

IMPORTANT

While the certificate generation operation is in progress, do not bring your own certificates and try to add those via the **+ Add certificate** option.

You are notified when the operation is successfully completed. To avoid any potential cache issues,

restart your browser.



3. After the certificates are generated:

- The status of all the certificates shows as Valid.

A screenshot of the Azure Stack Edge Pro (1 GPU) portal. The left sidebar shows various configuration options like Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, and Time. The 'Certificates' option is selected and highlighted with a red box. The main content area shows a table of certificates with columns: Name, Status, Expiration date, Thumbprint, and Download. The 'Local web UI' row is highlighted with a red box and its status is listed as 'Valid'. Other entries include Node (3Q7LHQ2), Azure Resource Manager, Blob storage, IoT device root CA, IoT device CA, and IoT device Key.

Name	Status	Expiration date	Thumbprint	Download
Node (3Q7LHQ2)	Valid	9/10/2022	959FBC07373672C550E0C9D527A2B583A8AC7B0E	Download
Azure Resource Manager	Valid	9/10/2022	B62ACCB713FF0EB212F9E222D6183BB114F5A08	Download
Blob storage	Valid	9/10/2022	1FD83836BF61A54CF3005229B56894D23F7630F0	Download
Local web UI	Valid	9/10/2022	F1576C89699EFBF97EF536787EF767FE53624999	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-

- You can select a specific certificate name, and view the certificate details.

A screenshot of the Azure Stack Edge Pro (1 GPU) portal. The left sidebar shows various configuration options like Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, and Time. The 'Certificates' option is selected and highlighted with a red box. The main content area shows a table of certificates with columns: Name, Status, Expiration date, Thumbprint. The 'Local web UI' row is highlighted with a red box and its status is listed as 'Valid'. A 'Certificate details' modal is open on the right side, showing the following information for the 'Local web UI' certificate:
Name: Local web UI
Issued to: CN=myasegpu1.wdshcsso.com
Issued by: CN=myasegpu1.wdshcsso.com
Valid from: 8/10/2020
Valid to: 9/10/2022
Thumbprint: F1576C89699EFBF97EF536787EF767FE53624999

- The **Download** column is now populated. This column has links to download the regenerated certificates.

A screenshot of the Azure Stack Edge Pro (1 GPU) portal. The left sidebar shows various configuration options like Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, and Time. The 'Certificates' option is selected and highlighted with a red box. The main content area shows a table of certificates with columns: Name, Status, Expiration date, Thumbprint, and Download. The 'Local web UI' row is highlighted with a red box and its status is listed as 'Valid'. The 'Download' column for this certificate is also highlighted with a red box, showing four download links.

Name	Status	Expiration date	Thumbprint	Download
Node (3Q7LHQ2)	Valid	9/10/2022	959FBC07373672C550E0C9D527A2B583A8AC7B0E	Download
Azure Resource Manager	Valid	9/10/2022	B62ACCB713FF0EB212F9E222D6183BB114F5A08	Download
Blob storage	Valid	9/10/2022	1FD83836BF61A54CF3005229B56894D23F7630F0	Download
Local web UI	Valid	9/10/2022	F1576C89699EFBF97EF536787EF767FE53624999	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-

4. Select the download link for a certificate and when prompted, save the certificate.

Certificates

Name	Status	Expiration date	Thumbprint	Download
Node (3Q7LHQ2)	Valid	9/10/2022	959FBC07373672C550E0C9D527A2B583A8AC7B0E	Download
Azure Resource Manager	Valid	9/10/2022	B62ACCBBD713FF0EB212F9E222D6183BB114F5A08	Download
Blob storage	Valid	9/10/2022	1FD83836BF61A54CF3005229B56894D23F7630F0	Download
Local web UI	Valid	9/10/2022	F1576C89699EFBF97EF536787EF767FE53624999	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-

5. Repeat this process for all the certificates that you wish to download.

Downloads

Name	Date modified	Type	Size
myasegpu1_Node (3Q7LHQ2).cer	9/10/2020 10:59 AM	Security Certificate	2 KB
myasegpu1_Azure Resource Manager.cer	9/10/2020 10:59 AM	Security Certificate	2 KB
myasegpu1_Blob storage.cer	9/10/2020 10:59 AM	Security Certificate	2 KB
myasegpu1_Local web UI.cer	9/10/2020 10:59 AM	Security Certificate	2 KB

1. In the local UI of your device, go to Configuration > Certificates. Select Generate certificates.

Certificates

Name	Status	Expiration date	Thumbprint	Download
Node (HVTCT1Z)	Not valid	11/11/2023	68E28D1E45656544C8DE59975B190979C2A134DB	Download
Node (1CSPHQ2)	Not valid	11/11/2023	A755667A3FAA0369AAECA1D22148367BF70D93E	Download
Azure Resource Manager	Not valid	11/11/2023	1AAE9DAB38B1543D7A723150F6321E2F679E67CF	Download
Blob storage	Not valid	11/11/2023	D286D61B83AD54CCE110F5EC7FA20C5DF597E6E9	Download
Local web UI	Not valid	11/11/2023	D286D61B83AD54CCE110F5EC7FA20C5DF597E6E9	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

2. In the Generate device certificates, select Generate.

Generate certificates

i Use device generated certificates only for testing purposes. For production workload, use signed certificates issued by your certificate authority.

The 'Generate certificates' does not apply when you bring your own certificates.

To regenerate and apply device certificates, select 'Generate'. After the operation is complete, close and restart the browser to avoid any cache issues.

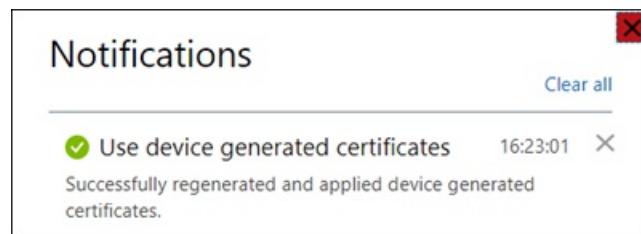
Generate

The device certificates are now generated and applied. It takes a few minutes to generate and apply the certificates.

IMPORTANT

While the certificate generation operation is in progress, do not bring your own certificates and try to add those via the **+ Add certificate** option.

You are notified when the operation is successfully completed. To avoid any potential cache issues, restart your browser.



3. After the certificates are generated:

- The status of all the certificates shows as Valid.

Name	Status	Expiration date	Thumbprint	Download
Node (HVTC1T2)	Valid	11/12/2023	6B3E374C5E2DEAEF68DE1AACD86F0616CE6EDEF8	Download
Node (1CSPHQ2)	Valid	11/12/2023	1161AEF5332E0EC358DC8107E1B1D98A7528A0D9	Download
Azure Resource Manager	Valid	11/12/2023	D27893F421A1E7D7BFEEC1AAC88AF83549550E7	Download
Blob storage	Valid	11/12/2023	539B88272A587BC8B40F3179E9F0A136B57FED98	Download
Local web UI	Valid	11/12/2023	C0B982E0AD469B3EFE1AB940658029B0F4BF1655	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

- You can select a specific certificate name, and view the certificate details.

Certificate details

Name
Local web UI

Issued to
CN=dbe-1csphq2.wdshcsso.com

Issued by
CN=dbe-1csphq2.wdshcsso.com

Valid from
10/12/2021

Valid to
11/12/2023

Thumbprint
C0B982E0AD469B3EFE1AB940658029B0F4BF1655

- The Download column is now populated. This column has links to download the regenerated certificates.

Name	Status	Expiration date	Thumbprint	Download
Node (HVTC1T2)	Valid	11/12/2023	6B3E374C5E2DEAEF68DE1AACD86F0616CE6EDEF8	Download
Node (1CSPHQ2)	Valid	11/12/2023	1161AEF5332E0EC358DC8107E1B1D98A7528A0D9	Download
Azure Resource Manager	Valid	11/12/2023	D27893F421A1E7D7BFEEC1AAC88AF83549550E7	Download
Blob storage	Valid	11/12/2023	539B88272A587BC8B40F3179E9F0A136B57FED98	Download
Local web UI	Valid	11/12/2023	C0B982E0AD469B3EFE1AB940658029B0F4BF1655	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

4. Select the download link for a certificate and when prompted, save the certificate.

Name	Status	Expiration date	Thumbprint	Download
Node (HVTC1T2)	Valid	11/12/2023	D7885B9EC929394EF0FA72C32353ED653D1440E9	Download
Node (1CSPHQ2)	Valid	11/12/2023	58AF2D7556CA217B76E3808D88C6F9CA1B7E81AD	Download
Azure Resource Manager	Valid	11/12/2023	D27893F421A1E7D7BFEEC1AAC88AFB3549550E7	Download
Blob storage	Valid	11/12/2023	D4E0D10BF9C9CB80B6FE54BC7F3C9900A3CB0512	Download
Local web UI	Valid	11/12/2023	BA16151F2A6051E3078B1768DEA3EC3F75A4C63F	Download
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Kubernetes dashboard certificate	Not present	-	-	-
Kubernetes dashboard key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

5. Repeat this process for all the certificates that you wish to download.

The device generated certificates are saved as DER certificates with the following name format:

- <Device name>_<Endpoint name>.cer

These certificates contain the public key for the corresponding certificates installed on the device.

You will need to install these certificates on the client system that you are using to access the endpoints on the Azure Stack Edge device. These certificates establish trust between the client and the device.

To import and install these certificates on the client that you are using to access the device, follow the steps in [Import certificates on the clients accessing your Azure Stack Edge Pro GPU device](#).

If using Azure Storage Explorer, you will need to install certificates on your client in PEM format and you will need to convert the device generated certificates into PEM format.

IMPORTANT

- The download link is only available for the device generated certificates and not if you bring your own certificates.
- You can decide to have a mix of device generated certificates and bring your own certificates as long as other certificate requirements are met. For more information, go to [Certificate requirements](#).

Bring your own certificates

You can bring your own certificates.

- Start by understanding the [Types of certificates](#) that can be used with your Azure Stack Edge device.
- Next, review the [Certificate requirements](#) for each type of certificate.
- You can then [Create your certificates via Azure PowerShell](#) or [Create your certificates via Readiness Checker tool](#).
- Finally, [Convert the certificates to appropriate format](#) so that they are ready to upload on to your device.

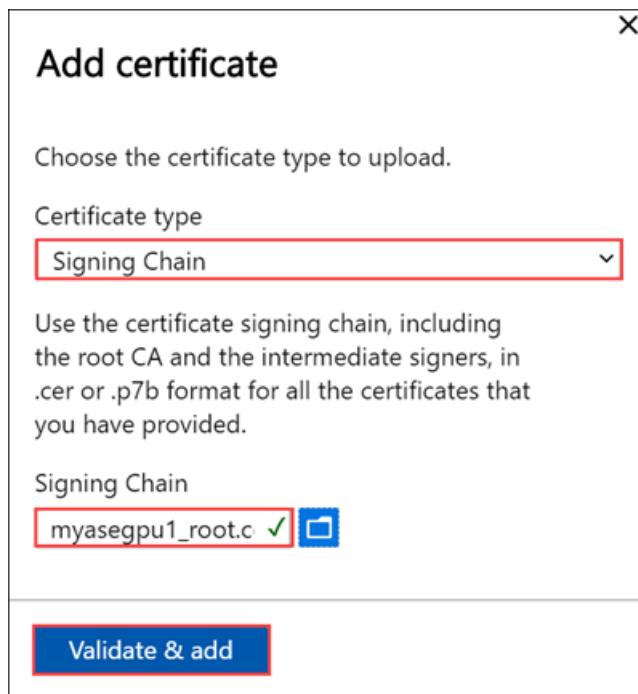
Follow these steps to upload your own certificates including the signing chain.

- To upload certificate, on the [Certificate](#) page, select **+ Add certificate**.

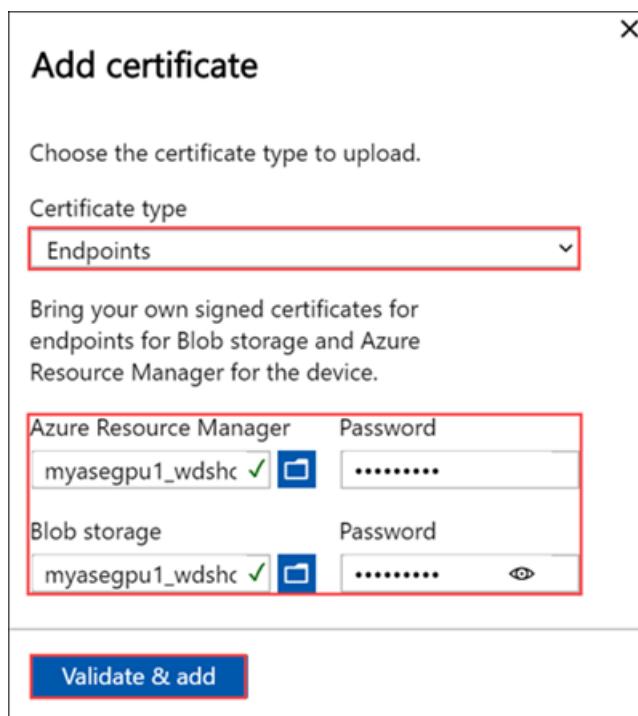
The screenshot shows the 'Certificates' page in the Azure Data Box Gateway interface. On the left, there's a sidebar with various configuration options like Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, and Certificates. The 'Certificates' option is highlighted with a red box. The main area shows a list of existing certificates: Signing Chain (Valid), Signing Chain (Valid), Node (WIN-ICH4FTEGN45) (Valid), and Azure Resource Manager (Valid). A red box highlights the '+ Add certificate' button. To the right, a modal window titled 'Add certificate' is open. It has a dropdown for 'Choose the certificate type to upload' set to 'Signing Chain'. Below it is a section for 'Use the certificate signing chain, including the root CA and the intermediate signers, in .cer or .p7b format for all the certificates that you have provided.' A file input field labeled 'Select a file' is shown. At the bottom of the modal are 'Validate & add' and 'Cancel' buttons.

- You can skip this step if you included all certificates in the certificate path when you [exported certificates in .pfx format](#). If you didn't include all certificates in your export, upload the signing chain, and then select **Validate & add**. You need to do this before you upload your other certificates.

In some cases, you may want to bring a signing chain alone for other purposes - for example, to connect to your update server for Windows Server Update Services (WSUS).



3. Upload other certificates. For example, you can upload the Azure Resource Manager and Blob storage endpoint certificates.



You can also upload the local web UI certificate. After you upload this certificate, you will be required to start your browser and clear the cache. You will then need to connect to the device local web UI.

Add certificate

Choose the certificate type to upload.

Certificate type
Node

Use the node certificates to connect to individual device nodes over a secure channel.

1HWF613	Password
myasegpu1_wdshc	>Password field with eye icon

Validate & add

You can also upload the node certificate.

Add certificate

Choose the certificate type to upload.

Certificate type
Local web UI

Use the local web UI certificate to access the website browser via SSL. After the certificate is applied, close and then restart the browser to avoid any SSL cache issues.

Local web UI	Password
myasegpu1_wdshc	Password field with eye icon

Validate & add

At any time, you can select a certificate and view the details to ensure that these match with the certificate that you uploaded.

Azure Stack Edge Pro (1 GPU)

Certificates

Certificate details

Name	Status	Expiration date
Signing Chain	Valid	9/10/2021
Node (3Q7LHQ2)	Valid	9/10/2021
Azure Resource Manager	Valid	9/10/2021
Blob storage	Valid	9/10/2021
Local web UI	Valid	9/10/2021
IoT device root CA	Not present	-
IoT device CA	Not present	-
IoT device Key	Not present	-

Name
Azure Resource Manager

Issued to
CN=myasegpu1.wdshcsso.com, OU=DIMA, OU=PKI, OU=Mycert, O=Test.Cert Field, C=US

Issued by
CN=DBE SW CA-45, OU=PKI, OU=MoD, O=Test.Cert. Field, C=US

Valid from
9/10/2020

Valid to
9/10/2021

Thumbprint
43158774AA21EDB3A8A4B0B54A1B605D25A63335

< Back to Get started | Next: Cloud details >

The certificate page should update to reflect the newly added certificates.

Name	Status	Expiration date	Thumbprint	Download
Signing Chain	Valid	9/10/2021	D9FDDC9F3FD19E851492965C246E1554E50A145D	-
Node (3Q7LHQ2)	Valid	9/10/2021	43158774AA21EDB3A8A4B0B54A1B605D25A63335	-
Azure Resource Manager	Valid	9/10/2021	43158774AA21EDB3A8A4B0B54A1B605D25A63335	-
Blob storage	Valid	9/10/2021	43158774AA21EDB3A8A4B0B54A1B605D25A63335	-
Local web UI	Valid	9/10/2021	43158774AA21EDB3A8A4B0B54A1B605D25A63335	-
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-

NOTE

Except for Azure public cloud, signing chain certificates are needed to be brought in before activation for all cloud configurations (Azure Government or Azure Stack).

Your device is now ready to be activated. Select < Back to Get started.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device

To learn how to activate your Azure Stack Edge Pro GPU device, see:

[Activate Azure Stack Edge Pro GPU device](#)

Tutorial: Activate Azure Stack Edge Pro with GPU

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you can activate your Azure Stack Edge Pro device with an onboard GPU by using the local web UI.

The activation process can take around 5 minutes to complete.

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Pro device with GPU, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro](#).
 - You've configured the network and compute network settings as detailed in [Configure network, compute network, web proxy](#)
 - You've uploaded your own or generated the device certificates on your device if you changed the device name or the DNS domain via the **Device** page. If you haven't done this step, you'll see an error during the device activation and the activation will be blocked. For more information, go to [Configure certificates](#).
- You have the activation key from the Azure Stack Edge service that you created to manage the Azure Stack Edge Pro device. For more information, go to [Prepare to deploy Azure Stack Edge Pro](#).

Activate the device

1. In the local web UI of the device, go to **Get started** page.
2. On the **Activation** tile, select **Activate**.

The screenshot shows the Azure Stack Edge Pro configuration interface. On the left, a sidebar lists various configuration options: Overview, Configuration (Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy), Device (Update server, Time, Certificates, Cloud details), and Maintenance. The 'Get started' option is selected and highlighted with a red box. The main pane is titled 'Get started with standalone device setup' for the device 'myasedgepu1'. It is divided into four sections: 1 Network, 2 Device setup, 3 Security, and 4 Activation. Section 1 shows Network (Configured), Compute network (Configured), and Web proxy (Not configured). Section 2 shows Device (Configured), Update (Configured with defaults), and Time (Configured with defaults). Section 3 shows Certificates (Configured). Section 4 contains instructions to use the activation key from the Azure portal to activate the device, with a blue 'Activate' button.

3. In the **Activate** pane, enter the **Activation key** that you got in [Get the activation key for Azure Stack Edge Pro](#).
4. Select **Apply**.

The screenshot shows the 'Activate' dialog box. At the top, it says 'Activate'. Below that, there is a descriptive text: 'Activate the device with Azure service. Learn how to [get the activation key](#). After the device is activated, the system checks for and applies any critical updates.' Underneath, there is a field labeled '*** Activation key**' with a placeholder '**<Activation key>**'. A green checkmark icon is positioned to the right of the input field. At the bottom, there is a large blue 'Activate' button.

5. First the device is activated. You're then prompted to download the key file.

Device activated

Successfully activated your device. Download the device key file to a secure location. These keys may be needed to facilitate a future system recovery.

[Download and continue](#)

Select **Download and continue** and save the *device-serial-no.json* file in a safe location outside of the device. **This key file contains the recovery keys for the OS disk and data disks on your device.** These keys may be needed to facilitate a future system recovery.

Here are the contents of the *json* file:

```
{  
  "Id": "<Device ID>",  
  "DataVolumeBitLockerExternalKeys": {  
    "hcsinternal": "<BitLocker key for data disk>",  
    "hcsdata": "<BitLocker key for data disk>"  
},  
  "SystemVolumeBitLockerRecoveryKey": "<BitLocker key for system volume>",  
  "ServiceEncryptionKey": "<Azure service encryption key>"  
}
```

The following table explains the various keys:

FIELD	DESCRIPTION
<code>Id</code>	This is the ID for the device.
<code>DataVolumeBitLockerExternalKeys</code>	These are the BitLocker keys for the data disks and are used to recover the local data on your device.
<code>SystemVolumeBitLockerRecoveryKey</code>	This is the BitLocker key for the system volume. This key helps with the recovery of the system configuration and system data for your device.
<code>ServiceEncryptionKey</code>	This key protects the data flowing through the Azure service. This key ensures that a compromise of the Azure service won't result in a compromise of stored information.

6. Go to the **Overview** page. The device state should show as **Activated**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) Overview page. The left sidebar has a red box around the 'Overview' tab. The main content area is divided into three sections: 'System', 'Device', and 'Configuration'. The 'Device' section has a red box around the 'State' field, which is listed as 'Activated'.

The device activation is complete. You can now add shares on your device.

If you encounter any issues during activation, go to [Troubleshoot activation and Azure Key Vault errors](#).

Deploy workloads

After you've activated the device, the next step is to deploy workloads.

- To deploy VM workloads, see [What are VMs on Azure Stack Edge?](#) and the associated VM deployment documentation.
- To deploy network functions as managed applications:
 - Make sure that you create a Device resource for Azure Network Function Manager (NFM) that is linked to the Azure Stack Edge resource. The device resource aggregates all the network functions deployed on Azure Stack Edge device. For detailed instructions, see [Tutorial: Create a Network Function Manager Device resource \(Preview\)](#).
 - You can then deploy Network Function Manager as per the instructions in [Tutorial: Deploy network functions on Azure Stack Edge \(Preview\)](#).
- To deploy IoT Edge and Kubernetes workloads:
 - You'll need to first configure compute as described in [Tutorial: Configure compute on Azure Stack Edge Pro GPU device](#). This step creates a Kubernetes cluster that acts as the hosting platform for IoT Edge on your device.
 - After a Kubernetes cluster is created on your Azure Stack Edge device, you can deploy application workloads on this cluster via any of the following methods:
 - Native access via `kubectl`
 - IoT Edge
 - Azure Arc

For more information on workload deployment, see [Kubernetes workload management on your Azure Stack Edge device](#).

Next steps

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

To learn how to transfer data with your Azure Stack Edge Pro device, see:

[Transfer data with Azure Stack Edge Pro](#)

System requirements for Azure Stack Edge Pro with GPU

9/21/2022 • 9 minutes to read • [Edit Online](#)

This article describes the important system requirements for your Microsoft Azure Stack Edge Pro GPU solution and for the clients connecting to Azure Stack Edge Pro. We recommend that you review the information carefully before you deploy your Azure Stack Edge Pro. You can refer back to this information as necessary during the deployment and subsequent operation.

The system requirements for the Azure Stack Edge Pro include:

- **Software requirements for hosts** - describes the supported platforms, browsers for the local configuration UI, SMB clients, and any additional requirements for the clients that access the device.
- **Networking requirements for the device** - provides information about any networking requirements for the operation of the physical device.

Supported OS for clients connected to device

Here is a list of the supported operating systems for clients or hosts connected to your device. These operating system versions were tested in-house.

OPERATING SYSTEM/PLATFORM	VERSIONS
Windows Server	2016 2019
Windows	10
SUSE Linux	Enterprise Server 12 (x86_64)
Ubuntu	16.04.3 LTS
CentOS	7.0
Mac OS	10.14.1

Supported protocols for clients accessing device

Here are the supported protocols for clients accessing your device.

PROTOCOL	VERSIONS	NOTES
SMB	2.X, 3.X	SMB 1 isn't supported.
NFS	3.0, 4.1	Mac OS is not supported with NFS v4.1.

Supported Azure Storage accounts

Here is a list of the supported storage accounts for your device.

STORAGE ACCOUNT	NOTES
Classic	Standard
General Purpose	Standard; both V1 and V2 are supported. Both hot and cool tiers are supported.

Supported Edge storage accounts

The following Edge storage accounts are supported with REST interface of the device. The Edge storage accounts are created on the device. For more information, see [Edge storage accounts](#).

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob	

*Page blobs and Azure Files are currently not supported.

Supported local Azure Resource Manager storage accounts

These storage accounts are created via the device local APIs when you are connecting to local Azure Resource Manager. The following storage accounts are supported:

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob, Page Blob	SKU type is Standard_LRS
Premium	GPv1: Block Blob, Page Blob	SKU type is Premium_LRS

Supported storage types

Here is a list of the supported storage types for the device.

FILE FORMAT	NOTES
Azure block blob	
Azure page blob	
Azure Files	

Supported browsers for local web UI

Here is a list of the browsers supported for the local web UI for the virtual device.

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Google Chrome	Latest version	
Microsoft Edge	Latest version	

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Internet Explorer	Latest version	If enhanced security features are enabled, you may not be able to access local web UI pages. Disable enhanced security, and restart your browser.
FireFox	Latest version	
Safari on Mac	Latest version	

Networking port requirements

Port requirements for Azure Stack Edge Pro

The following table lists the ports that need to be opened in your firewall to allow for SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access to your device. *Out* or *outbound* refers to the direction in which your Azure Stack Edge Pro device sends data externally, beyond the deployment, for example, outbound to the internet.

PORt NO.	IN OR OUT	PORT SCOPE	REQUIRED	NOTES
TCP 80 (HTTP)	Out	WAN	No	Outbound port is used for internet access to retrieve updates. The outbound web proxy is user configurable.
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable.
UDP 123 (NTP)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based NTP server.
UDP 53 (DNS)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based DNS server. We recommend using a local DNS server.
TCP 5985 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTP.

Port No.	In or Out	Port Scope	Required	Notes
TCP 5986 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTPS.
UDP 67 (DHCP)	Out	LAN	In some cases See notes	This port is required only if you're using a local DHCP server.
TCP 80 (HTTP)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. Accessing the local UI over HTTP will automatically redirect to HTTPS.
TCP 443 (HTTPS)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. This port is also used to connect Azure Resource Manager to the device local APIs, to connect Blob storage via REST APIs, and to the Security token service (STS) to authenticate via access and refresh tokens.
TCP 445 (SMB)	In	LAN	In some cases See notes	This port is required only if you are connecting via SMB.
TCP 2049 (NFS)	In	LAN	In some cases See notes	This port is required only if you are connecting via NFS.

Port requirements for IoT Edge

Azure IoT Edge allows outbound communication from an on-premises Edge device to Azure cloud using supported IoT Hub protocols. Inbound communication is only required for specific scenarios where Azure IoT Hub needs to push down messages to the Azure IoT Edge device (for example, Cloud To Device messaging).

Use the following table for port configuration for the servers hosting Azure IoT Edge runtime:

Port No.	In or Out	Port Scope	Required	Guidance
----------	-----------	------------	----------	----------

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	GUIDANCE
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound open for IoT Edge provisioning. This configuration is required when using manual scripts or Azure IoT Device Provisioning Service (DPS).

For complete information, go to [Firewall and port configuration rules for IoT Edge deployment](#).

Port requirements for Kubernetes on Azure Stack Edge

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	GUIDANCE
TCP 31000 (HTTPS)	In	LAN	In some cases. See notes.	This port is required only if you are connecting to the Kubernetes dashboard to monitor your device.
TCP 6443 (HTTPS)	In	LAN	In some cases. See notes.	This port is required by Kubernetes API server only if you are using <code>kubectl</code> to access your device.

IMPORTANT

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are in the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your Azure Stack Edge Pro device and the service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. These changes require the network administrator to monitor and update firewall rules for your Azure Stack Edge Pro as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on Azure Stack Edge Pro fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

NOTE

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for gateway feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.com/* https://*.servicebus.windows.net/* https://login.microsoftonline.com https://login.microsoftonline.net	Azure Stack Edge service Azure Service Bus Authentication Service - Azure Active Directory
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.windows.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt https://management.azure.com/	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://azureprofilerfrontdoor.cloudapp.net	Azure Traffic Manager
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
<a href="http://<vault-name>.vault.azure.net:443">http://<vault-name>.vault.azure.net:443	Key Vault

URL patterns for compute feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscl.io	
https://*.azuredcr.io	Personal and third-party container registries (optional)
https://*.azure-devices.net	IoT Hub access (required)
https://*.docker.com	StorageClass (required)

URL patterns for monitoring

Add the following URL patterns for Azure Monitor if you're using the containerized version of the Log Analytics

agent for Linux.

URL PATTERN	PORT	COMPONENT OR FUNCTIONALITY
https://ods.opinsights.azure.com	443	Data ingestion
https://*.oms.opinsights.azure.com	443	Operations Management Suite (OMS) onboarding
https://*.dc.services.visualstudio.com	443	Agent telemetry that uses Azure Public Cloud Application Insights

For more information, see [Network firewall requirements for monitoring container insights](#).

URL patterns for gateway for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.us/* https://*.servicebus.usgovcloudapi.net/* https://login.microsoftonline.us	Azure Data Box Edge/ Azure Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.us	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.usgovcloudapi.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
https://(vault-name).vault.usgovcloudapi.net:443	Key Vault

URL patterns for compute for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscr.com	
https://*.azure-devices.us	IoT Hub access (required)
https://*.azuredcrus	Personal and third-party container registries (optional)

URL patterns for monitoring for Azure Government

Add the following URL patterns for Azure Monitor if you're using the containerized version of the Log Analytics agent for Linux.

URL PATTERN	PORT	COMPONENT OR FUNCTIONALITY
https://ods.opinsights.azure.us	443	Data ingestion
https://*.oms.opinsights.azure.us	443	Operations Management Suite (OMS) onboarding
https://*.dc.services.visualstudio.com	443	Agent telemetry that uses Azure Public Cloud Application Insights

Internet bandwidth

The devices are designed to continue to operate when your internet connection is slow or gets interrupted. In normal operating conditions, we recommend that you use:

- A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
- A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Use WAN throttling to limit your WAN throughput to 64 Mbps or higher.

Compute sizing considerations

Use your experience while developing and testing your solution to ensure there is enough capacity on your Azure Stack Edge Pro device and you get the optimal performance from your device.

Factors you should consider include:

- **Container specifics** - Think about the following.
 - What is your container footprint? How much memory, storage, and CPU is your container consuming?
 - How many containers are in your workload? You could have a lot of lightweight containers versus a few resource-intensive ones.
 - What are the resources allocated to these containers versus what are the resources they are consuming (the footprint)?
 - How many layers do your containers share? Container images are a bundle of files organized into a stack of layers. For your container image, determine how many layers and their respective sizes to calculate resource consumption.
 - Are there unused containers? A stopped container still takes up disk space.
 - In which language are your containers written?
- **Size of the data processed** - How much data will your containers be processing? Will this data

consume disk space or the data will be processed in the memory?

- **Expected performance** - What are the desired performance characteristics of your solution?

To understand and refine the performance of your solution, you could use:

- The compute metrics available in the Azure portal. Go to your Azure Stack Edge resource and then go to **Monitoring > Metrics**. Look at the **Edge compute - Memory usage** and **Edge compute - Percentage CPU** to understand the available resources and how are the resources getting consumed.
- To monitor and troubleshoot compute modules, go to [Debug Kubernetes issues](#).

Finally, make sure that you validate your solution on your dataset and quantify the performance on Azure Stack Edge Pro before deploying in production.

Next step

- [Deploy your Azure Stack Edge Pro](#)

Azure Stack Edge Blob storage requirements

9/21/2022 • 3 minutes to read • [Edit Online](#)

This article lists the versions of the Azure APIs, Azure client libraries, and tools supported with the Azure Stack Edge Blob storage. Azure Stack Edge Blob storage provides blob management functionality with Azure-consistent semantics. This article also summarizes the known Azure Stack Edge Blob storage differences from the Azure Storage services.

We recommend that you review the information carefully before you connect to the Azure Stack Edge Blob storage, and then refer back to it as necessary.

Storage differences

FEATURE	AZURE STORAGE	AZURE STACK EDGE BLOB STORAGE
Azure Files	Cloud-based SMB and NFS file shares supported	Not supported
Storage account type	General-purpose and Azure Blob storage accounts	General-purpose v1 only
Blob name	1,024 characters (2,048 bytes)	880 characters (1,760 bytes)
Block blob maximum size	4.75 TiB (100 MiB X 50,000 blocks)	4.75 TiB (100 MiB x 50,000 blocks) for Azure Stack Edge
Page blob maximum size	8 TiB	1 TiB
Page blob page size	512 bytes	4 KiB

Supported API versions

The following versions of Azure Storage service APIs are supported with Azure Stack Edge Blob storage.

Azure Stack Edge 2.1.1377.2170 onwards

- [2019-02-02](#)
- [2018-11-09](#)
- [2018-03-28](#)
- [2017-11-09](#)
- [2017-07-29](#)
- [2017-04-17](#)
- [2016-05-31](#)
- [2015-12-11](#)
- [2015-07-08](#)
- [2015-04-05](#)

Supported Azure client libraries

For Azure Stack Edge Blob storage, there are specific client libraries and specific endpoint suffix requirements.

The Azure Stack Edge Blob storage endpoints do not have full parity with the latest version of the Azure Blob Storage REST API; see the [supported API versions for Azure Stack Edge](#). For the storage client libraries, you need to be aware of the version that is compatible with the REST API.

Azure Stack Edge 2.1.1377.2170 onwards

The following Azure client library versions are supported for Azure Stack Edge Blob storage.

CLIENT LIBRARY	SUPPORTED VERSION	LINK	ENDPOINT SPECIFICATION
.NET	11.0.0	NuGet package: Common: https://www.nuget.org/packages/Microsoft.Azure.Storage.Common/11.0.0 Blob: https://www.nuget.org/packages/Microsoft.Azure.Storage.Blob/11.0.0 Queue: https://www.nuget.org/packages/Microsoft.Azure.Storage.Queue/11.0.0 GitHub release: https://github.com/Azure/azure-storage-net/releases/tag/v11.0.0	app.config file
Java	12.0.0-preview.3	Maven package: https://mvnrepository.com/artifact/com.azure/azure-storage-file/12.0.0-preview.3 GitHub release: https://github.com/Azure/azure-sdk-for-java/tree/master/sdk/storage	Connection string setup
Node.js	2.8.3	NPM link: https://www.npmjs.com/package/azure-storage (Run: <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <pre>npm install azure-storage@2.7.0</pre> </div>) GitHub release: https://github.com/Azure/azure-storage-node/releases/tag/v2.8.3	Service instance declaration
C++	5.2.0	NuGet package: https://www.nuget.org/packages/wastorage.v140/5.2.0 GitHub release: https://github.com/Azure/azure-storage-cpp/releases/tag/v5.2.0	Connection string setup

Client Library	Supported Version	Link	Endpoint Specification
PHP	1.2.0	GitHub release: Common: https://github.com/Azure/azure-storage-php/releases/tag/v1.2.0-common Blob: https://github.com/Azure/azure-storage-php/releases/tag/v1.2.0-blob Install via Composer (To learn more, See the details below.)	Connection string setup
Python	1.1.0	GitHub release: Common: https://github.com/Azure/azure-storage-python/releases/tag/v1.0.0-common Blob: https://github.com/Azure/azure-storage-python/releases/tag/v1.1.0-blob	Service instance declaration
Ruby	1.0.1	RubyGems package: Common: https://rubygems.org/gems/azure-storage-common/versions/1.0.1 Blob: https://rubygems.org/gems/azure-storage-blob/versions/1.0.1 GitHub release: Common: https://github.com/Azure/azure-storage-ruby/releases/tag/v1.0.1-common Blob: https://github.com/Azure/azure-storage-ruby/releases/tag/v1.0.1-blob	Connection string setup

Install the PHP client via Composer - Current

To install the PHP client via Composer:

1. Create a file named composer.json in the root of the project with following code (example uses Azure Storage Blob service).

```
{
  "require": {
    "Microsoft/azure-storage-blob": "1.2.0"
  }
}
```

2. Download `composer.phar` to the project root.

3. Run: `php composer.phar install`.

Endpoint declaration

In the Azure Stack Edge Blob storage SDK, the endpoint suffix - `<device serial number>.microsoftdatabox.com` - identifies the Azure Stack Edge domain. For more information on the blob service endpoint, go to [Transfer data via storage accounts with Azure Stack Edge Pro GPU](#).

Examples

.NET

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the `app.config` file:

```
<add key="StorageConnectionString"
      value="DefaultEndpointsProtocol=https;AccountName=myaccount;AccountKey=mykey;
      EndpointSuffix=<><serial no. of the device>.microsoftdatabox.com </>
```

Java

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the setup of connection string:

```
public static final String storageConnectionString =
    "DefaultEndpointsProtocol=http;" +
    "AccountName=your_storage_account;" +
    "AccountKey=your_storage_account_key;" +
    "EndpointSuffix=<serial no. of the device>.microsoftdatabox.com ";
```

Node.js

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the declaration instance:

```
var blobSvc = azure.createBlobService('myaccount', 'mykey',
  'myaccount.blob. <serial no. of the device>.microsoftdatabox.com');
```

C++

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the setup of the connection string:

```
const utility::string_t storage_connection_string(U("DefaultEndpointsProtocol=https;
  AccountName=your_storage_account;
  AccountKey=your_storage_account_key;
  EndpointSuffix=<serial no. of the device>.microsoftdatabox.com "));
```

PHP

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the setup of the connection string:

```
$connectionString = 'BlobEndpoint=http://<storage account name>.blob.<serial no. of the
device>.microsoftdatabox.com /;
  AccountName=<storage account name>;AccountKey=<storage account key>'
```

Python

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the declaration instance:

```
block_blob_service = BlockBlobService(account_name='myaccount',
account_key='mykey',
endpoint_suffix='<serial no. of the device>.microsoftdatabox.com')
```

Ruby

For Azure Stack Edge Blob storage, the endpoint suffix is specified in the setup of the connection string:

```
set
AZURE_STORAGE_CONNECTION_STRING=DefaultEndpointsProtocol=https;
AccountName=myaccount;
AccountKey=mykey;
EndpointSuffix=<serial no. of the device>.microsoftdatabox.com
```

Next steps

- [Prepare to deploy Azure Stack Edge Pro with GPU](#)

Azure Stack Edge limits

9/21/2022 • 3 minutes to read • [Edit Online](#)

Consider these limits as you deploy and operate your Microsoft Azure Stack Edge Pro GPU or Azure Stack Edge Pro FPGA solution.

Azure Stack Edge service limits

- The storage account should be physically closest to the region where the device is deployed (can be different from where the service is deployed).
- Moving a Data Box Gateway resource to a different subscription or resource group is not supported. For more details, go to [Move resources to new resource group or subscription](#).

Azure Stack Edge device limits

The following table describes the limits for the Azure Stack Edge device.

DESCRIPTION	VALUE
No. of files per device	100 million
No. of shares per container	1
Maximum no. of share endpoints and REST endpoints per device (GPU devices only)	24
Maximum no. of tiered storage accounts per device (GPU devices only)	24
Maximum file size written to a share	5 TB
Maximum number of resource groups per device	800

Azure storage limits

This section describes the limits for Azure Storage service, and the required naming conventions for Azure Files, Azure block blobs, and Azure page blobs, as applicable to the Azure Stack Edge / Data Box Gateway service. Review the storage limits carefully and follow all the recommendations.

For the latest information on Azure storage service limits and best practices for naming shares, containers, and files, go to:

- [Naming and referencing containers](#)
- [Naming and referencing shares](#)
- [Block blobs and page blob conventions](#)

IMPORTANT

If there are any files or directories that exceed the Azure Storage service limits, or do not conform to Azure Files/Blob naming conventions, then these files or directories are not ingested into the Azure Storage via the Azure Stack Edge / Data Box Gateway service.

Data upload caveats

Following caveats apply to data as it moves into Azure.

- We suggest that more than one device should not write to the same container.
- If you have an existing Azure object (such as a blob or a file) in the cloud with the same name as the object that is being copied, device will overwrite the file in the cloud.
- An empty directory hierarchy (without any files) created under share folders is not uploaded to the blob containers.
- You can copy the data using drag and drop with File Explorer or via command line. If the aggregate size of files being copied is greater than 10 GB, we recommend you use a bulk copy program such as Robocopy or rsync. The bulk copy tools retry the copy operation for intermittent errors and provide additional resiliency.
- If the share associated with the Azure storage container uploads blobs that do not match the type of blobs defined for the share at the time of creation, then such blobs are not updated. For example, you create a block blob share on the device. Associate the share with an existing cloud container that has page blobs. Refresh that share to download the files. Modify some of the refreshed files that are already stored as page blobs in the cloud. You will see upload failures.
- After a file is created in the shares, renaming of the file isn't supported.
- Deletion of a file from a share does not delete the entry in the storage account.
- If using rsync to copy data, then `rsync -a` option is not supported.

Azure storage account size and object size limits

Here are the limits on the size of the data that is copied into storage account. Make sure that the data you upload conforms to these limits. For the most up-to-date information on these limits, see [Scalability and performance targets for Blob storage](#) and [Azure Files scalability and performance targets](#).

SIZE OF DATA COPIED INTO AZURE STORAGE ACCOUNT	DEFAULT LIMIT
Block Blob and page blob	500 TB per storage account

Azure object size limits

Here are the sizes of the Azure objects that can be written. Make sure that all the files that are uploaded conform to these limits.

AZURE OBJECT TYPE	UPLOAD LIMIT
Block Blob	~ 4.75 TB
Page Blob	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

AZURE OBJECT TYPE	UPLOAD LIMIT
Azure Files	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

IMPORTANT

Creation of files (irrespective of the storage type) is allowed up to 5 TB. However, if you create a file whose size is greater than the upload limit defined in the preceding table, the file does not get uploaded. You have to manually delete the file to reclaim the space.

Next steps

- [Prepare to deploy Azure Stack Edge Pro GPU](#)
- [Prepare to deploy Azure Stack Edge Pro FPGA](#)

Azure Stack Edge security and data protection

9/21/2022 • 6 minutes to read • [Edit Online](#)

Security is a major concern when you're adopting a new technology, especially if the technology is used with confidential or proprietary data. Azure Stack Edge helps you ensure that only authorized entities can view, modify, or delete your data.

This article describes the Azure Stack Edge security features that help protect each of the solution components and the data stored in them.

Azure Stack Edge consists of four main components that interact with each other:

- **Azure Stack Edge service, hosted in Azure.** The management resource that you use to create the device order, configure the device, and then track the order to completion.
- **Azure Stack Edge Pro FPGA device.** The transfer device that's shipped to you so you can import your on-premises data into Azure.
- **Clients/hosts connected to the device.** The clients in your infrastructure that connect to the Azure Stack Edge Pro FPGA device and contain data that needs to be protected.
- **Cloud storage.** The location in the Azure cloud platform where data is stored. This location is typically the storage account linked to the Azure Stack Edge resource that you create.

Azure Stack Edge service protection

The Azure Stack Edge service is a management service that's hosted in Azure. The service is used to configure and manage the device.

- To access the Azure Stack Edge service, your organization needs to have an Enterprise Agreement (EA) or Cloud Solution Provider (CSP) subscription. For more information, see [Sign up for an Azure subscription](#).
- Because this management service is hosted in Azure, it's protected by the Azure security features. For more information about the security features provided by Azure, go to the [Microsoft Azure Trust Center](#).
- For SDK management operations, you can get the encryption key for your resource in **Device properties**. You can view the encryption key only if you have permissions for the Resource Graph API.

Azure Stack Edge device protection

The Azure Stack Edge device is an on-premises device that helps transform your data by processing it locally and then sending it to Azure. Your device:

- Needs an activation key to access the Azure Stack Edge service.
- Is protected at all times by a device password.
- Is a locked-down device. The device BMC and BIOS are password-protected. The BIOS is protected by limited user-access.
- Has secure boot enabled.
- Runs Windows Defender Device Guard. Device Guard lets you run only trusted applications that you define in your code-integrity policies.

Protect the device via activation key

Only an authorized Azure Stack Edge device is allowed to join the Azure Stack Edge service that you create in your Azure subscription. To authorize a device, you need to use an activation key to activate the device with the Azure Stack Edge service.

The activation key that you use:

- Is an Azure Active Directory (Azure AD) based authentication key.
- Expires after three days.
- Isn't used after device activation.

After you activate a device, it uses tokens to communicate with Azure.

For more information, see [Get an activation key](#).

Protect the device via password

Passwords ensure that only authorized users can access your data. Azure Stack Edge devices boot up in a locked state.

You can:

- Connect to the local web UI of the device via a browser and then provide a password to sign in to the device.
- Remotely connect to the device PowerShell interface over HTTP. Remote management is turned on by default. You can then provide the device password to sign in to the device. For more information, see [Connect remotely to your Azure Stack Edge Pro FPGA device](#).

Keep these best practices in mind:

- We recommend that you store all passwords in a secure place so you don't have to reset a password if it's forgotten. The management service can't retrieve existing passwords. It can only reset them via the Azure portal. If you reset a password, be sure to notify all users before you reset it.
- You can access the Windows PowerShell interface of your device remotely over HTTP. As a security best practice, you should use HTTP only on trusted networks.
- Ensure that device passwords are strong and well protected. Follow the [password best practices](#).
- Use the local web UI to [change the password](#). If you change the password, be sure to notify all remote access users so they don't have problems signing in.

Protect your data

This section describes the Azure Stack Edge Pro FPGA security features that protect in-transit and stored data.

Protect data at rest

For data at rest:

- Access to data stored in shares is restricted.
 - SMB clients that access share data need user credentials associated with the share. These credentials are defined when the share is created.
 - The IP addresses of NFS clients that access a share need to be added when the share is created.
- BitLocker XTS-AES 256-bit encryption is used to protect local data.

Protect data in flight

For data in flight:

- Standard TLS 1.2 is used for data that travels between the device and Azure. There is no fallback to TLS 1.1 and earlier. Agent communication will be blocked if TLS 1.2 isn't supported. TLS 1.2 is also required for portal and SDK management.
- When clients access your device through the local web UI of a browser, standard TLS 1.2 is used as the default secure protocol.

- The best practice is to configure your browser to use TLS 1.2.
- If the browser doesn't support TLS 1.2, you can use TLS 1.1 or TLS 1.0.
- We recommend that you use SMB 3.0 with encryption to protect data when you copy it from your data servers.

Protect data via storage accounts

Your device is associated with a storage account that's used as a destination for your data in Azure. Access to the storage account is controlled by the subscription and two 512-bit storage access keys associated with that storage account.

One of the keys is used for authentication when the Azure Stack Edge device accesses the storage account. The other key is held in reserve, so you can rotate the keys periodically.

For security reasons, many datacenters require key rotation. We recommend that you follow these best practices for key rotation:

- Your storage account key is similar to the root password for your storage account. Carefully protect your account key. Don't distribute the password to other users, hard code it, or save it anywhere in plain text that's accessible to others.
- Regenerate your account key via the Azure portal if you think it could be compromised. For more information, see [Manage storage account access keys](#).
- Your Azure admin should periodically change or regenerate the primary or secondary key by using the Storage section of the Azure portal to access the storage account directly.
- Rotate and then [sync your storage account keys](#) regularly to help protect your storage account from unauthorized users.

Manage personal information

The Azure Stack Edge service collects personal information in the following scenarios:

- **Order details.** When an order is created, the shipping address, email address, and contact information of the user is stored in the Azure portal. The information saved includes:
 - Contact name
 - Phone number
 - Email address
 - Street address
 - City
 - ZIP Code/postal code
 - State
 - Country/province/region
 - Shipping tracking number

Order details are encrypted and stored in the service. The service retains the information until you explicitly delete the resource or order. The deletion of the resource and the corresponding order is blocked from the time the device is shipped until the device returns to Microsoft.

- **Shipping address.** After an order is placed, Data Box service provides the shipping address to third-party carriers like UPS.

- **Share users.** Users on your device can also access the data located on the shares. A list of users who can access the share data can be viewed. When the shares are deleted, this list is also deleted.

To view the list of users who can access or delete a share, follow the steps in [Manage shares on the Azure Stack Edge Pro FPGA](#).

For more information, review the Microsoft privacy policy on the [Trust Center](#).

Next steps

[Deploy your Azure Stack Edge Pro FPGA device](#)

Technical specifications and compliance for Azure Stack Edge Pro with GPU

9/21/2022 • 4 minutes to read • [Edit Online](#)

The hardware components of your Azure Stack Edge Pro with an onboard Graphics Processing Unit (GPU) adhere to the technical specifications and regulatory standards outlined in this article. The technical specifications describe hardware, power supply units (PSUs), storage capacity, enclosures, and environmental standards.

Compute and memory specifications

The Azure Stack Edge Pro device has the following specifications for compute and memory:

SPECIFICATION	VALUE
CPU type	Dual Intel Xeon Silver 4214 (Cascade Lake) CPU
CPU: raw	24 total cores, 48 total vCPUs
CPU: usable	40 vCPUs
Memory type	Dell Compatible 16 GB PC4-23400 DDR4-2933Mhz 2Rx8 1.2v ECC Registered RDIMM
Memory: raw	128 GB RAM (8 x 16 GB)
Memory: usable	102 GB RAM

Compute acceleration specifications

A Graphics Processing Unit (GPU) is included on every Azure Stack Edge Pro device that enables Kubernetes, deep learning, and machine learning scenarios.

SPECIFICATION	VALUE
GPU	One or two nVidia T4 GPUs For more information, see NVIDIA T4 .

Power supply unit specifications

The Azure Stack Edge Pro device has two 100-240 V power supply units (PSUs) with high-performance fans. The two PSUs provide a redundant power configuration. If a PSU fails, the device continues to operate normally on the other PSU until the failed module is replaced. The following table lists the technical specifications of the PSUs.

SPECIFICATION	750 W PSU
Maximum output power	750 W

SPECIFICATION	
Frequency	50/60 Hz
Voltage range selection	Auto ranging: 100-240 V AC
Hot pluggable	Yes

Network interface specifications

Your Azure Stack Edge Pro device has six network interfaces, PORT1 - PORT6.

SPECIFICATION	DESCRIPTION
Network interfaces	<p>2 X 1 GbE interfaces – 1 management interface Port 1 is used for initial setup and is static by default. After the initial setup is complete, you can use the interface for data with any IP address. However, on reset, the interface reverts back to static IP.</p> <p>The other interface Port 2 is user configurable, can be used for data transfer, and is DHCP by default.</p> <p>4 X 25-GbE interfaces – These data interfaces, Port 3 through Port 6, can be configured by user as DHCP (default) or static. They can also operate as 10-GbE interfaces.</p>

Your Azure Stack Edge Pro device has the following network hardware:

- Custom Microsoft [QLogic](#) Cavium 25G NDC adapter - Port 1 through port 4.
- Mellanox dual port 25G ConnectX-4 channel network adapter - Port 5 and port 6.

Here are the details for the Mellanox card:

PARAMETER	DESCRIPTION
Model	ConnectX®-4 Lx EN network interface card
Model Description	25 GbE dual-port SFP28; PCIe3.0 x8; ROHS R6
Device Part Number (R640)	MCX4121A-ACAT
PSID (R640)	MT_2420110034

For a full list of supported cables, switches, and transceivers for these network cards, go to:

- [QLogic](#) Cavium 25G NDC adapter interoperability matrix.
- Mellanox dual port 25G ConnectX-4 channel network adapter compatible products.

Storage specifications

The Azure Stack Edge Pro devices have five 2.5" NVMe DC P4610 SSDs, each with a capacity of 1.6 TB. The boot drive is a 240 GB SATA SSD. The total usable capacity for the device is roughly 4.19 TB. The following table lists the storage capacity of the device.

SPECIFICATION	VALUE
Number of NVMe SSDs	5
Single NVMe SSD capacity	1.6 TB
Boot SATA solid-state drives (SSD)	1
Boot SSD capacity	240 GB
Total capacity	8.0 TB
Total usable capacity	~ 4.19 TB
RAID configuration	Storage Spaces Direct with a combination of mirroring and parity
SAS controller	HBA330 12 Gbps

Enclosure dimensions and weight specifications

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The following table lists the dimensions of the 1U device enclosure in millimeters and inches.

ENCLOSURE	MILLIMETERS	INCHES
Height	44.45	1.75"
Width	434.1	17.09"
Length	740.4	29.15"

The following table lists the dimensions of the shipping package in millimeters and inches.

PACKAGE	MILLIMETERS	INCHES
Height	311.2	12.25"
Width	642.8	25.31"
Length	1,051.1	41.38"

Enclosure weight

The device package weighs 66 lbs. and requires two persons to handle it. The weight of the device depends on the configuration of the enclosure.

ENCLOSURE	WEIGHT
Total weight including the packaging	61 lbs.

ENCLOSURE	WEIGHT
Weight of the device	35 lbs.

Enclosure environment specifications

This section lists the specifications related to the enclosure environment such as temperature, humidity, and altitude.

Temperature and humidity

ENCLOSURE	AMBIENT TEMPERATURE RANGE	AMBIENT RELATIVE HUMIDITY	MAXIMUM DEW POINT
Operational	10°C - 35°C (50°F - 86°F)	10% - 80% non-condensing.	29°C (84°F)
Non-operational	-40°C to 65°C (-40°F - 149°F)	5% - 95% non-condensing.	33°C (91°F)

Airflow, altitude, shock, vibration, orientation, safety, and EMC

ENCLOSURE	OPERATIONAL SPECIFICATIONS
Airflow	System airflow is front to rear. System must be operated with a low-pressure, rear-exhaust installation.
Ingress protection (IP)	This type of rack-mounted equipment for indoor use typically isn't tested for ingress protection (protection against solids and liquids for an electrical enclosure). Manufacturer's safety assessment shows IPX0 (no ingress protection).
Maximum altitude, operational	3048 meters (10,000 feet) with maximum operating temperature de-rated determined by Operating temperature de-rating specifications .
Maximum altitude, non-operational	12,000 meters (39,370 feet)
Shock, operational	6 G for 11 milliseconds in 6 orientations
Shock, non-operational	71 G for 2 milliseconds in 6 orientations
Vibration, operational	0.26 G _{RMS} 5 Hz to 350 Hz random
Vibration, non-operational	1.88 G _{RMS} 10 Hz to 500 Hz for 15 minutes (all six sides tested.)
Orientation and mounting	Standard 19" rack mount (1U)
Safety and approvals	EN 60950-1:2006 +A1:2010 +A2:2013 +A11:2009 +A12:2011/IEC 60950-1:2005 ed2 +A1:2009 +A2:2013 EN 62311:2008

ENCLOSURE	OPERATIONAL SPECIFICATIONS
EMC	FCC A, ICES-003 EN 55032:2012/CISPR 32:2012 EN 55032:2015/CISPR 32:2015 EN 55024:2010 +A1:2015/CISPR 24:2010 +A1:2015 EN 61000-3-2:2014/IEC 61000-3-2:2014 (Class D) EN 61000-3-3:2013/IEC 61000-3-3:2013
Energy	Commission Regulation (EU) No. 617/2013
RoHS	EN 50581:2012

Operating temperature de-rating specifications

OPERATING TEMPERATURE DE-RATING	AMBIENT TEMPERATURE RANGE
Up to 35°C (95°F)	Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 950 m (3,117 ft).
35°C to 40°C (95°F to 104°F)	Maximum temperature is reduced by 1°C/175 m (1°F/319 ft) above 950 m (3,117 ft).
40°C to 45°C (104°F to 113°F)	Maximum temperature is reduced by 1°C/125 m (1°F/228 ft) above 950 m (3,117 ft).

Next steps

[Deploy your Azure Stack Edge Pro](#)

Azure Stack Edge Pro FPGA power cord specifications

9/21/2022 • 6 minutes to read • [Edit Online](#)

Your Azure Stack Edge Pro FPGA device will need a power cord that will vary depending on your Azure region.

Supported power cords

You can use the following table to find the correct cord specifications for your region:

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Albania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Algeria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Angola	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Argentina	250	10	H05VV-F 3x1.00	IRAM 2073	C13	2500
Australia	250	10	H05VV-F 3x1.00	AS/NZS 3112	C13	2438
Austria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Azerbaijan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bahamas	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Bahrain	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Bangladesh	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Barbados	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Belarus	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Belgium	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bermuda	125	10	SVE 18/3	NEMA 5-15P	C13	1830

Country	Rated Voltage (V)	Rated Current (A)	Cord Standard	Input Connector	Output Connector	Length mm
Bolivia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bosnia and Herzegovina	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Brazil	250	10	H05Z1Z1-F 3x.75	NBR 14136	C13	1914
Bulgaria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Cambodia	250	10	H05VV-F 3X0.75	CEE 7/7	C13	1800
Canada	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Cayman Islands	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Chile	250	10	H05VV-F 3x0.75	CEI 23-50	C13	1800
China	250	10	RVV300/500 3X0.75	GB 2099.1	C13	2000
Colombia	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Costa Rica	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Côte D'Ivoire (Ivory Coast)	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Croatia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Cyprus	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Czech Republic	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Denmark	250	10	H05VV-F 3X0.75	SB107-2-DI	C13	1800
Dominican Republic	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Ecuador	125	10	SVE 18/3	NEMA 5-15P	C13	1830

Country	Rated Voltage (V)	Rated Current (A)	Cord Standard	Input Connector	Output Connector	Length mm
Egypt	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
El Salvador	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Estonia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ethiopia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Finland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
France	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Georgia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Germany	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ghana	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Guyana	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Greece	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Guatemala	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Honduras	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Hong Kong	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Hungary	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Iceland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
India	250	10	IS694 3x0.75	IS 1293	C13	1830
Indonesia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ireland	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Israel	250	2.5	H05VV-F 3x1.00	SI 32	C13	2000
Italy	250	10	H05VV-F 3x0.75	CEI 23-50	C13	1800
Jamaica	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Japan	125	15	VCTF 3x2.00 Act on Product Safety of Electrical Appliances and Materials	JIS C 8303	C13	2300
Jordan	250	5	H05Z1Z1-F 3x0.75	BS 1363	C13	1830
Kazakhstan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Kenya	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Kuwait	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Kyrgyzstan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Latvia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Lebanon	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Liechtenstein	250	10	H05VV-F 3x0.75	SEV 1011	C13	1800
Lithuania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Luxembourg	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Macau	2250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Macedonia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Malaysia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Malta	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Mauritius	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Mexico	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Moldova	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Monaco	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Mongolia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Montenegro	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Morocco	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Namibia	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
Nepal	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
Netherlands	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
New Zealand	250	10	H05VV-F 3x1.00	AS/NZS 3112	C13	2438
Nicaragua	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Nigeria	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Norway	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Oman	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Pakistan	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Panama	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Paraguay	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Peru	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Philippines	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Poland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Portugal	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Puerto Rico	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Qatar	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Romania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Russia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Rwanda	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Saint Kitts and Nevis	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Samoa	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Saudi Arabia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Senegal	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Serbia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Singapore	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Slovakia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Slovenia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
South Africa	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
South Korea	250	10	H05W-F 3x1.75	KS C 8305	C13	1830
Spain	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Sri Lanka	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Sweden	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Switzerland	250	10	H05VV-F 3x0.75	SEV 1011	C13	1800
Taiwan	125	10	VCTF 3x1.25	CNS10917	C13	2000
Tajikistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Tanzania	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Thailand	250	10	H05VV-F 3x0.75	TI16S3	C13	1829
Trinidad and Tobago	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Tunisia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Turkey	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Turkmenistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Uganda	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Ukraine	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
United Arab Emirates	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
United Kingdom	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
United States	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Uruguay	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Uzbekistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Venezuela	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Vietnam	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Yemen	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Zambia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Zimbabwe	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

Next steps

[Azure Stack Edge Pro FPGA technical specifications](#)

Clustering on your Azure Stack Edge Pro GPU device

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2

This article provides a brief overview of clustering on your Azure Stack Edge device.

About failover clustering

Azure Stack Edge can be set up as a single standalone device or a two-node cluster. A two-node cluster consists of two independent Azure Stack Edge devices that are connected by physical cables and by software. These nodes when clustered work together as in a Windows failover cluster, provide high availability for applications and services that are running on the cluster.

If one of the clustered nodes fails, the other node begins to provide service (the process is known as failover). The clustered roles are also proactively monitored to make sure that they're working properly. If they aren't working, they're restarted or moved to the second node.

Azure Stack Edge uses Windows Server Failover Clustering for its two-node cluster. For more information, see [Failover clustering in Windows Server](#).

Cluster quorum and witness

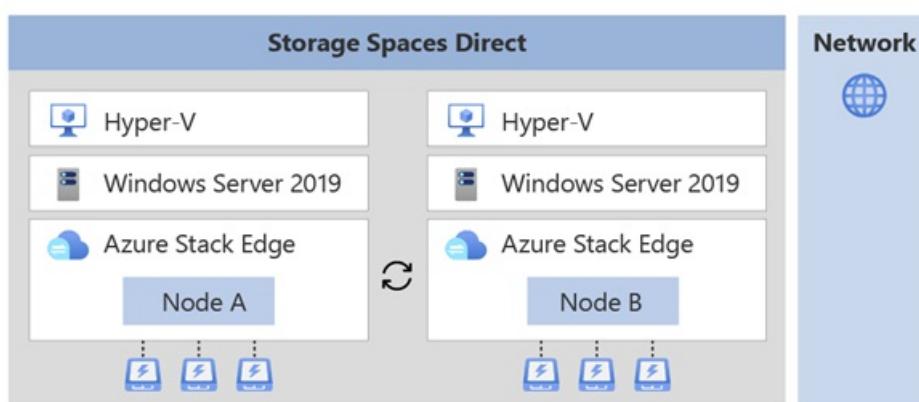
A quorum is always maintained on your Azure Stack Edge cluster to remain online in the event of a failure. If one of the nodes fails, then the majority of the surviving nodes must verify that the cluster remains online. The concept of majority only exists for clusters with an odd number of nodes. For more information on cluster quorum, see [Understand quorum](#).

For an Azure Stack Edge cluster with two nodes, if a node fails, then a cluster witness provides the third vote so that the cluster stays online (since the cluster is left with two out of three votes - a majority). A cluster witness is required on your Azure Stack Edge cluster. You can set up the witness in the cloud or in a local fileshare using the local UI of your device.

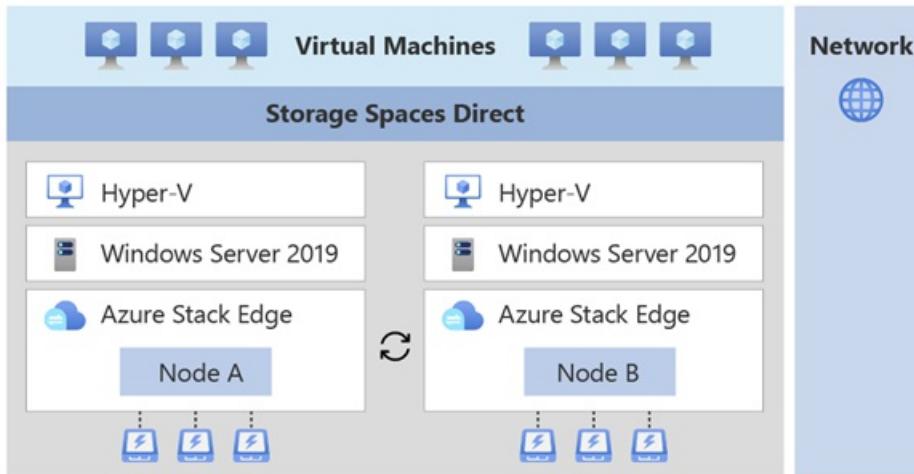
For more information on cluster witness, see [Cluster witness on Azure Stack Edge](#).

Infrastructure cluster

The infrastructure cluster on your device provides persistent storage and is shown in the following diagram:



- The infrastructure cluster consists of the two independent nodes running Windows Server operating system with a Hyper-V layer. The nodes contain physical disks for storage and network interfaces that are connected back-to-back or with switches.
- The disks across the two nodes are used to create a logical storage pool. The storage spaces direct on this pool provides mirroring and parity for the cluster.
- You can deploy your application workloads on top of the infrastructure cluster.
 - Non-containerized workloads such as VMs can be directly deployed on top of the infrastructure cluster.



- Containerized workloads use Kubernetes for workload deployment and management. A Kubernetes cluster that consists of a master VM and two worker VMs (one for each node) is deployed on top of the infrastructure cluster.

The Kubernetes cluster allows for application orchestration whereas the infrastructure cluster provides persistent storage.

Supported networking topologies

Based on the use-case and workloads, you can select how the two Azure Stack Edge device nodes will be connected. The networking topologies available will differ depending on whether you use an Azure Stack Edge Pro GPU device or an Azure Stack Edge Pro 2 device.

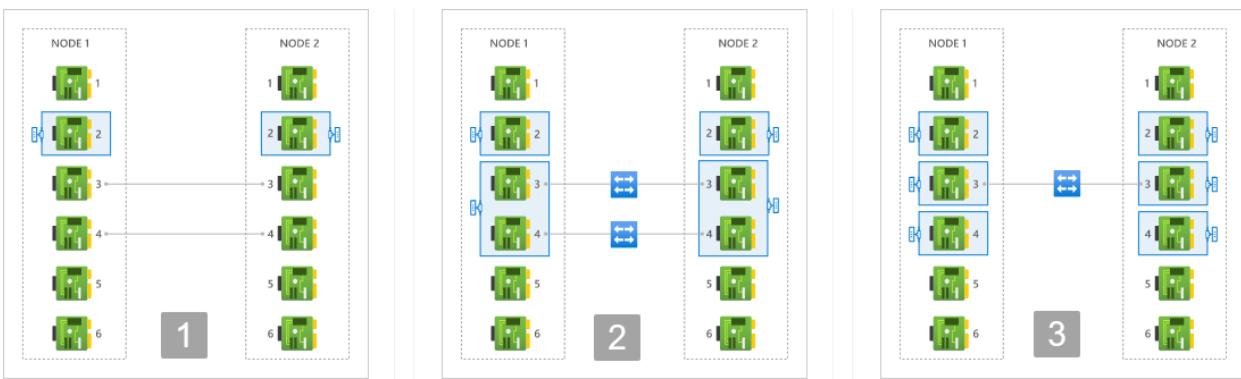
The supported network topologies for each of the device types are described here.

- [Azure Stack Edge Pro GPU](#)
- [Azure Stack Edge Pro 2](#)

On your Azure Stack Edge Pro GPU device node:

- Port 2 is used for management traffic.
- Port 3 and Port 4 are used for storage and cluster traffic. This traffic includes that needed for storage mirroring and Azure Stack Edge cluster heartbeat traffic that is required for the cluster to be online.

The following network topologies are available:



- 1. Switchless** - Use this option when you don't have high speed switches available in the environment for storage and cluster traffic.

In this option, Port 3 and Port 4 are connected back-to-back without a switch. These ports are dedicated to storage and Azure Stack Edge cluster traffic and aren't available for workload traffic. Optionally you can also provide IP addresses for these ports.

- 2. Using switches and NIC teaming** - Use this option when you have high speed switches available for use with your device nodes for storage and cluster traffic.

Each of ports 3 and 4 of the two nodes of your device are connected via an external switch. The Port 3 and Port 4 are teamed on each node and a virtual switch and two virtual NICs are created that allow for port-level redundancy for storage and cluster traffic. These ports can be used for workload traffic as well.

- 3. Using switches and without NIC teaming** - Use this option when you need an extra dedicated port for workload traffic and port-level redundancy isn't required for storage and cluster traffic.

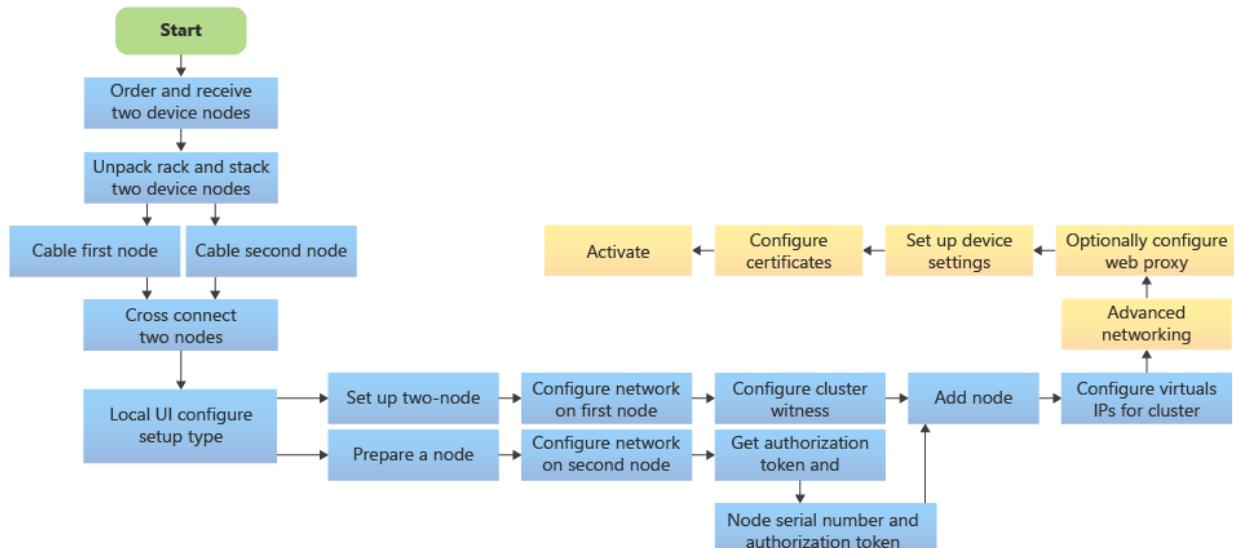
Port 3 on each node is connected via an external switch. If Port 3 fails, the cluster may go offline. Separate virtual switches are created on Port 3 and Port 4.

For more information, see how to [Choose a network topology for your device node](#).

Cluster deployment

- [Azure Stack Edge Pro GPU](#)
- [Azure Stack Edge Pro 2](#)

Before you configure clustering on your device, you must cable the devices as per one of the supported network topologies that you intend to configure. To deploy a two-node infrastructure cluster on your Azure Stack Edge devices, follow these high-level steps:



1. Order two independent Azure Stack Edge devices. For more information, see [Order an Azure Stack Edge device](#).
2. Cable each node independently as you would for a single node device. Based on the workloads that you intend to deploy, cross connect the network interfaces on these devices via cables, and with or without switches. For detailed instructions, see [Cable your two-node cluster device](#).
3. Start cluster creation on the first node. Choose the network topology that conforms to the cabling across the two nodes. The chosen topology would dictate the storage and clustering traffic between the nodes. See detailed steps in [Configure network and web proxy on your device](#).
4. Prepare the second node. Configure the network on the second node the same way you configured it on the first node. Get the authentication token on this node.
5. Use the authentication token from the prepared node and join this node to the first node to form a cluster.
6. Set up a cloud witness using an Azure Storage account or a local witness on an SMB fileshare.
7. Assign a virtual IP to provide an endpoint for Azure Consistent Services or when using NFS.
8. Assign compute or management intents to the virtual switches created on the network interfaces. You may also configure Kubernetes node IPs and Kubernetes service IPs here for the network interface enabled for compute.
9. Optionally configure web proxy, set up device settings, configure certificates and then finally, activate the device.

For more information, see the two-node device deployment tutorials starting with [Get deployment configuration checklist](#).

Clustering workloads

On your two-node cluster, you can deploy non-containerized workloads or containerized workloads.

- **Non-containerized workloads such as VMs:** The two-node cluster will ensure high availability of the virtual machines that are deployed on the device cluster. Live migration of VMs isn't supported.
- **Containerized workloads such as Kubernetes or IoT Edge:** The Kubernetes cluster deployed on top of the device cluster consists of one Kubernetes master VM and two Kubernetes worker VMs. Each Kubernetes node has a worker VM that is pinned to each Azure Stack Edge node. Failover results in the failover of Kubernetes master VM (if needed) and Kubernetes-based rebalancing of pods on the surviving worker VM.

For more information, see [Kubernetes on a clustered Azure Stack Edge device](#).

Cluster management

You can manage the Azure Stack Edge cluster via the PowerShell interface of the device, or through the local UI. Some typical management tasks are:

- [Undo node preparation](#)
- [Configure cloud witness](#)
- [Set up a local witness](#)
- [Configure virtual IP settings](#)
- [Remove the cluster](#)

Cluster updates

A two-node clustered device upgrade will first apply the device updates followed by the Kubernetes cluster updates. Rolling updates to device nodes ensure minimal downtime of workloads.

When you apply these updates via the Azure portal, you only have to start the process on one node and both

the nodes are updated. For step-by-step instructions, see [Apply updates to your two-node Azure Stack Edge device](#).

Billing

If you deploy an Azure Stack Edge two-node cluster, each node is billed separately. For more information, see [Pricing page for Azure Stack Edge](#).

Next steps

- Learn about [Cluster witness for your Azure Stack Edge](#).
- See [Kubernetes for your Azure Stack Edge](#)
- Understand [Cluster failover scenarios](#)

Cluster witness on your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2

This article provides a brief overview of cluster witness on your Azure Stack Edge device including cluster witness requirements, setup, and management.

About cluster quorum and witness

In Windows Server Failover Clustering, quorum needs to be maintained in order for the Windows Server cluster to remain online in the event of a failure. When nodes in a Windows Server cluster fail, surviving nodes need to verify that they constitute the majority of the cluster to remain online.

However, the concept of majority only exists for clusters with an odd number of nodes. When the number of nodes in a cluster is even, the system requires a way to make the total number of votes odd. This is where the role of cluster witness is important. The cluster witness is given a vote, so that in the event of a failure, the total number of votes in the cluster (which originally had an even number of nodes) is odd.

For more information on cluster quorum, see [Understand cluster quorum](#).

Cluster quorum and witness on Azure Stack Edge

Windows Server Failover Clustering is implemented on a two-node Azure Stack Edge device. A quorum is always maintained on your Azure Stack Edge cluster so that the device can remain online in the event of a failure. If one of the nodes fails, then the majority of the surviving nodes must verify that the cluster remains online. The concept of majority only exists for clusters with an odd number of nodes.

For an Azure Stack Edge cluster with two nodes, if a node fails, then a cluster witness provides the third vote so that the cluster stays online (since the cluster is left with 2/3 votes - a majority).

Cluster witness on Azure Stack Edge

A two-node Azure Stack Edge cluster requires a cluster witness, so that if one of the Azure Stack Edge nodes fails, the cluster witness accounts for the third vote, and the cluster stays online (since the cluster is left with 2/3 votes - a majority). On the other hand, if both the device nodes fail simultaneously, or a second Azure Stack Edge node fails after the first has failed, there is no majority vote, and the cluster goes offline.

This system requires both Azure Stack Edge nodes to have connectivity to each other and the cluster witness. If the cluster witness were to go offline or lose connectivity with either of the device nodes, the total number of votes in the event of a single Azure Stack Edge node failure would be even. In this case, Windows Server Failover Clustering will try to remediate this by arbitrarily picking a device node that will not get to vote (in order to make the total number of votes odd). In this case, if the Azure Stack Edge node that failed happened to be the one that got the single vote in the Azure Stack Edge cluster, there will be no majority vote and the cluster will go offline. This is why, in order to prevent the Azure Stack Edge cluster from going offline in the event of a single device node failure, it is important for the cluster witness to be online and have connectivity to both the device nodes.

Witness requirements

Cluster witness can be in the cloud or live locally. In each case, there are certain requirements that the witness

must meet.

- **Cloud witness requirements**

- Both the device nodes in the cluster should have a reliable internet connection.
- Make sure that the HTTPS default port 443 is open on your device as cloud witness uses this port to establish outbound communication with the Azure blob service.

- **Local witness requirements**

- SMB 2.0 File share is created on-premises but not on the nodes of your device.
- A minimum of 5 MB of free space exists on the file share.
- Your device can access the file share over the network.

Cluster witness setup and configuration

In order for the witness to have an independent vote, it must always be hosted outside of the Azure Stack Edge nodes in the device cluster. The witness can be deployed in either of the following ways.

- **Cloud witness** - Use the cloud witness when both the nodes on your Azure Stack Edge cluster are connected to Azure. To set up a cloud witness, use an Azure Storage account in the cloud and configure the witness via the local UI of the device.

We recommend that you deploy the cloud witness with redundant connections so that the witness is highly available. For more information, see [Set up cloud witness via the local UI](#).

- **Local witness** - Use the local witness when both the nodes are not connected to Azure or have sporadic connectivity. If you're in an IT environment with other machines and file shares, use a file share witness. To set up a local witness, you can use an SMB fileshare on a local server in the network where the device is deployed and configure the fileshare path to the server via the local UI.

We recommend that you deploy the witness in a way that it is highly available. For example, a switch running a file server could be used to host a file share. For more information, see [Set up local witness via the local UI](#).

Next steps

- Learn how to [Configure cloud witness for Azure Stack Edge Pro GPU](#).
- Learn how to [Set up local witness for Azure Stack Edge Pro GPU](#).

Cluster failover scenarios on your Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This article identifies the common failover scenarios, how the Azure Stack Edge device responds, and the overall impact on the workloads deployed on the cluster should a failover occur.

About failover

Azure Stack Edge can be set up as a single standalone device or a two-node cluster. In a two-node cluster, the clustered nodes provide high availability for applications and services that are running on the cluster.

If one of the clustered node fails, the other node begins to provide service - this process is known as failover. Failover may also occur if hardware components associated with one or both nodes of your device such as disk drives, power supply units (PSUs), or network fail or when you update your device nodes.

Failover scenarios

Failover may occur as a result of hardware component failure, node failure or when updating the Azure Stack Edge cluster.

Hardware failures

These tables summarize the failure scenarios for a physical hardware component associated with your device cluster such as one or more of disk drives, power supply, or network.

Disk drive failures

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
1 disk drive fails	No failures	Yes	No	Cluster is degraded until the disk is replaced.
2 or more disk drives fail	No failures	Yes	No	Cluster is degraded until the disk is replaced.
1 or more disk drives fail	1 or more disk drives fail	No		Cluster goes offline.

Power supply unit failures

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
1 PSU fails	No failures	Yes	No	Another power supply failure on node A will result in failover to node B.

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
1 PSU fails	1 PSU fails	Yes	No	Another power supply failure on either node will result in failover.
2 PSUs fail	No failures	Yes	Yes	VMs on node A fail over to node B.
2 PSUs fail (TBC)	1 PSU fails	Yes	Yes	VMs on node A fail over to node B.
2 PSUs fail	2 PSUs fail	No		Cluster goes offline.

Network failures

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
Port 1, Port 2, Port 5, or Port 6 fails	No failures	Yes	No	Failed port is unavailable. Apps listening on this port are impacted
1 or both of Port 3 and Port 4 fail	No failures	Yes	Yes	VMs on node A fail over to node B

Node failures and updates

Node failure

This table summarizes the failure scenarios when an entire node has failed on your cluster.

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
Entire node fails	No failures	Yes	Yes	VMs from node A fail over to node B
Entire node fails	Entire node fails	No	-	Cluster goes offline
Reboot	No failures	Yes	Yes	VMs from node A fail over to node B
Reboot	Reboot	No	-	Cluster is offline until the reboot completes
Core component fails. For example, motherboard, DIMM, and OS disk.	No failures	Yes	Yes	VMs from node A fail over to node B
Core component fails. For example, motherboard, DIMM, and OS disk.	Core component fails. For example, motherboard, DIMM, and OS disk.	No	-	Cluster goes offline

Node update

NODE A	NODE B	CLUSTER SURVIVES	FAILOVER	DETAILS
Node update	No failures	Yes	Yes	VMs from node A fail over to node B
Node update	2 PSUs fail	No	-	Cluster goes offline
Node update	Entire node fails or goes offline	No	-	Cluster goes offline
Node update	Reboot	No	-	Cluster goes offline
Node update	Core component fails such as motherboard, DIMM, and OS disk.	No	-	Cluster goes offline

Next steps

- Learn about [VM sizes and types for Azure Stack Edge Pro GPU](#).

Manage your Azure Stack Edge cluster

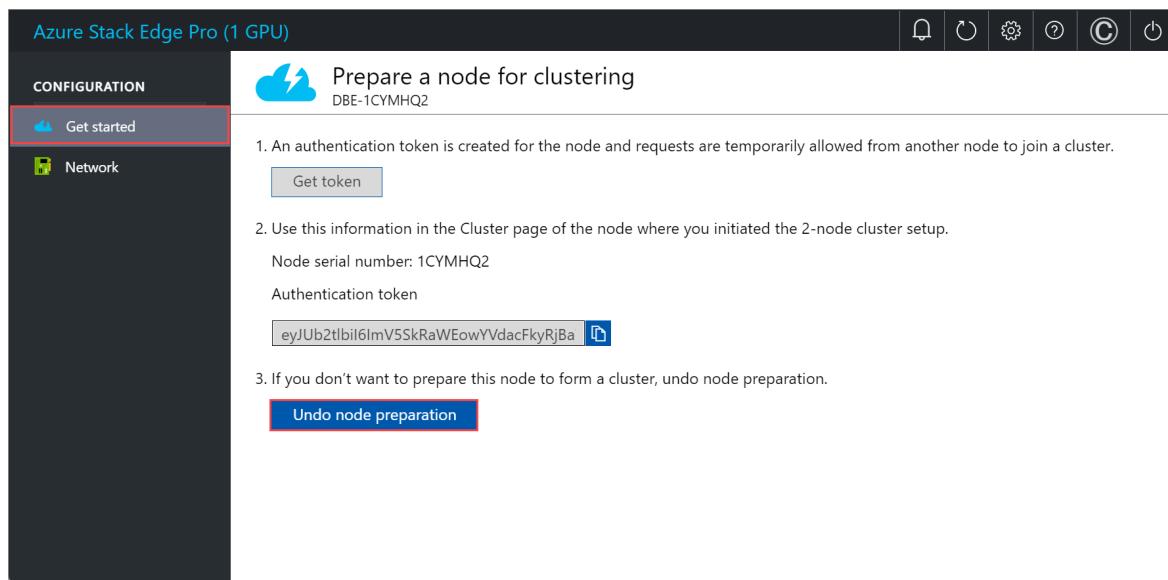
9/21/2022 • 4 minutes to read • [Edit Online](#)

This article provides a brief overview of clustering-related management tasks on your Azure Stack Edge device. Some of these tasks include how to add a node, configure or modify a cluster witness or remove the cluster. The cluster can be managed via the local UI of your device.

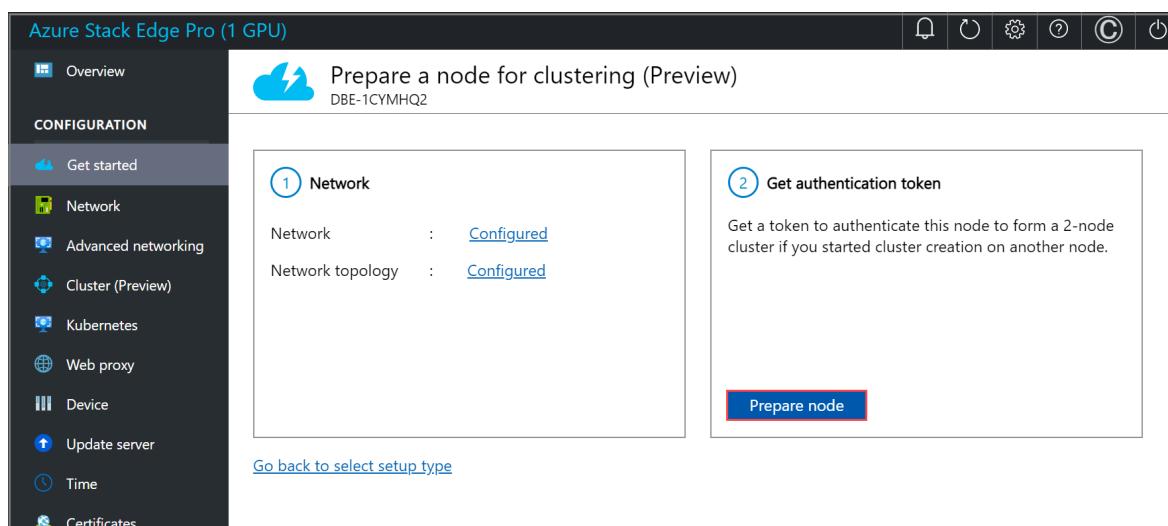
Undo node preparation

Perform these steps on the node of the device that you were trying to prepare. You may use the undo node preparation option when you decide not to proceed with preparing this node to form a cluster.

1. In the local UI, go to the **Get started** page. Under **Prepare a node for clustering**, select **Undo node preparation**.



2. When you select **Undo node preparation**, you'll go back to the **Get authentication token** tile and **Prepare node** option will be available. If you decide to prepare this node again, you'll need to select **Prepare node** again.



View existing nodes

1. In the local UI, go to the **Cluster** page.
2. Under **Existing nodes**, you can view the existing nodes for your cluster.

Cluster (Preview)

Successfully configured the device.

Add a prepared node, view existing nodes, or modify cluster witness.

Cluster name: 1CSPHQ2CL

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestoracccalkohli	myasecont	core.windows.net

Existing nodes

Add new nodes or view existing nodes

Serial number	Version	Status
1CSPHQ2	2.2.1842.4304	Healthy
HVTCT12	2.2.1842.4304	Healthy

Actions: Modify, Add node, Replace node, Apply

Replace a node

You may need to replace a node if one of the nodes on your device is down or not healthy. Perform these steps on the node that you're trying to replace.

1. In the local UI, go to the **Cluster** page. Under **Existing nodes**, view the status of the nodes. You'll want to replace the node that shows the status as **Down**.

Cluster (Preview)

Successfully configured the device.

Add a prepared node, view existing nodes, or modify cluster witness.

Cluster name: 1CSPHQ2CL

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestoracccalkohli	myasecont	core.windows.net

Existing nodes

Add new nodes or view existing nodes

Serial number	Version	Status
1CSPHQ2	2.2.1842.4304	Healthy
HVTCT12	2.2.1842.4304	Down

Actions: Modify, Add node, Replace node, Apply

2. Select **Replace node** and enter the following inputs.

- a. Choose the node to replace. This should be automatically selected as the node, which is down.
- b. Prepare another node. Configure the networking on this node in the same way as you set up on the first node. Get the node serial number and authentication token from the new incoming node.

- c. Provide the **Node serial number** for the incoming replacement node.
- d. Supply the **Node token** for the incoming replacement node.
- e. Select **Validate & add**. The credentials of the incoming node are now validated.

The screenshot shows a modal dialog titled "Replace node". At the top, there is a note: "* Select a node to replace" followed by a dropdown menu containing "HVTC1T2". Below this, instructions say: "Prepare another node and add it to form a cluster. Before you add another node:" followed by a bulleted list:

- Configure the networking on the incoming node in the same way as you set up on this node.
- Get the node serial number and authentication token by preparing the incoming node.

[Learn how to get the node serial number and token.](#)

Enter information for the incoming node.

Node serial number: ✓

Node token: ✓

Validate & add

- f. Once the validation has successfully completed, select **Add node** to complete the node replacement. It may take several minutes for the replacement node to get added to form the cluster.

Configure cluster witness

Follow these steps to configure the cluster witness.

Configure cloud witness

Perform these steps on the first node of the device.

1. In the local UI, go to the **Cluster** page. Under **Cluster witness type**, select **Modify**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview) - highlighted with a red box), Kubernetes, Web proxy, Device, Update server, Time, Certificates, and Cloud details. The Maintenance section includes Power, Hardware health, Software update, Password change, and Device reset. The main content area is titled 'Cluster (Preview)' and shows 'DBE-1CSPHQ2'. It has a note about adding prepared nodes or modifying cluster witness. The 'Cluster witness' section is expanded, showing 'Witness type' set to 'None' and a 'Modify' button. Below is the 'Existing nodes' section with an 'Add node' and 'Replace node' button. A table lists one node: Serial number 1CSPHQ2, Version 2.2.1842.4304, and Status Healthy. An 'Apply' button is at the bottom. Navigation buttons at the bottom are '< Back to Get started' and 'Next: Web proxy >'.

2. In the **Modify cluster witness** blade, enter the following inputs.
 - a. Choose the **Witness type** as **Cloud**.
 - b. Enter the **Azure Storage account name**.
 - c. Specify Storage account authentication from Access key or SAS token.
 - d. If you chose Access key as the authentication mechanism, enter the Access key of the Storage account, Azure Storage container where the witness lives, and the service endpoint.
 - e. Select **Apply**.

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

Cloud

* Azure Storage account name

myasestoracctalkohli

* Storage account authentication

Access key SAS token

* Access key

ir/MHKGMGoLZKfoJqzS28CBAATeryg5w%

Azure Storage container

myasecont

Service endpoint

core.windows.net

Apply

Configure local witness

Perform these steps on the first node of the device.

1. In the local UI, go to the Cluster page. Under Cluster witness type, select Modify.

The screenshot shows the Azure Stack Edge Pro (1 GPU) management interface. The left sidebar contains navigation links for Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Help (Feedback, Report a problem). The main content area is titled "Cluster (Preview)" and shows the cluster name "1CSPHQ2CL". It includes sections for "Cluster witness" (Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share. Witness type: None, Modify button), "Existing nodes" (Add new nodes or view existing nodes, Add node, Replace node buttons, table with one row: Serial number 1CSPHQ2, Version 2.2.1842.4304, Status Healthy, Apply button), and navigation links "< Back to Get started" and "Next: Web proxy >".

2. In the **Modify cluster witness** blade, enter the following inputs.

- a. Choose the **Witness type** as **Local**.
- b. Enter the file share path as **//server/fileshare** format.
- c. Select **Apply**.

X

Modify cluster witness

Choose an Azure Storage account as a cloud witness or a local SMB share as file share witness. [Learn more about the cluster witness requirements.](#)

* Witness type

File share

* Share path

//clusterserver/clusterwitnessshare

Credentials required

* Username

mysmbuser1

* Password

Apply

Configure virtual IPs

For Azure consistent services and NFS, you'll also need to define a virtual IP that allows you to connect to a clustered device as opposed to a specific node. A virtual IP is an available IP in the cluster network and any client connecting to the cluster network on the two-node device should be able to access this IP.

For Azure Consistent Services

For Azure Consistent Services, follow these steps to configure virtual IP.

1. In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Azure Consistent Services**.

Azure Stack Edge Pro (1 GPU)

CONFIGURATION

- Overview
- Get started
- Network
- Advanced networking
- Cluster (Preview)**
- Kubernetes
- Web proxy
- Device
- Update server
- Time
- Certificates
- Cloud details

MAINTENANCE

- Power
- Hardware health
- Software update
- Password change
- Device reset
- Diagnostic tests
- Support

Cluster (Preview)

Successfully configured the device.

Cluster witness

Configure cluster witness to establish quorum if a node goes down. Use an Azure Storage account as a cloud witness or a local SMB file share.

Witness type	Status	Azure Storage account name	Azure Storage container	Service endpoint
Cloud	Online	myasestorac talkohli	myasecont	core.windows.net

Existing nodes

Add new nodes or view existing nodes

Virtual IP settings

For each of the services, specify the network and the virtual IP.

Name	Network	Virtual IP
Azure Consistent Services	-	
Network File System	-	

< Back to Get started | Next: Web proxy >

2. In the **Virtual IP settings** blade, input the following.

- From the dropdown list, select the **Azure Consistent Services network**.
- Choose IP settings from **DHCP** or **static**.
- If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the Azure Consistent Services network that you specified. If you selected DHCP, a virtual IP is automatically picked from the Azure Consistent Services network that you selected.

3. Select **Apply**.

Virtual IP settings

* Azure Consistent Services network
192.168.0.0

* IP settings
DHCP **Static**

Azure Consistent Services Virtual IP
IP will be auto allocated.

Apply

For Network File System

For clients connecting via NFS protocol to the two-node device, follow these steps to configure virtual IP.

1. In the local UI on the **Cluster** page, under the **Virtual IP settings** section, select **Network File System**.

Name	Network	Virtual IP
Azure Consistent Services	10.126.72.0	10.126.77.178
Network File System	-	10.126.77.178

2. In the **Virtual IP settings** blade, input the following.

- a. From the dropdown list, select the **NFS network**.
- b. Choose IP settings from **DHCP** or **Static**.
- c. If you chose IP settings as static, enter a virtual IP. This should be a free IP from within the NFS network that you specified. If you selected DHCP, a virtual IP is automatically picked from the NFS network that you selected.

3. Select **Apply**.

Virtual IP settings

* Network File System network
192.168.0.0

* IP settings
 DHCP Static

Network File System Virtual IP
IP will be auto allocated.

Apply

NOTE

Virtual IP settings are required. If you do not configure this IP, you will be blocked when configuring the **Device settings** in the next step.

Remove the cluster

In this release, the only way to remove or destroy the cluster is to reset the device.

NOTE

To remove the cluster, you need to reset only one device node. In this release, if a reset is triggered on one node in a two-node cluster, it will trigger reset on both the nodes in the cluster.

Follow these steps to reset the device:

1. In the local web UI of your first device node, go to **Maintenance > Device reset**.
2. Select **Reset device**.
3. On the **Confirm reset** dialog, enter **Yes** and select **Yes** to continue with the device reset. Resetting the device will delete all the local data on the device.

The reset process will take approximately 35-40 minutes.

Next steps

- Learn about [VM sizes and types for Azure Stack Edge Pro GPU](#).

Kubernetes failover scenarios on a clustered Azure Stack Edge device

9/21/2022 • 4 minutes to read • [Edit Online](#)

Kubernetes cluster is deployed as a popular open-source platform to orchestrate containerized applications. This article describes how Kubernetes works on your 2-node Azure Stack Edge device including the failure modes and the corresponding device responses.

About Kubernetes on Azure Stack Edge

On your Azure Stack Edge device, you can create a Kubernetes cluster by configuring the compute. When the compute role is configured, the Kubernetes cluster including the master and worker nodes are all deployed and configured for you. This cluster is then used for workload deployment via `kubectl`, IoT Edge, or Azure Arc.

The Azure Stack Edge device is available as a 1-node configuration or a 2-node configuration that constitutes the infrastructure cluster. The Kubernetes cluster is separate from the infrastructure cluster and is deployed on top of the infrastructure cluster. The infrastructure cluster provides the persistent storage for your Azure Stack Edge device while the Kubernetes cluster is responsible solely for application orchestration.

The Kubernetes cluster comprises a master node and worker nodes. The Kubernetes nodes in a cluster are virtual machines that run your applications and cloud workflows.

- The Kubernetes master node is responsible for maintaining the desired state for your cluster. The master node also controls the worker node.
- The worker nodes run the containerized applications.

Kubernetes cluster on two-node device

The Kubernetes cluster on the 2-node device has one master node and two worker nodes. The 2-node device is highly available, and if one of the nodes fails, both the device and the Kubernetes cluster keep running. For more information on the Kubernetes cluster architecture, go to [Kubernetes core concepts](#).

On a 2-node Azure Stack Edge device, the Kubernetes master VM and a Kubernetes worker VM are running on node A of your device. On the node B, a single Kubernetes worker VM is running.

Each worker VM in the Kubernetes cluster is a pinned Hyper-V VM. A pinned VM is tied to the specific node it is running on. If the node A on the device fails, the master VM fails over to node B. But the worker VM on node A which is a pinned VM does not fail over to node B and vice-versa. Instead, the pods from the worker VM on node A are rebalanced onto node B.

In order for the rebalanced pods to have enough capacity to run on the device node B, the system enforces that no more than 50% of each ASE node's capacity be used during regular 2-node Azure Stack Edge cluster operations. This capacity usage is done on a best effort basis and there are circumstances (for example, workloads requiring unavailable GPU resources when they are rebalanced to ASE Node B) in which rebalanced pods may not have sufficient resources to run.

These scenarios are covered in detail in the next section on [Failure Modes and Behavior](#).

Failure modes and behavior

The Azure Stack Edge device nodes may fail under certain conditions. The various failure modes and the corresponding device responses are tabulated in this section.

Azure Stack Edge node failures or reboots

NODE	FAILURES	RESPONSES
Node A has failures (Node B has no failures)	<p>Following possible failures can occur:</p> <ul style="list-style-type: none"> • Both PSUs fail • One or both Port 3, Port 4 fail • Core component fails, includes motherboard, DIMM, OS disk • Entire node fails 	<p>Following responses are seen for each of these failures:</p> <ul style="list-style-type: none"> • Kubernetes master VM fails over from node A to node B • Master VM takes few minutes to come up on node B • Pods from node A are rebalanced on node B • GPU workloads keep running if GPU is available on node B
Node A reboots (Node B has no failures)	Node reboots	After node A completes rebooting and the worker VM is available, master VM will rebalance the pods from node B.
Node B has failures (Node A has no failures)	<p>Following possible failures can occur:</p> <ul style="list-style-type: none"> • Both PSUs fail • One or both Port 3, Port 4 fail • Core component fails, includes motherboard, DIMM, OS disk • Entire node fails 	<p>Following responses are seen for each of these failures:</p> <ul style="list-style-type: none"> • Kubernetes master VM rebalances pods from node B. This could take a few minutes.
Node B reboots (Node A has no failures)	Node reboots	After node B completes rebooting and the worker VM is available, master VM will rebalance the pods from node B.

Azure Stack Edge node updates

UPDATE TYPE	RESPONSES
Device node update	Rolling updates are applied to device nodes and the nodes will reboot.
Kubernetes service update	<p>Kubernetes service update includes:</p> <ul style="list-style-type: none"> • A failover of the Kubernetes master VM from device node A to device node B • A Kubernetes master update. • Kubernetes worker node updates (not necessarily in that order). <p>The entire update process could take 30 minutes or more, and during this window the Kubernetes cluster is available for any management operations (like deploying a new workload). Although pods will be drained from the device node while it is being updated, workloads may be offline for several seconds during this process.</p>

Next steps

- Learn more about Kubernetes storage on [Azure Stack Edge device](#).
- Understand the Kubernetes networking model on [Azure Stack Edge device](#).
- Deploy [Azure Stack Edge](#) in Azure portal.

What is the Azure Stack Edge Pro R?

9/21/2022 • 5 minutes to read • [Edit Online](#)

Azure Stack Edge Pro R is rugged, edge computing device designed for use in harsh environments. Azure Stack Edge Pro R is delivered as a hardware-as-a-service solution. Microsoft ships you a cloud-managed device that acts as network storage gateway and has a built-in Graphical Processing Unit (GPU) that enables accelerated AI-inferencing.

This article provides you an overview of the Azure Stack Edge Pro R solution, key capabilities, and the scenarios where you can deploy this device.

Key capabilities

Azure Stack Edge Pro R has the following capabilities:

CAPABILITY	DESCRIPTION
Rugged hardware	Rugged server class hardware designed for harsh environments. Device contained in a portable transit case.
Cloud-managed	Device and service are managed via the Azure portal.
Edge compute workloads	Allows analysis, processing, filtering of data. Supports VMs and containerized workloads. <ul style="list-style-type: none">For information on VM workloads, see VM overview on Azure Stack Edge.For containerized workloads, see Kubernetes overview on Azure Stack Edge
Accelerated AI inferencing	Enabled by an Nvidia T4 GPU. For more information, see GPU sharing on your Azure Stack Edge device .
Data access	Direct data access from Azure Storage Blobs and Azure Files using cloud APIs for additional data processing in the cloud. Local cache on the device is used for fast access of most recently used files.
Disconnected mode	Deploy, run, manage applications in offline mode. Disconnected mode supports offline upload scenarios. For more information, see Use Azure Stack Edge in disconnected mode
Supported file transfer protocols	Support for standard SMB, NFS, and REST protocols for data ingestion. For more information on supported versions, go to Azure Stack Edge Pro R system requirements .
Data refresh	Ability to refresh local files with the latest from cloud. For more information, see Refresh a share on your Azure Stack Edge .

CAPABILITY	DESCRIPTION
Double encryption	Use of self-encrypting drives provides the first layer of encryption. VPN provides the second layer of encryption. BitLocker support to locally encrypt data and secure data transfer to cloud over <i>https</i> . For more information, see Configure VPN on your Azure Stack Edge Pro R device .
Bandwidth throttling	Throttle to limit bandwidth usage during peak hours. For more information, see Manage bandwidth schedules on your Azure Stack Edge .
Easy ordering	Bulk ordering and tracking of the device via Azure Edge Hardware Center (Preview). For more information, see Order a device via Azure Edge Hardware Center .

Use cases

Here are the various scenarios where Azure Stack Edge Pro R can be used for rapid Machine Learning (ML) inferencing at the edge and preprocessing data before sending it to Azure.

- **Inference with Azure Machine Learning** - With Azure Stack Edge Pro R, you can run ML models to get quick results that can be acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models. For more information on how to use the Azure ML hardware accelerated models on the Azure Stack Edge Pro R device, see [Deploy Azure ML hardware accelerated models on Azure Stack Edge Pro R](#).
- **Preprocess data** - Transform data before sending it to Azure to create a more actionable dataset. Preprocessing can be used to:
 - Aggregate data.
 - Modify data, for example to remove personal data.
 - Subset data to optimize storage and bandwidth, or for further analysis.
 - Analyze and react to IoT Events.
- **Transfer data over network to Azure** - Use Azure Stack Edge Pro R to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

Components

The Azure Stack Edge Pro R solution comprises of an Azure Stack Edge resource, Azure Stack Edge Pro R rugged, physical device, and a local web UI.

- **Azure Stack Edge Pro R physical device** - A 1-node compute and storage device contained in a rugged transit case. An optional Uninterruptible Power Supply (UPS) is also available.



To procure a device, go to the Azure Edge Hardware Center and place an order. Azure Edge Hardware Center service lets you choose from a variety of Azure Stack Edge SKUs as per your business need. You can order multiple units of a device type, ship multiple devices to different locations, save addresses for future orders, and also track the status of your orders.

Once the order is delivered, you can configure your device and create an Azure Stack Edge resource to manage the device.

For more information, go to [Create an order for your Azure Stack Edge Pro R device](#).

- **Azure Stack Edge resource** – A resource in the Azure portal that lets you manage a rugged, Azure Stack Edge Pro R device from a web interface that you can access from different geographical locations. Use the Azure Stack Edge resource to create and manage resources, view, and manage devices and alerts, and manage shares.
- **Azure Stack Edge Pro R local web UI** - A browser-based local user interface on your Azure Stack Edge Pro R device primarily intended for the initial configuration of the device. Use the local web UI also to run diagnostics, shut down and restart the Azure Stack Edge Pro device, view copy logs, and contact Microsoft Support to file a service request.

The local web UI on the device currently supports the following languages with their corresponding language codes:

LANGUAGE	CODE	LANGUAGE	CODE	LANGUAGE	CODE
English {default}	en	Czech	cs	German	de
Spanish	es	French	fr	Hungarian	hu
Italian	it	Japanese	ja	Korean	ko
Dutch	nl	Polish	pl	Portuguese - Brazil	pt-br
Portuguese - Portugal	pt-pt	Russian	ru	Swedish	sv
Turkish	tr	Chinese - simplified	zh-hans	Chinese - traditional	zh-hant

Region availability

Azure Stack Edge Pro R physical device, Azure resource, and target storage account to which you transfer data do not all have to be in the same region.

- **Resource availability** - For a list of all the regions where the Azure Stack Edge resource is available, go to [Azure products available by region](#).
- **Device availability** - For a list of all the countries where the Azure Stack Edge Pro R device is available, go to [Availability](#) section in the [Azure Stack Edge Pro R](#) tab for [Azure Stack Edge Pro R pricing](#).
- **Destination Storage accounts** - The storage accounts that store the data are available in all Azure regions. The regions where the storage accounts store Azure Stack Edge Pro R data should be located close to where the device is located for optimum performance. A storage account located far from the device results in long latencies and slower performance.

Azure Stack Edge service is a non-regional service. For more information, see [Regions and Availability Zones in Azure](#). Azure Stack Edge service does not have dependency on a specific Azure region, making it resilient to zone-wide outages and region-wide outages.

For a discussion of considerations for choosing a region for the Azure Stack Edge service, device, and data storage, see [Choosing a region for Azure Stack Edge](#).

Next steps

- Review the [Azure Stack Edge Pro R system requirements](#).

Azure Stack Edge Pro R safety instructions

9/21/2022 • 9 minutes to read • [Edit Online](#)



READ SAFETY AND HEALTH INFORMATION

Read all the safety information in this article before you use your Azure Stack Edge Pro R device. Failure to follow instructions could result in fire, electric shock, injuries, or damage to your properties. Read all safety information below before using Azure Stack Edge Pro R.

Safety icon conventions

The following signal words for hazard alerting signs are:

ICON	DESCRIPTION
	DANGER: Indicates a hazardous situation that, if not avoided, will result in death or serious injury. WARNING: Indicates a hazardous situation that, if not avoided, could result in death or serious injury. CAUTION: Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

The following hazard icons are to be observed when setting up and running your Azure Stack Edge Pro R Edge device:

ICON	DESCRIPTION
	Read All Instructions First
! NOTICE:	Indicates information considered important, but not hazard-related.
	Hazard Symbol
	Tip Hazard
	Heavy Weight Hazard
	Electric Shock Hazard

ICON	DESCRIPTION
	No User Serviceable Parts. Do not access unless properly trained.
	Multiple power sources. Disconnect all power cords to remove all power from the equipment.
	Pinching points are present.
	Indicates hot components or surfaces.

Handling precautions and site selection



WARNING:

- Proper equipment (for instance, pallet jack) and personal protective equipment (PPE), for instance, gloves must be used when moving and handling the as-shipped device.



WARNING:

- Place the equipment on a flat, hard, and stable surface to avoid a potential tip or crushing hazard.
- Do not stack more than 2 devices on each other.
- Ensure system is secure prior to stacking.
- Do not relocate or move stacked devices.
- Do not stack devices that are energized with external cables.
- Ensure power cords are not crushed or damaged during stacking operations.
- Devices are not to be used as tables or workspaces.



CAUTION:

- Inspect the *as-received* device for damages. If the device enclosure is damaged, [contact Microsoft Support](#) to obtain a replacement. Do not attempt to operate the device.
- If you suspect the device is malfunctioning, [contact Microsoft Support](#) to obtain a replacement. Do not attempt to service the device.
- The device contains no user-serviceable parts. Hazardous voltage, current, and energy levels are present inside. Do not open. Return the device to Microsoft for servicing.



WARNING:

- Removing the power supply module of the UPS exposes energized parts within the UPS. Do not insert

foreign objects inside the power supply module compartment.

- Do not try to lift an Azure Stack Edge Pro R Edge device by yourself. An enclosure can weigh up between 52 kg and 93 kg (115 lbs and 205 lbs); use mechanical assistance or other suitable assistance when moving and lifting equipment. Conform to local occupational health and safety requirements when moving and lifting equipment.
- Do not attempt lifting the equipment without proper mechanical aid. Be aware that attempting to lift this weight can cause severe injuries.



WARNING:

- The system is designed to operate in a controlled environment. Choose a site that is:
 - Well-ventilated and away from sources of heat including direct sunlight and radiators.
 - Not exposed to moisture or rain.
 - Located in a space that minimizes vibration and physical shock. The system is designed for shock and vibration according to MIL-STD-810G.
 - Isolated from strong electromagnetic fields produced by electrical devices.
 - Provided with properly grounded outlets.
 - Provided with adequate space to access the power supply cord(s), because they serve as the product's main power disconnect.
- Ethernet cables are not provided with the product. To reduce electromagnetic interference, it is recommended that Cat 6 Shielded Twisted-pair (STP) cabling be used.
- Set up the equipment in a work area allowing for adequate air circulation around the equipment; ensure that the front and back covers are fully removed while the device is running.
- Ethernet cables are not provided with the product. To reduce electromagnetic interference, it is recommended that Cat 6 Shielded (STP) cabling be used.
- Install the equipment in temperature-controlled area free of conductive contaminants and allow for adequate air circulation around the equipment.
- Keep the equipment away from sources of liquid and excessively humid environments.
- Do not allow any liquid or any foreign object to enter the system. Do not place beverages or any other liquid containers on or near the system.

Heater precautions



WARNING:

- Automatic heater operation while the system is powered on may create a touch hazard due to high surface temperatures on the heater assembly cover. Do not touch this surface while the system is powered on. Allow a 10-minute cool down period after the system is powered off.



WARNING:

- When the system is powered on, automatic actuation of the rear plenum door may create a pinch-point hazard. Keep hands clear of this area when the system is powered on.

Electrical precautions



WARNING:

- Provide a safe electrical earth connection to the power supply cord. The alternating current (AC) cord has a three-wire grounding plug (a plug that has a grounding pin). This plug fits only a grounded AC outlet. Do not defeat the purpose of the grounding pin.
- Given that the plug on the power supply cord is the main disconnect device, ensure that the socket outlets are located near the device and are easily accessible.
- Unplug the power cord(s) (by pulling the plug, not the cord) and disconnect all cables if any of the following conditions exist:
 - The power cord or plug becomes frayed or otherwise damaged.
 - You spill something into the device casing.
 - The device is exposed to rain or excess moisture.
 - The device was dropped and the device casing is damaged.
 - You suspect the device needs service or repair.
- Permanently unplug the unit before you move it or if you think it has become damaged in any way.
- To prevent high leakage current, when a single transit case has more than one uninterrupted power supply (UPS), it is recommended that each UPS is connected to an independent branch circuit. However, in the event that a power distribution unit (PDU) or other device is used where the safety ground of each UPS relies on a single feeder grounding conductor of the PDU, the grounding terminal on the exterior of each UPS must also be used with a supplemental building ground conductor.

NOTE

If a PDU is used which already has a supplemental grounding conductor, using the additional grounding terminal on the UPS is not required.

- Provide a suitable power source with electrical overload protection to meet the following power specifications:
 - Voltage: 100 to 240 Volts AC
 - Current: 20 A, maximum per power cord. Power cord(s) are provided.
 - Frequency: 50 to 60 Hz



WARNING:

- For systems without an uninterrupted power supply (UPS), unplug all AC power cord(s) to completely remove AC power from the equipment.
- For systems with UPS, unplug all AC power cord(s) and use the UPS power switch to de-energize the System. UPS contains hazardous AC and DC voltages.
- If a system includes a UPS, the UPS was provided with a shielded input power cable. You must use the shielded input power cable, do not replace or modify the cord.



WARNING:

- For systems equipped with UPS, AC and/or DC voltage will always involve a potential risk of AC voltage at UPS output generated from either batteries or utility. To avoid equipment damage or personal injury, always assume that there may be voltage at the UPS output, even when disconnected from the primary power source.
- For systems equipped with UPS, all UPS energized external connections are female. Do not remove the case

or insert anything into these or any connectors on the UPS.



WARNING:

- Do not attempt to modify or use AC power cord(s) other than the ones provided with the equipment.



CAUTION:

- This equipment contains lithium coin cell and/or lithium iron phosphate batteries. Do not attempt servicing the equipment. Batteries in this equipment are not user serviceable. Risk of explosion if battery is replaced by an incorrect type.
- Removing the battery module of the UPS exposes energized parts within the UPS. Do not insert foreign objects inside the battery module compartment.

Regulatory information

This section contains regulatory information for Azure Stack Edge Pro R device, regulatory model number: Azure Stack Edge Pro R .

The Azure Stack Edge Pro R Edge device is designed for use with NRTL Listed (UL, CSA, ETL, etc.), and IEC/EN 60950-1 or IEC/EN 62368-1 compliant (CE marked) Information Technology equipment.

The device is designed to operate in the following environments:

ENVIRONMENT	SPECIFICATIONS
Temperature specifications	<ul style="list-style-type: none">• Storage temperature: -33°C–63°C (-28°F–145°F)• Continuous operation: 5°C–43°C (41°F–110°F)• Maximum temperature gradient (operating and storage): 20°C/h (68°F/h)
Relative humidity specifications	<ul style="list-style-type: none">• Storage: 5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times.• Operating: 5% to 85% relative humidity with 29°C (84.2°F) maximum dew point
Maximum altitude specifications	<ul style="list-style-type: none">• Operating (Without UPS): 15,000 ft (4,572 meters)• Operating (With UPS): 10,000 ft (3,048 meters)• Storage: 40,000 ft (12,192 meters)



NOTICE: Changes or modifications made to the equipment not expressly approved by Microsoft may void the user's authority to operate the equipment.

CANADA and USA:



NOTICE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment

in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3(A)/NMB-3(A) Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA United States: (800) 426-9400 Canada: (800) 933-4750

EUROPEAN UNION:

Request a copy of the EU Declaration of Conformity. Send email to CSI_Compliance@microsoft.com.



WARNING!

This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Disposal of waste batteries and electrical and electronic equipment:



This symbol on the product or its batteries or its packaging means that this product and any batteries it contains must not be disposed of with your household waste. Instead, it is your responsibility to hand this over to an applicable collection point for the recycling of batteries and electrical and electronic equipment. This separate collection and recycling will help to conserve natural resources and prevent potential negative consequences for human health and the environment due to the possible presence of hazardous substances in batteries and electrical and electronic equipment, which could be caused by inappropriate disposal. For more information about where to drop off your batteries and electrical and electronic waste, please contact your local city/municipality office, your household waste disposal service, or the shop where you purchased this product. Contact erecycle@microsoft.com for additional information on WEEE.

This product contains coin cell battery(ies).

Microsoft Ireland Sandyford Ind Est Dublin D18 KX32 IRL Telephone number: +353 1 295 3826 Fax number: +353 1 706 4110

Next steps

- [Prepare to deploy Azure Stack Edge Pro R Edge](#)

Azure Stack Edge Pro R system requirements

9/21/2022 • 8 minutes to read • [Edit Online](#)

This article describes the important system requirements for your Azure Stack Edge Pro R solution and for the clients connecting to Azure Stack Edge Pro R. We recommend that you review the information carefully before you deploy your Azure Stack Edge Pro R. You can refer back to this information as necessary during the deployment and subsequent operation.

The system requirements for the Azure Stack Edge Pro R include:

- **Software requirements for hosts** - describes the supported platforms, browsers for the local configuration UI, SMB clients, and any additional requirements for the clients that access the device.
- **Networking requirements for the device** - provides information about any networking requirements for the operation of the physical device.

Supported OS for clients connected to device

Here is a list of the supported operating systems for clients or hosts connected to your device. These operating system versions were tested in-house.

OPERATING SYSTEM/PLATFORM	VERSIONS
Windows Server	2016 2019
Windows	10
SUSE Linux	Enterprise Server 12 (x86_64)
Ubuntu	16.04.3 LTS
CentOS	7.0
Mac OS	10.14.1

Supported protocols for clients accessing device

Here are the supported protocols for clients accessing your device.

PROTOCOL	VERSIONS	NOTES
SMB	2.X, 3.X	SMB 1 isn't supported.
NFS	3.0, 4.1	Mac OS is not supported with NFS v4.1.

Supported storage accounts

Here is a list of the supported storage accounts for your device.

STORAGE ACCOUNT	NOTES
Classic	Standard
General Purpose	Standard; both V1 and V2 are supported. Both hot and cool tiers are supported.

Supported tiered storage accounts

When managed from Azure Stack, the following tiered storage accounts are supported with SMB/NFS/REST interfaces.

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob	
	Blob storage: Block Blob	Supported only for NAS

*Page blobs and Azure Files are currently not supported in Azure Stack. **Hot and cold tier do not exist in Azure Stack. Use the Azure PowerShell to move the data to the archive tier once the data is uploaded. For step-by-step instructions, go to [Use Azure PowerShell to set the blob tier](#)

Supported storage types

Here is a list of the supported storage types for the device.

FILE FORMAT	NOTES
Azure block blob	
Azure page blob	
Azure Files	

Supported browsers for local web UI

Here is a list of the browsers supported for the local web UI for the virtual device.

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Google Chrome	Latest version	
Microsoft Edge	Latest version	
Internet Explorer	Latest version	If enhanced security features are enabled, you may not be able to access local web UI pages. Disable enhanced security, and restart your browser.
FireFox	Latest version	
Safari on Mac	Latest version	

Networking port requirements

Port requirements for Azure Stack Edge Pro R

The following table lists the ports that need to be opened in your firewall to allow for SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access to your device. *Out* or *outbound* refers to the direction in which your Azure Stack Edge Pro R device sends data externally, beyond the deployment, for example, outbound to the internet.

Port No.	In or Out	Port Scope	Required	Notes
TCP 80 (HTTP)	Out	WAN	No	Outbound port is used for internet access to retrieve updates. The outbound web proxy is user configurable.
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable.
UDP 123 (NTP)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based NTP server.
UDP 53 (DNS)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based DNS server. We recommend using a local DNS server.
TCP 5985 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTP.
TCP 5986 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTPS.
UDP 67 (DHCP)	Out	LAN	In some cases See notes	This port is required only if you're using a local DHCP server.

Port No.	In or Out	Port Scope	Required	Notes
TCP 80 (HTTP)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. Accessing the local UI over HTTP will automatically redirect to HTTPS.
TCP 443 (HTTPS)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. This port is also used to connect Azure Resource Manager to the device local APIs, to connect Blob storage via REST APIs, and to the Security token service (STS) to authenticate via access and refresh tokens.
TCP 445 (SMB)	In	LAN	In some cases See notes	This port is required only if you are connecting via SMB.
TCP 2049 (NFS)	In	LAN	In some cases See notes	This port is required only if you are connecting via NFS.

Port requirements for IoT Edge

Azure IoT Edge allows outbound communication from an on-premises Edge device to Azure cloud using supported IoT Hub protocols. Inbound communication is only required for specific scenarios where Azure IoT Hub needs to push down messages to the Azure IoT Edge device (for example, Cloud To Device messaging).

Use the following table for port configuration for the servers hosting Azure IoT Edge runtime:

Port No.	In or Out	Port Scope	Required	Guidance
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound open for IoT Edge provisioning. This configuration is required when using manual scripts or Azure IoT Device Provisioning Service (DPS).

For complete information, go to [Firewall and port configuration rules for IoT Edge deployment](#).

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your Azure Stack Edge Pro R device and the service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. These changes require the network administrator to monitor and update firewall rules for your Azure Stack Edge Pro R as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on Azure Stack Edge Pro R fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

NOTE

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for gateway feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
<code>https://*.databoxedge.azure.com/*</code> <code>https://*.servicebus.windows.net/*</code> <code>https://login.microsoftonline.com</code> <code>https://login.microsoftonline.net</code>	Azure Stack Edge service Azure Service Bus Authentication Service - Azure Active Directory
<code>http://crl.microsoft.com/pki/*</code> <code>http://www.microsoft.com/pki/*</code>	Certificate revocation
<code>https://*.core.windows.net/*</code> <code>https://*.data.microsoft.com</code> <code>http://*.msftncsi.com</code> <code>https://www.msftconnecttest.com/connecttest.txt</code> <code>https://management.azure.com/</code>	Azure storage accounts and monitoring
<code>http://windowsupdate.microsoft.com</code> <code>http://*.windowsupdate.microsoft.com</code> <code>https://*.windowsupdate.microsoft.com</code> <code>http://*.update.microsoft.com</code> <code>https://*.update.microsoft.com</code> <code>http://*.windowsupdate.com</code> <code>http://download.microsoft.com</code> <code>http://*.download.windowsupdate.com</code> <code>http://wustat.windows.com</code> <code>http://ntservicepack.microsoft.com</code> <code>http://*.ws.microsoft.com</code> <code>https://*.ws.microsoft.com</code> <code>http://*.mp.microsoft.com</code>	Microsoft Update servers
<code>http://*.deploy.akamaitechnologies.com</code>	Akamai CDN
<code>https://azureprofilerfrontdoor.cloudapp.net</code>	Azure Traffic Manager
<code>http://*.data.microsoft.com</code>	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry

URL PATTERN	COMPONENT OR FUNCTIONALITY
http://<vault-name>.vault.azure.net:443	Key Vault

URL patterns for compute feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscr.io	
https://*.azurecr.io	Personal and third-party container registries (optional)
https://*.azure-devices.net	IoT Hub access (required)

URL patterns for gateway for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.us/* https://*.servicebus.usgovcloudapi.net/* https://login.microsoftonline.us	Azure Data Box Edge/ Azure Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.us	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.usgovcloudapi.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
https://(vault-name).vault.usgovcloudapi.net:443	Key Vault

URL patterns for compute for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscr.com	
https://*.azure-devices.us	IoT Hub access (required)
https://*.azuredcr.us	Personal and third-party container registries (optional)
https://*.docker.com	StorageClass (required)

Internet bandwidth

The devices are designed to continue to operate when your internet connection is slow or gets interrupted. In normal operating conditions, we recommend that you use:

- A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
- A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Use WAN throttling to limit your WAN throughput to 64 Mbps or higher.

Compute sizing considerations

Use your experience while developing and testing your solution to ensure there is enough capacity on your Azure Stack Edge Pro R device and you get the optimal performance from your device.

Factors you should consider include:

- **Container specifics** - Think about the following.
 - How many containers are in your workload? You could have a lot of lightweight containers versus a few resource-intensive ones.
 - What are the resources allocated to these containers versus what are the resources they are consuming?
 - How many layers do your containers share?
 - Are there unused containers? A stopped container still takes up disk space.
 - In which language are your containers written?
- **Size of the data processed** - How much data will your containers be processing? Will this data consume disk space or the data will be processed in the memory?
- **Expected performance** - What are the desired performance characteristics of your solution?

To understand and refine the performance of your solution, you could use:

- The compute metrics available in the Azure portal. Go to your Azure Stack Edge Pro R resource and then go to **Monitoring > Metrics**. Look at the **Edge compute - Memory usage** and **Edge compute - Percentage CPU** to understand the available resources and how are the resources getting consumed.
- The [Monitoring commands available via the PowerShell interface of the device](#).

Finally, make sure that you validate your solution on your dataset and quantify the performance on Azure Stack Edge Pro R before deploying in production.

Next step

- [Deploy your Azure Stack Edge Pro R](#)

Azure Stack Edge Pro R limits

9/21/2022 • 3 minutes to read • [Edit Online](#)

Consider these limits as you deploy and operate your Azure Stack Edge Pro R solution.

Azure Stack Edge Pro R service limits

- The storage account should be physically closest to the region where the device is deployed (can be different from where the service is deployed).
- Moving a Azure Stack Edge resource to a different subscription or resource group is not supported. For more details, go to [Move resources to new resource group or subscription](#).

Azure Stack Edge Pro R device limits

The following table describes the limits for the Azure Stack Edge Pro R device.

DESCRIPTION	VALUE
No. of files per device	100 million
No. of shares per container	1
Maximum no. of share endpoints and REST endpoints per device	24
Maximum no. of tiered storage accounts per device	24
Maximum file size written to a share	5 TB
Maximum number of resource groups per device	800

Azure storage limits

This section describes the limits for Azure Storage service, and the required naming conventions for Azure Files, Azure block blobs, and Azure page blobs, as applicable to the Azure Stack Edge service. Review the storage limits carefully and follow all the recommendations.

For the latest information on Azure storage service limits and best practices for naming shares, containers, and files, go to:

- [Naming and referencing containers](#)
- [Naming and referencing shares](#)
- [Block blobs and page blob conventions](#)

IMPORTANT

If there are any files or directories that exceed the Azure Storage service limits, or do not conform to Azure Files/Blob naming conventions, then these files or directories are not ingested into the Azure Storage via the Azure Stack Edge service.

Data upload caveats

Following caveats apply to data as it moves into Azure.

- We suggest that more than one device should not write to the same container.
- If you have an existing Azure object (such as a blob or a file) in the cloud with the same name as the object that is being copied, device will overwrite the file in the cloud.
- An empty directory hierarchy (without any files) created under share folders is not uploaded to the blob containers.
- You can copy the data using drag and drop with File Explorer or via command line. If the aggregate size of files being copied is greater than 10 GB, we recommend you use a bulk copy program such as Robocopy or rsync. The bulk copy tools retry the copy operation for intermittent errors and provide additional resiliency. If using Blob storage via REST, AzCopy or Azure Storage Explorer can be used.
- If the share associated with the Azure storage container uploads blobs that do not match the type of blobs defined for the share at the time of creation, then such blobs are not updated. For example, you create a block blob share on the device. Associate the share with an existing cloud container that has page blobs. Refresh that share to download the files. Modify some of the refreshed files that are already stored as page blobs in the cloud. You will see upload failures.
- After a file is created in the shares, renaming of the file isn't supported.
- Deletion of a file from a share does not delete the entry in the storage account.
- If using rsync to copy data, then `rsync -a` option is not supported.

Azure storage account size and object size limits

Here are the limits on the size of the data that is copied into storage account. Make sure that the data you upload conforms to these limits. For the most up-to-date information on these limits, go to [Azure blob storage scale targets](#) and [Azure Files scale targets](#).

SIZE OF DATA COPIED INTO AZURE STORAGE ACCOUNT	DEFAULT LIMIT
Block Blob and page blob	500 TB per storage account

Azure object size limits

Here are the sizes of the Azure objects that can be written. Make sure that all the files that are uploaded conform to these limits.

AZURE OBJECT TYPE	UPLOAD LIMIT
Block Blob	4.75 TB
Page Blob	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.
Azure Files	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

IMPORTANT

Creation of files (irrespective of the storage type) is allowed up to 5 TB. However, if you create a file whose size is greater than the upload limit defined in the preceding table, the file does not get uploaded. You have to manually delete the file to reclaim the space.

Next steps

- [Prepare to deploy Azure Stack Edge Pro R](#)

Azure Stack Edge Pro R technical specifications

9/21/2022 • 3 minutes to read • [Edit Online](#)

The hardware components of your Azure Stack Edge Pro R device adhere to the technical specifications outlined in this article. The technical specifications describe the Power supply units (PSUs), storage capacity, enclosures, and environmental standards.

Compute, memory specifications

The Azure Stack Edge Pro R device has the following specifications for compute and memory:

SPECIFICATION	VALUE
CPU type	Dual Intel Xeon Silver 4114 CPU
CPU: raw	20 total cores, 40 total vCPUs
CPU: usable	32 vCPUs
Memory type	Dell Compatible 16 GB RDIMM, 2666 MT/s, Dual rank
Memory: raw	256 GB RAM (16 x 16 GB)
Memory: usable	217 GB RAM

Compute acceleration specifications

A Graphics Processing Unit (GPU) is included on every device that enables Kubernetes, deep learning, and machine learning scenarios.

SPECIFICATION	VALUE
GPU	One nVidia T4 GPU For more information, see NVIDIA T4 .

Power supply unit specifications

The Azure Stack Edge Pro R device has two 100-240 V Power supply units (PSUs) with high-performance fans. The two PSUs provide a redundant power configuration. If a PSU fails, the device continues to operate normally on the other PSU until the failed module is replaced. The following table lists the technical specifications of the PSUs.

SPECIFICATION	550 W PSU
Maximum output power	550 W
Heat dissipation (maximum)	2891 BTU/hr
Frequency	50/60 Hz

SPECIFICATION	550 W PSU
Voltage range selection	Auto ranging: 115-230 V AC
Hot pluggable	Yes

Network specifications

The Azure Stack Edge Pro R device has four network interfaces, PORT1 - PORT4.

SPECIFICATION	DESCRIPTION
Network interfaces	2 x 1 GbE RJ45 PORT 1 is used as the management interface for initial setup and is static by default. After the initial setup is complete, you can use the interface for data with any IP address. However, on reset, the interface reverts to static IP. The other interface, PORT 2, which is user-configurable, can be used for data transfer, and is DHCP by default.
Network interfaces	2 x 25 GbE SFP28 These data interfaces on PORT 3 and PORT 4 can be configured as DHCP (default) or static.

Your Azure Stack Edge Pro R device has the following network hardware:

- **Mellanox dual port 25G ConnectX-4 channel network adapter** - PORT 3 and PORT 4.

For a full list of supported cables, switches, and transceivers for these network cards, go to [Mellanox dual port 25G ConnectX-4 channel network adapter compatible products](#).

Storage specifications

Azure Stack Edge Pro R devices have eight data disks and two M.2 SATA disks that serve as operating system disks. For more information, go to [M.2 SATA disks](#).

Storage for 1-node device

The following table has details for the storage capacity of the 1-node device.

SPECIFICATION	VALUE
Number of solid-state drives (SSDs)	8
Single SSD capacity	8 TB
Total capacity	64 TB
Total usable capacity*	~ 42 TB

*Some space is reserved for internal use.

Enclosure dimensions and weight specifications

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The following table lists the dimensions of the device and the UPS with the rugged case in millimeters and inches.

ENCLOSURE	MILLIMETERS	INCHES
Height	301.2	11.86
Width	604.5	23.80
Length	740.4	35.50

Enclosure weight

The weight of the device depends on the configuration of the enclosure.

ENCLOSURE	WEIGHT
Total weight of 1-node device + rugged case with end caps	~114 lbs

Enclosure environment specifications

This section lists the specifications related to the enclosure environment such as temperature, vibration, shock, and altitude.

SPECIFICATION	VALUE
Temperature range	0 – 43° C (operational)
Vibration	MIL-STD-810 Method 514.7* Procedure I CAT 4, 20
Shock	MIL-STD-810 Method 516.7* Procedure IV, Logistic
Altitude	Operational: 10,000 feet Non-operational: 40,000 feet

* All references are to MIL-STD-810G Change 1 (2014)

Next steps

- [Deploy your Azure Stack Edge](#)

Deployment checklist for your Azure Stack Edge Pro R device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This article describes the information that can be gathered ahead of the actual deployment of your Azure Stack Edge Pro R device.

Use the following checklist to ensure you have this information after you have placed an order for an Azure Stack Edge Pro R device and before you have received the device.

Deployment checklist

STAGE	PARAMETER	DETAILS
Device management	<ul style="list-style-type: none">Azure subscriptionResource providers registeredAzure Storage account	<ul style="list-style-type: none">Enabled for Azure Stack Edge Pro/Data Box Gateway, owner or contributor access.In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for Microsoft.DataBoxEdge and register. Repeat for Microsoft.Devices if deploying IoT workloads.Need access credentials.
Device installation	Power cables in the package. For US, an SVE 18/3 cable rated for 125 V and 15 Amps with a NEMA 5-15P to C13 (input to output) connector is shipped.	For more information, see the list of Supported power cords by country .
	<ul style="list-style-type: none">At least 1 X 1-GbE RJ-45 network cable for Port 1At least 1 X 25-GbE SFP+ copper cable for Port 3, Port 4	Customer needs to procure these cables. For a full list of supported network cables, switches, and transceivers for device network cards, see Cavium FastlinQ 41000 Series Interoperability Matrix and Mellanox dual port 25G ConnectX-4 channel network adapter compatible products .
Network readiness	Check to see how ready your network is for the deployment of an Azure Stack Edge device.	Use the Azure Stack Network Readiness Checker to test all needed connections.
First-time device connection	Laptop whose IPv4 settings can be changed. This laptop connects to Port 1 via a switch or a USB to Ethernet adaptor.	

Stage	Parameter	Details
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.
Network settings	<p>Device comes with 2 x 1-GbE, 4 x 25-GbE network ports.</p> <ul style="list-style-type: none"> Port 1 is used to configure management settings only. One or more data ports can be connected and configured. At least one data network interface from among Port 2 - Port 6 needs to be connected to the Internet (with connectivity to Azure). DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.
Compute network settings	<ul style="list-style-type: none"> Require 2 free, static, contiguous IPs for Kubernetes nodes, and 1 static IP for IoT Edge service. Require one additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	<ul style="list-style-type: none"> Web proxy server IP/FQDN, port Web proxy username, password 	
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	Configure primary and secondary NTP server on local network. If local server is not available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public Windows update server is used.
Device settings	<ul style="list-style-type: none"> Device fully qualified domain name (FQDN) DNS domain 	
(Optional) Certificates	If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.	Configure certificates only if you change device name and/or DNS domain.
VPN		

STAGE	PARAMETER	DETAILS
Encryption-at-rest	Recommend using automatically generated encryption key.	If using your own key, you need a 32 character long Base-64 encoded key.
Activation	Require activation key from the Azure Stack Edge Pro/ Data Box Gateway resource.	Once generated, the key expires in 3 days.

Next steps

- Prepare to deploy your [Azure Stack Edge Pro device](#).
- Use the [Azure Stack Edge Network Readiness Tool](#) to verify your network settings.

Tutorial: Prepare to deploy Azure Stack Edge Pro R

9/21/2022 • 13 minutes to read • [Edit Online](#)

This tutorial is the first in the series of deployment tutorials that are required to completely deploy Azure Stack Edge Pro R. This tutorial describes how to prepare the Azure portal to deploy an Azure Stack Edge resource. The tutorial uses a 1-node Azure Stack Edge Pro R device shipped with an Uninterruptible Power Supply (UPS).

You need administrator privileges to complete the setup and configuration process. The portal preparation takes less than 10 minutes.

In this tutorial, you learn how to:

- Create a new resource
- Get the activation key

Get started

To deploy Azure Stack Edge Pro R, refer to the following tutorials in the prescribed sequence.

TO DO THIS STEP	USE THESE DOCUMENTS
Preparation	These steps must be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information before and during the deployment.
Deployment prerequisites	These prerequisites validate the environment is ready for deployment.
Deployment tutorials	These tutorials are required to deploy your Azure Stack Edge Pro R device in production.
1. Prepare the Azure portal for device	Create and configure your Azure Stack Edge resource before you install an Azure Stack Box Edge physical device.
2. Install the device	Inspect and cable your physical device.
3. Connect to the device	Once the device is installed, connect to device local web UI.
4. Configure network settings	Configure network including the compute network and web proxy settings for your device.
5. Configure device settings	Assign a device name and DNS domain, configure update server and device time.
6. Configure security settings	Configure certificates, VPN, encryption-at-rest for your device. Use device generated certificates or bring your own certificates.

TO DO THIS STEP	USE THESE DOCUMENTS
7. Activate the device	Use the activation key from service to activate the device. The device is ready to set up SMB or NFS shares or connect via REST.
8. Configure compute	Configure the compute role on your device. A Kubernetes cluster is also created.

You can now begin to set up the Azure portal.

Deployment configuration checklist

Before you deploy your device, you need to collect information to configure the software on your Azure Stack Edge Pro device. Preparing some of this information ahead of time helps streamline the process of deploying the device in your environment. Use the [Azure Stack Edge Pro R deployment configuration checklist](#) to note down the configuration details as you deploy your device.

Prerequisites

Following are the configuration prerequisites for your Azure Stack Edge resource, your Azure Stack Edge device, and the datacenter network.

For the Azure Stack Edge resource

Before you begin, make sure that:

- Your Microsoft Azure subscription is enabled for an Azure Stack Edge resource. Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#).
- You have owner or contributor access at resource group level for the Azure Stack Edge, IoT Hub, and Azure Storage resources.
- To create an order in the Azure Edge Hardware Center, you need to make sure that the Microsoft.EdgeOrder provider is registered. For information on how to register, go to [Register resource provider](#).
- To create any Azure Stack Edge resource, you should have permissions as a contributor (or higher) scoped at resource group level. You also need to make sure that the `Microsoft.DataBoxEdge` provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create any IoT Hub resource, make sure that Microsoft.Devices provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create a Storage account resource, again you need contributor or higher access scoped at the resource group level. Azure Storage is by default a registered resource provider.
- You have admin or user access to Azure Active Directory Graph API. For more information, see [Azure Active Directory Graph API](#).
- You have your Microsoft Azure storage account with access credentials.

For the Azure Stack Edge device

Before you deploy a physical device, make sure that:

- You've [run the Azure Stack Network Readiness Checker tool](#) to check network readiness for your Azure Stack Edge device. You can use the tool to check whether your firewall rules are blocking access to any essential URLs for the service and verify custom URLs, among other tests. For more information, see

Check network readiness for your Azure Stack Edge device.

- You've reviewed the safety information for this device at: [Safety guidelines for your Azure Stack Edge device](#).
- You have received the physical device.
- You have access to a flat, stable, and level work surface where the device can rest safely.
- The site where you intend to set up the device has standard AC power from an independent source or a rack power distribution unit (PDU).

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured per the networking requirements for your Azure Stack Edge device. For more information, see [Azure Stack Edge Pro R System Requirements](#).
- For normal operating conditions of your device, you have:
 - A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
 - A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Create a new resource

If you have an existing Azure Stack Edge resource to manage your physical device, skip this step and go to [Get the activation key](#).

- [Azure Edge Hardware Center \(Preview\)](#)
- [Azure CLI](#)

Azure Edge Hardware Center (Preview) lets you explore and order a variety of hardware from the Azure hybrid portfolio including Azure Stack Edge Pro devices.

When you place an order through the Azure Edge Hardware Center, you can order multiple devices, to be shipped to more than one address, and you can reuse ship to addresses from other orders.

Ordering through Azure Edge Hardware Center will create an Azure resource that will contain all your order-related information. One resource each will be created for each of the units ordered. You will have to create an Azure Stack Edge resource after you receive the device to activate and manage it.

To place an order through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.
2. Select **+ Create a resource**. Search for and select **Azure Edge Hardware Center**. In the Azure Edge Hardware Center, select **Create**.

Home > Create a resource > Marketplace >

Azure Edge Hardware Center

Microsoft



Azure Edge Hardware Center

Microsoft
☆☆☆☆ 0.0 (0 ratings)

[Create](#)

Overview Plans Usage Information + Support Reviews

Use Azure Edge Hardware Center to order first-party Azure hardware that lets you build and run hybrid apps across datacenters, edge locations, remote offices and the cloud.

Azure Edge Hardware Center lets you choose from a variety of hardware as per your business need and helps you keep track of all the ordered hardware at a single place.

More offers from Microsoft [See All](#)

 Workspace Microsoft Virtual Machine Azure Virtual Desktop resource	 Microsoft HPC Pack 2012 R2 Microsoft Virtual Machine Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux workloads.	 Windows 10 IoT Core Services Microsoft Azure Service Commercialize your project with enterprise-grade security and support	 Web App + SQL Microsoft Azure Service Enjoy secure and flexible development, deployment, and scaling options for your web app
--	--	--	--

[Create](#) [Create](#) [Create](#) [Create](#)

3. Select a subscription, and then select **Next**.

Home > Create a resource > Marketplace > Azure Edge Hardware Center >

Get started ...

Get started [...](#) [X](#)

Info Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select a subscription

Select a subscription to manage deployed resources and costs.

Subscription [Contoso_USEast](#)

[Next](#)

4. To start your order, select **Order** beside the product family that you want to order - for example, **Azure Stack Edge**. If you don't see the product family, you may need to use a different subscription; select **Try selecting a different subscription**.

Get started



i Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select product family

Showing 1 product families for selected subscription: ExpressPod BVT (Creates order in BVT env)



Azure Stack Edge

Azure managed physical edge compute device

Order

Can't see the product family you are looking for? [Try selecting a different subscription.](#)

5. Select the shipping destination for your order.

Azure Edge Hardware Center



i Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select shipping destination



Azure Stack Edge

Order to be billed against subscription: Contoso_USWest ([Change](#))

Select the country/region where you would like your device to be shipped. *

United States ▼

Next

6. On the **Select Hardware** page, use the **Select** button to select the hardware product to order. For example, here **Azure Stack Edge Pro - GPU** was selected.

 Select Hardware ... X

Hardware family: Azure Stack Edge ([Change](#)) Subscription: Contoso_USWest Ship to country/region: United States

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Device specifications	<ul style="list-style-type: none"> • 1U rack mount device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Azure Private Edge Zones enabled 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Pro R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Portable, server class device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Specialized rugged casing tailored for harsh environments 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Mini R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Ultra-portable, WiFi enabled device with battery • Hardware accelerated ML using VPU • Specialized rugged casing tailored for harsh environments 	\$\$\$ USD	Select

After you select a hardware product, you'll select the device configuration to order. For example, if you chose Azure Stack Edge Pro - GPU, you can choose from Azure Stack Edge Pro - 1 GPU and Azure Stack Edge Pro - 2 GPU models.

7. Select the device configuration, and then choose **Select**. The available configurations depend on the hardware you selected. The screen below shows available configurations for Azure Stack Edge Pro - GPU devices.

If you're ordering Azure Stack Edge Mini R devices, which all have the same configuration, you won't see this screen.

Home >
Select Hardware ...

Hardware family: Azure Stack Edge ([Change](#)) Azure managed physical edge compute device

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Hardware specifications	<p>Azure Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. The device is powered with NVIDIA T4 GPUs to provide accelerated AI inferencing at the edge. You can choose from the available configurations with one or two GPUs basis your business need</p> <p>Select a configuration</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Usable compute</th> <th>Usable memory</th> <th>Usable storage</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> <tr> <td><input type="radio"/> Azure Stack Edge Pro - 2 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> </tbody> </table> <p>Learn more Azure Stack Edge Pro - GPU documentation</p>				Model	Usable compute	Usable memory	Usable storage	<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB	<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB
Model	Usable compute	Usable memory	Usable storage													
<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB													
<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB													

[Select](#)

The **Create order** wizard opens.

8. On the **Basics** tab, provide an **Order name**, **Resource group**, and **Region**. Then select **Next: Shipping + quantity >**.

Create order

X

Basics Shipping + quantity Notifications Tags Review + create

Hardware details

 Azure Stack Edge Pro - 1 GPU

Usable compute : 40 vCPU Usable memory : 102 GB

Usable storage : 4.2 TB

Order details

Order name *

Pro1GPUdevices

The selected subscription will be used to manage deployed resources and billing. Select or create a new resource group to organize and manage all your resources.

Subscription *

Contoso_USEast

Resource group *

USEast_ASE



[Create new](#)

Region *

East US



Review + create

< Previous

Next : Shipping + quantity >

Next, you'll add each ship to address you want to send devices to and then specify how many devices to send to each address. You can order up to 20 units (devices) per order.

9. On the **Shipping + quantity** tab, add each ship to address to send devices to:

- To add a new ship to address, select **Add a new address**.

A required **Address alias** field on the **New address** screen identifies the address for later use. Select **Add** when you finish filling in the address fields. Then use **Select address(es)** to add the address to your order.

- To use a ship to address from a previous order, or to use an address that you just added, choose **Select address(es)**. Then, on the **Select address(es)** screen, select one or more addresses, and choose **Select**.

<input type="checkbox"/>	Contact person	Address
<input checked="" type="checkbox"/>	Gus Poland 4255555555 gusp@contoso.com Contoso LE	contoso-redmond One Microsoft Way Building 52 Redmond WA 98152 United States
<input type="checkbox"/>	Gus Poland 4085555555 gusp@contoso.com Contoso LE	contoso-sunnyvale 1020 Enterprise Way Building 2 Sunnyvale CA 94089 United States
<input checked="" type="checkbox"/>	Claudia Olivares 4085555555 gusp@contoso.com Contoso LE	SVBldg2 1020 Enterprise Way Building 2 Sunnyvale

The **Shipping + quantity** tab now has a separate item for each ship to address.

Each order item name includes a name prefix (the order name followed by the address alias), with an item number for each device that is shipped to that address.

Create order

Basics **Shipping + quantity** Notifications Tags Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Su CA 94089 US	1	Pro1GPUDevicesSVBldg2-01 Order name Address alias Item #
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01

Review + create < Previous Next : Notifications >

- For each address, enter the **Quantity** of devices to ship on the **Shipping + quantity** tab.

When you enter a quantity of more than one, a **+n more** label appears after the order item name.

Create order

Basics **Shipping + quantity** Notifications Tags Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Sunnyva CA 94089 US	3	Pro1GPUDevicesSVBldg2-... +2 more [Delete]
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01 [Delete]

Add a new address Select address(es)

Review + create < Previous Next : Notifications >

- If you want to change the names of order items, select and click the order item name to open the **Rename order item** pane. If you're shipping more than one item to an address, select **+n more**.

You can make two types of name change:

- To use a different name prefix for all of the order items, edit the **Name prefix** and then select

Apply, as shown on the following screen.

- You can also edit the name of each order item individually.

When you finish, select **Done**.

Select **Next: Notifications** > to continue.

12. If you want to receive status notifications as your order progresses, enter the email address for each recipient on the **Notifications** tab.

To add an email address, enter the address, and select **Add**. You can add up to 20 email addresses.

The screenshot shows the 'Create order' interface. At the top, there's a breadcrumb navigation: Home > Select Hardware >. Below it is a title bar with 'Create order' and a close button ('X'). The main area has several tabs: Basics, Shipping + quantity, Notifications (which is highlighted with a red box), Tags, and Review + create. A note below the tabs states: 'We will update you regarding your order progress. You can specify up to 20 email address(es) to receive updates for your order status. Your subscription owner and admin will receive email notifications by default.' Under the 'Email' section, there's a text input field containing 'claudiao@contoso.com' and a blue 'Add' button. Below this, two email addresses are listed: 'gusp@contoso.com' and 'OpsMgmt@contoso.com', each with a 'Remove' link. At the bottom, there are three buttons: a blue 'Review + create' button (also highlighted with a red box), a light blue '< Previous' button, and a light blue 'Next : Tags >' button.

When you finish, select **Review + create** to continue.

13. On the **Review + create** tab:

- Review your order. The order is automatically validated when you open this screen. If you see a **Validation failed** banner, you'll have to fix the issues before you create the order.
- Review the **Privacy terms**, and select the check box to agree to them.
- Select **Create**.



Validation passed.

Basics Shipping + quantity Notifications Tags Review + create

Order name Pro1GPUdevices

Total hardware units 4

Total monthly service fee <Fee>

Total shipping fee <Fee>

Hardware details

Azure Stack Edge Pro - 1 GPU

Usable compute 40 vCPU

Usable memory 102 GB

Usable storage 4.2 TB

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Basics

Subscription Contoso_USEast

Resource Group USEast_ASE

Region East US

Notifications

Emails gusp@contoso.com, OpsMgmt@contoso.com

Shipping + quantity

▼ Total hardware units (4)

Shipping address	Order item name
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-01
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-02
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-03
contoso-sunnyvale, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicescontoso-su-01

Create

< Previous

Next >

During deployment, the order opens in the portal, with the status of each order item displayed. After deployment completes, you may need to click the Down arrow by **Deployment details** to see the status of individual items.

Resource	Type	Status	Operation details
SVBldg2	Microsoft.EdgeOrder/addresses	OK	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	OK	Operation details
Pro1GPUDevicesSunnyvale2-02	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-03	Microsoft.EdgeOrder/orderItems	OK	Operation details

- To view details for an order item, shown below, select the item in the **Resource** column of the deployment details.

Order item information			
Placed on	: 8/6/2021	Shipping address	1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US
Order name	: Pro1GPUDevices	Contact information	Claudia Olivares 4085550111, claudiao@contoso.com
View Updates			

Hardware information	
<p>Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage</p> <p>While your hardware arrives, configure your infrastructure. Learn more</p>	

- After a device ships (**Shipped** tag is green), a **Configure hardware** option is added to the item details. Select that option to create a management resource for the device in Azure Stack Edge.

The screenshot shows the Azure Edge Hardware Center interface for an order named "DemoOrderASAdd1-03". The "Overview" tab is selected. Key details include:

- Resource group (change):** USEast_ASE
- Location (change):** eastus2euap
- Subscription (change):** Contoso_USEast
- Subscription ID:** 1a23bc45-678d-90f1-2ghi-j34klm6n678o
- Tags (change):** Ordered, Shipped (highlighted with a red box), Delivered
- Order name:** Pro1GPUDevices
- Order item name:** Pro1GPUDevicesSunnyvale2-02 -03
- Placed on:** 6/24/2021
- Order name:** DemoOrderAS
- Shipping address:** abc street, xyz city, pqr state 7698798 US
- Contact information:** Anam Shaher, 8768789798, ashaheer@hotmail.com
- Hardware information:** Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage
- Configure hardware:** A button to configure and activate the hardware.

The subscription, resource group, and deployment area are filled in from the order, but you can change them.

The screenshot shows the "Create management resource" wizard for an Azure Stack Edge device.

Basics Step:

Device	Order resource name	Status
Azure Stack Edge Pro - 1 GPU	DemoOrderASAdd1-03	Delivered

PROJECT DETAILS: Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * ⓘ: Contoso_USEast

Resource group * ⓘ: USEast_ASE

INSTANCE DETAILS:

Name * ⓘ: (empty input field)

Deploy Azure resource in * ⓘ: (US) East US

Buttons at the bottom:

- Review + create
- Previous
- Next: Tags

After you activate the device, you'll be able to open the management resource from the item, and open the order item from the management resource.

Create management resources for devices

To manage devices that you order from the Azure Edge Hardware Center, you'll create management resources in Azure Stack Edge.

When a device is activated, the management resource is associated with the order item. You'll be able to open the order item from the management resource and open the management resource from the order item.

After a device is shipped, a **Configure hardware** link is added to the order item detail, giving you a direct way to open a wizard for creating a management resource. You can also use the **Create management resource** option in Azure Stack Edge.

To create a management resource for a device ordered through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.
2. There are two ways to get started creating a new management resource:
 - Through the Azure Edge Hardware Center: Search for and select **Azure Edge Hardware Center**. In the Hardware Center, display **All order items**. Select the item **Name**. In the item **Overview**, select **Configure hardware**.

The **Configure hardware** option appears after a device is shipped.



- In Azure Stack Edge: Search for and select **Azure Stack Edge**. Select **+ Create**. Then select **Create management resource**.



The **Create management resource** wizard opens.

3. On the **Basics** tab, enter the following settings:

SETTING	VALUE
Select a subscription ¹	Select the subscription to use for the management resource.
Resource group ¹	Select the resource group to use for the management resource.
Name	Provide a name for the management resource.
Deploy Azure resource in	Select the country or region where the metadata for the management resource will reside. The metadata can be stored in a different location than the physical device.

¹ An organization may use different subscriptions and resource groups to order devices than they use to manage them.

Create management resource

Azure Stack Edge

X

i After you've created this resource, you can activate an Azure Stack Edge device and manage it through this resource. If you don't have a physical device, you can order it through the [Azure Edge Hardware Center](#).

Basics Tags Review + create**PROJECT DETAILS**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * ⓘ

DataBox_Edge_Test

Resource group * ⓘ

myaserg

Create new

INSTANCE DETAILS

Name * ⓘ

myasetestorder

Deploy Azure resource in * ⓘ

(US) East US

Review + create

Previous

Next: Tags

Select **Review + create** to continue.

4. On the **Review + create** tab, review basic settings for the management resource and the terms of use. Then select **Create**.

If you started this procedure by clicking **Configure hardware** for a delivered item in an Azure Edge Hardware Center order, the device, order resource name, and order status are listed at the top of the screen.

Create management resource

X

Azure Stack Edge

All validations have passed.

Basics Tags Review + create

Device	Order resource name	Status
Azure Stack Edge Pro - 2 GPU	nidhitest1nidhiaddr-04	Delivered

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Basics

Subscription	ExpressPod BVT (Creates order in BVT env)
Resource group	nidhitest
Name	myNewDevice
Region	(US) East US

Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.

Create

Previous

Next

The **Create** button isn't available until all validation checks have passed.

5. When the process completes, the **Overview** pane for new resource opens.

Sunnyvale-ASE1GPUdevices-01 | Overview

Your deployment is complete

Deployment name: Sunnyvale-ASE1GPUdevices-01 Start time: 6/29/2021, 6:04:02 PM
Subscription: Azure Data Box testing Correlation ID: bee14110-d803-4ff4-82a5-6f7e1420d216
Resource group: ContosoEastRG

Deployment details (Download)

Resource	Type	Status	Operation details
Sunnyvale-ASE1GPUdevice	Microsoft.DataBoxEdge/...	OK	Operation details

Next steps

[Go to resource](#)

Get the activation key

After the Azure Stack Edge resource is up and running, you'll need to get the activation key. This key is used to activate and connect your Azure Stack Edge Pro device with the resource. You can get this key now while you are in the Azure portal.

- Select the resource that you created, and select **Overview**.

2. In the right pane, provide a name for the Azure Key Vault or accept the default name. The key vault name can be between 3 and 24 characters.

A key vault is created for each Azure Stack Edge resource that is activated with your device. The key vault lets you store and access secrets, for example, the Channel Integrity Key (CIK) for the service is stored in the key vault.

Once you've specified a key vault name, select **Generate activation key** to create an activation key.

The screenshot shows the Azure Stack Edge 'myasetest' overview page. The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring (Device events, Alerts, Metrics). The main content area has a heading 'Activate device once it arrives' with the sub-instruction 'Use the activation key to activate your device. Store the key safely in your Key Vault.' Below this, there's a text input field labeled 'Azure key vault name *' containing 'ase-myasetest-ed30d9ee38'. A red box highlights this input field. Next to it is a blue button labeled 'Generate activation key' with a red box around it. Below these fields is a note: 'Ensure that your infrastructure is configured. Refer steps to configure.' On the right, there's a section titled 'Edge services' with three cards: 'Virtual machines' (New), 'IoT Edge', and 'Cloud storage gateway'. The 'Cloud storage gateway' card includes the sub-instruction 'Seamlessly send your data to Azure Storage account.'

Wait a few minutes while the key vault and activation key are created. Select the copy icon to copy the key and save it for later use.

IMPORTANT

- The activation key expires three days after it is generated.
- If the key has expired, generate a new key. The older key is not valid.

Next steps

In this tutorial, you learned about Azure Stack Edge topics such as:

- Create a new resource
- Get the activation key

Advance to the next tutorial to learn how to install Azure Stack Edge.

[Install Azure Stack Edge](#)

Tutorial: Install Azure Stack Edge Pro R

9/21/2022 • 4 minutes to read • [Edit Online](#)

This tutorial describes how to install an Azure Stack Edge Pro R physical device. The installation procedure involves cabling the device.

The installation can take around 30 minutes to complete.

In this tutorial, you learn how to:

- Inspect the device
- Cable the device

Prerequisites

The prerequisites for installing a physical device as follows:

For the Azure Stack Edge resource

Before you begin, make sure that:

- You've completed all the steps in [Prepare to deploy Azure Stack Edge Pro R](#).
 - You've created an Azure Stack Edge resource to deploy your device.
 - You've generated the activation key to activate your device with the Azure Stack Edge resource.

For the Azure Stack Edge Pro R physical device

Before you deploy a device:

- Make sure that the device rests safely on a flat, stable, and level work surface.
- Verify that the site where you intend to set up has:
 - Standard AC power from an independent source

-OR-

- A rack power distribution unit (PDU). The device is shipped with an uninterruptible power supply (UPS)

For the network in the datacenter

Before you begin:

- Review the networking requirements for deploying Azure Stack Edge Pro R, and configure the datacenter network per the requirements. For more information, see [Azure Stack Edge Pro R networking requirements](#).
- Make sure that the minimum Internet bandwidth is 20 Mbps for optimal functioning of the device.

Inspect the device

This device is shipped as a single unit. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the device case for any damage. Open the case and inspect the device. If the case or the device appears to be damaged, contact Microsoft Support to help you assess whether the device is in good working order.

3. After the case is opened, make sure that you have:

- One single enclosure Azure Stack Edge Pro R device
- One uninterruptible power supply (UPS)
- 2 short power cables to connect device to the UPS
- 1 power cable to connect UPS to power source

If you didn't receive all of the items listed here, contact Azure Stack Edge Pro R support. The next step is to cable your device.

Cable the device

The following procedures explain how to cable your Azure Stack Edge Pro R device for power and network.

Before you start cabling your device, you need the following:

- Your Azure Stack Edge Pro R physical device on the installation site.
- One power cable.
- At least one 1-GbE RJ-45 network cable to connect to the management interface. There are two 1-GbE network interfaces, one management and one data, on the device.
- One 10/25-GbE SFP+ copper cable for each data network interface to be configured. At least one data network interface from among PORT 3 or PORT 4 needs to be connected to the Internet (with connectivity to Azure).
- Access to one power distribution unit (recommended).

NOTE

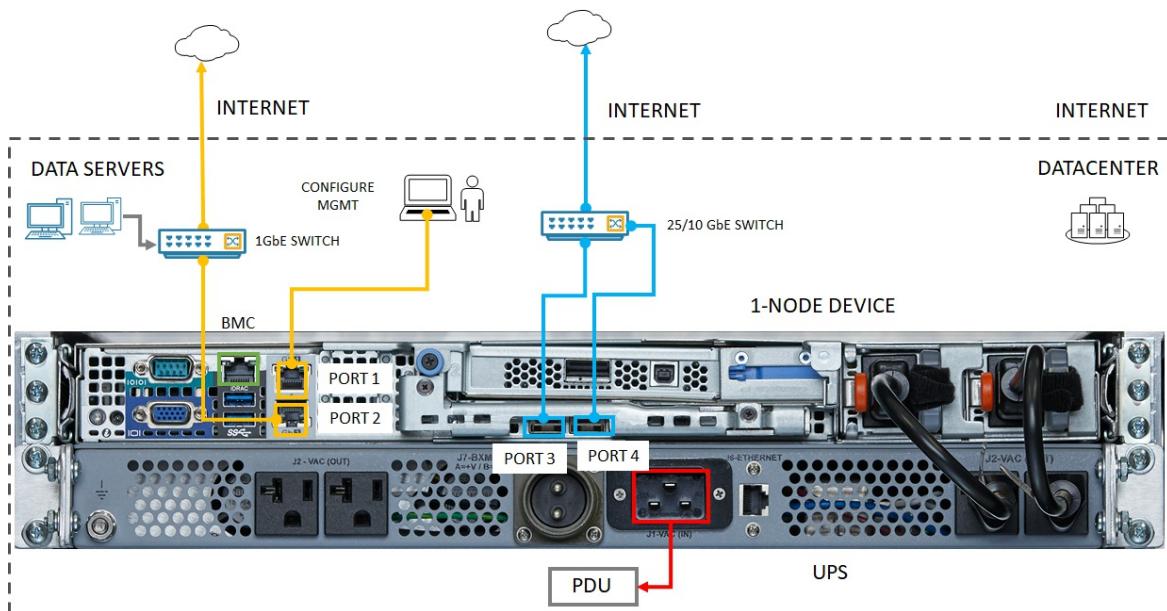
- If you are connecting only one data network interface, we recommend that you use a 25/10-GbE network interface such as PORT 3 or PORT 4 to send data to Azure.
- For best performance and to handle large volumes of data, consider connecting all the data ports.
- The Azure Stack Edge Pro R device should be connected to the datacenter network so that it can ingest data from data source servers.

On your Azure Stack Edge Pro R device:

- The front panel has disk drives and a power button.
 - There are 8 disk slots in the front of your device.
 - The device also has 2 X M.2 SATA disks inside that serve as operating system disks.
- The back plane includes redundant power supply units (PSUs).
- The back plane has four network interfaces:
 - Two 1-Gbps interfaces.
 - Two 25-Gbps interfaces that can also serve as 10-Gbps interfaces.
 - A baseboard management controller (BMC).

Take the following steps to cable your device for power and network.

1. Identify the various ports on the back plane of your device.



2. Locate the disk slots and the power button on the front of the device.



3. Connect one end of the power cord to the UPS. Attach the other end of the power cord to the rack power distribution unit (PDUs).

4. Press the power button to turn on the device.

5. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. PORT 1 is the dedicated management interface.

6. Connect one or more of PORT 2, PORT 3, or PORT 4 to the datacenter network/Internet.

- If connecting PORT 2, use the RJ-45 network cable.
- For the 10/25-GbE network interfaces, use the SFP+ copper cables.

NOTE

Using USB ports to connect any external device, including keyboards and monitors, is not supported for Azure Stack Edge devices.

Next steps

In this tutorial, you learned about Azure Stack Edge Pro R topics such as how to:

- Unpack the device
- Cable the device

Advance to the next tutorial to learn how to connect to your device.

[Connect to Azure Stack Edge Pro R](#)

Tutorial: Connect to Azure Stack Edge Pro R

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how you can connect to your Azure Stack Edge Pro R device by using the local web UI.

The connection process can take around 5 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Connect to a physical device

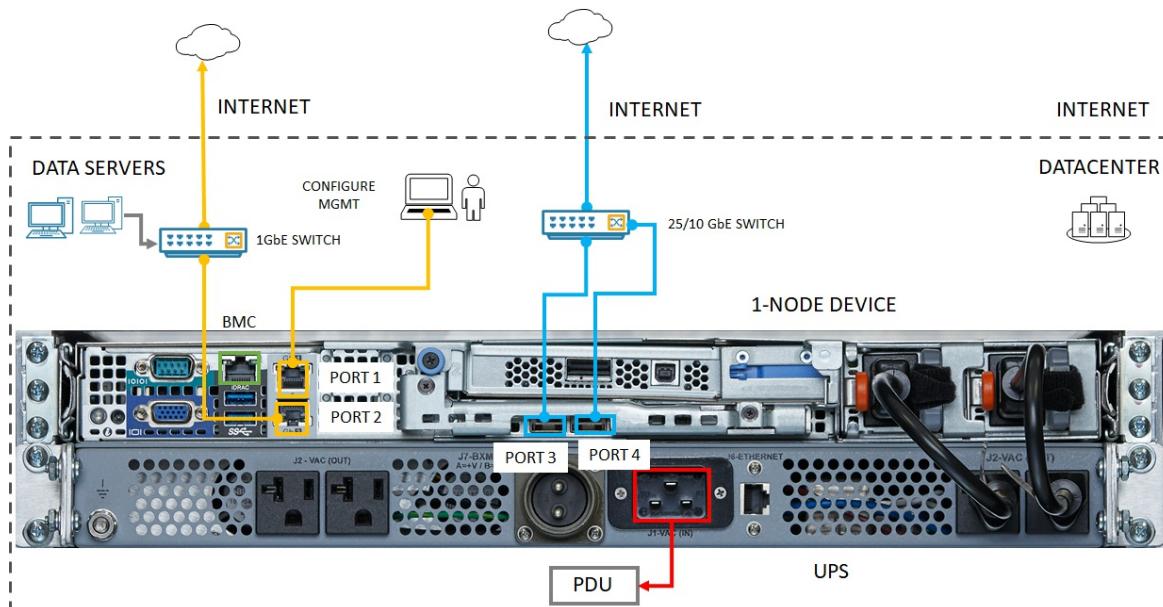
Prerequisites

Before you configure and set up your Azure Stack Edge Pro R device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro R](#).
- You've run the Azure Stack Network Readiness Checker tool to verify that your network meets Azure Stack Edge requirements. For instructions, see [Check network readiness for Azure Stack Edge devices](#).

Connect to the local web UI setup

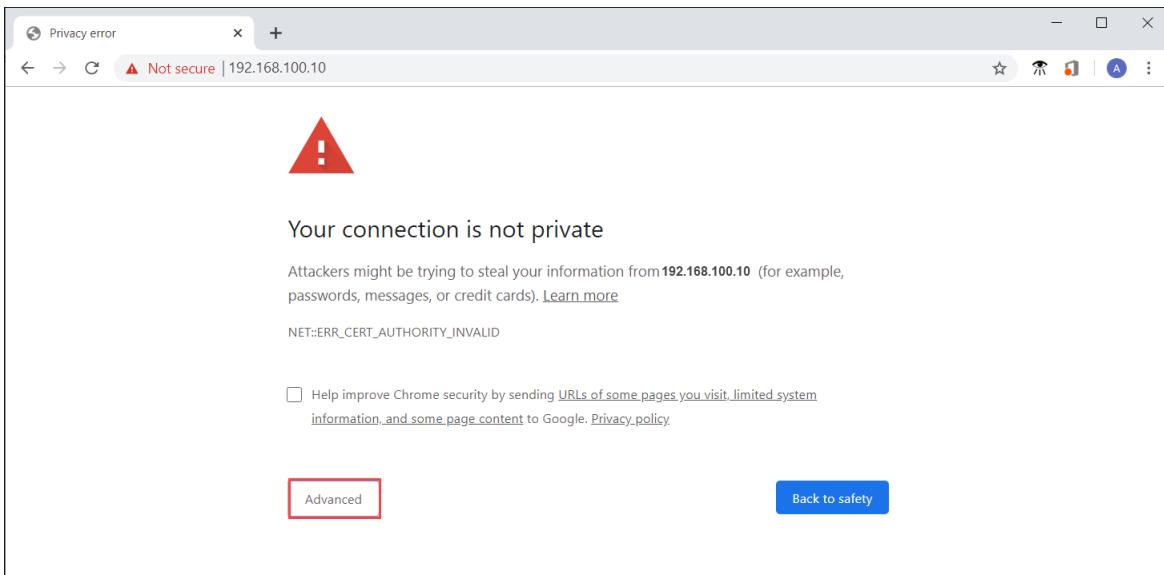
1. Configure the Ethernet adapter on your computer to connect to the Azure Stack Edge Pro R device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
2. Connect the computer to PORT 1 on your device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter. Use the following illustration to identify PORT 1 on your device.



3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>.

This action may take a few minutes after you've turned on the device.

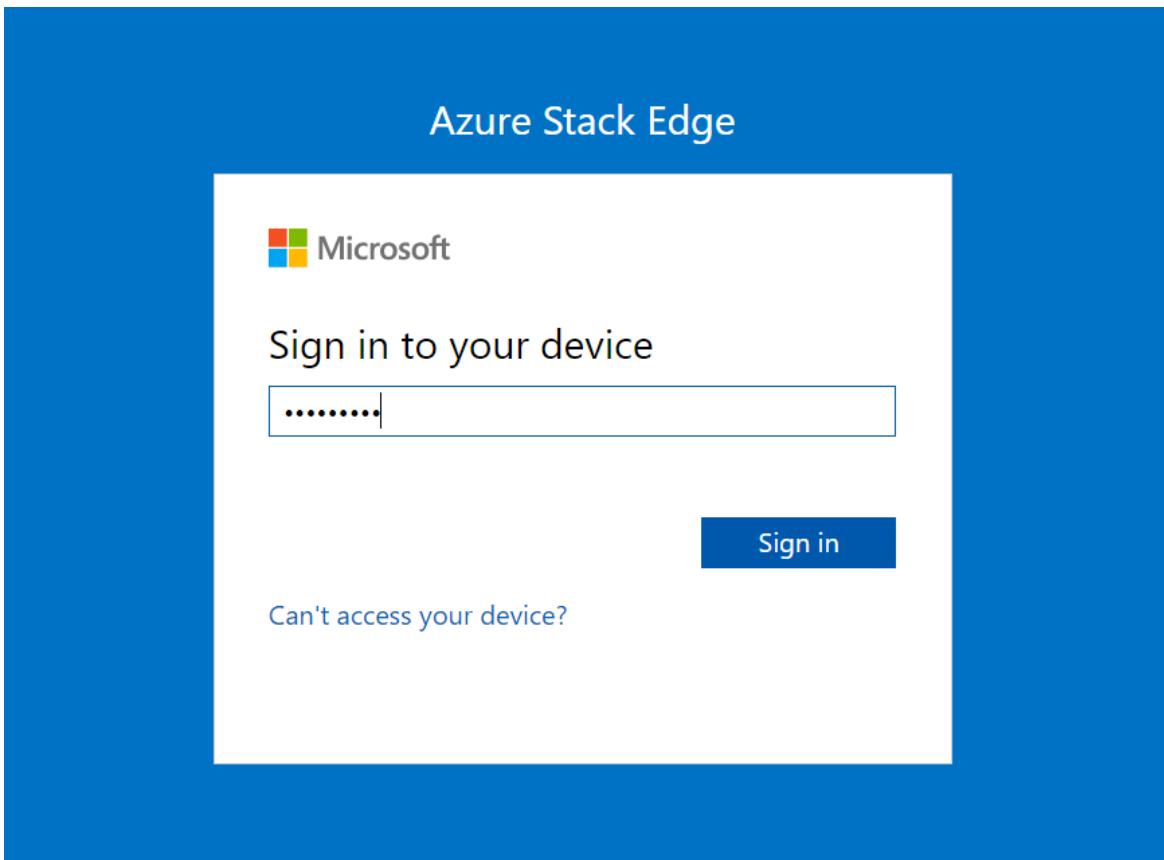
You see an error or a warning indicating that there is a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters.

You're now at the **Overview** page of your device. The next step is to configure the network settings for your device.

Next steps

In this tutorial, you learned about:

- Prerequisites

- Connect to a physical device

To learn how to configure network settings on your Azure Stack Edge Pro R device, see:

[Configure network](#)

Tutorial: Configure network for Azure Stack Edge Pro R

9/21/2022 • 5 minutes to read • [Edit Online](#)

This tutorial describes how to configure network for your Azure Stack Edge Pro R device by using the local web UI.

The connection process can take around 20 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure network
- Enable compute network
- Configure web proxy

Prerequisites

Before you configure and set up your Azure Stack Edge Pro R device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro R](#).
- You've connected to the local web UI of the device as detailed in [Connect to Azure Stack Edge Pro R](#)

Configure network

Your **Get started** page displays the various settings that are required to configure and register the physical device with the Azure Stack Edge service.

Follow these steps to configure the network for your device.

1. In the local web UI of your device, go to the **Get started** page.
2. On the **Network** tile, select **Configure** to go to the **Network** page.

On your physical device, there are four network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3 and PORT 4 are all 10/25-Gbps network interfaces. PORT 1 is automatically configured as a management-only port, and PORT 2 to PORT 4 are all data ports. The **Network** page is as shown below.

The screenshot shows the 'Network' configuration page for an Azure Stack Edge Pro R device with 1 GPU. The left sidebar has a 'CONFIGURATION' section with tiles for Overview, Get started (highlighted with a red box), Network (also highlighted with a red box), Compute, Web proxy, Device, Update server, Time, and Certificates. The main content area is titled 'Network' and shows the 'DBE-4N5WN23' device ID. It has a 'Network interfaces' table with the following data:

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	4C-D9-8F-BB-27-86
Port 2	-	-	-	
Port 3	-	-	-	
Port 4	-	-	-	

At the bottom are buttons for '< Back to Get started' and 'Next: Compute >' (also highlighted with a red box).

3. To change the network settings, select a port and in the right pane that appears, modify the IP address, subnet, gateway, primary DNS, and secondary DNS.

- If you select Port 1, you can see that it is preconfigured as static.

Network settings (Port 1)

* IP settings

DHCP Static

* Subnet mask

255.255.255.0 ✓

Gateway

Primary DNS

Secondary DNS

Serial number	IP address	MAC address
4N5WN23	192.168.100.10 ✓	4C-D9-8F-BB-27-86

Apply

- If you select Port 2, Port 3, or Port 4, all of these ports are configured as DHCP by default.



Network settings (Port 3)

* IP settings

DHCP Static

Subnet mask

255.255.0.0

Gateway

Primary DNS

5.5.5.1

Secondary DNS

Serial number	IP address	MAC address
4N5WN23	5.5.73.156	B8-59-9F-F7-CC-BB

Apply

As you configure the network settings, keep in mind:

- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.
- If DHCP isn't enabled, you can assign static IPs if needed.
- You can configure your network interface as IPv4.
- Network Interface Card (NIC) Teaming or link aggregation is not supported with Azure Stack Edge.
- Serial number for any port corresponds to the node serial number.

NOTE

If you need to connect to your device from an outside network, see [Enable device access from outside network](#) for additional network settings.

Once the device network is configured, the page updates as shown below.

Azure Stack Edge Pro R (1 GPU)

Network
DBE-4N5WN23

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	4C-D9-8F-BB-27-86
Port 2	10.128.26.140	255.255.252.0	10.128.24.1	4C-D9-8F-BB-27-87
Port 3	5.5.73.156	255.255.0.0	-	B8-59-9F-F7-CC-BB
Port 4	5.5.73.155	255.255.0.0	-	B8-59-9F-F7-CC-BA

< Back to Get started | Next: Compute >

NOTE

We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has activated with the service, and then change. You can then view the IPs of all the adapters in the **Device properties** in the Azure portal for your service.

After you have configured and applied the network settings, select **Next: Compute** to configure compute network.

Enable compute network

Follow these steps to enable compute and configure compute network.

1. In the **Compute** page, select a network interface that you want to enable for compute.

Azure Stack Edge Pro R (1 GPU)

Compute
DBE-4N5WN23

Configure one network interface on your device for compute. Use this network interface to connect to any compute modules running on your device.

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.128.44.0	No
Port 3	5.5.0.0	No
Port 4	5.5.0.0	No

< Back to Get started | Next: Web proxy >

2. In the **Network settings** dialog, select **Enable**. When you enable compute, a virtual switch is created on your device on that network interface. The virtual switch is used for the compute infrastructure on the device.
3. Assign **Kubernetes node IPs**. These static IP addresses are for the compute VM.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. Given Azure Stack Edge is a 1-node device, a minimum of 2 contiguous IPv4 addresses are provided. These IP addresses must be in the same network where you enabled compute and the virtual switch was created.

IMPORTANT

Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).

4. Assign **Kubernetes external service IPs**. These are also the load balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside of the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Pro R Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

5. Select **Apply**.



Network settings (Port2)

* Enable for compute

If you select a new interface for compute, this action moves any virtual machines to the new interface and the previous interface is disabled.

Compute IPs

For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs

Enter a contiguous range of 2 static IPs for your device.

Kubernetes external service IPs

Specify the static IP range for services exposed outside of Kubernetes cluster.

6. The configuration takes a couple minutes to apply and you may need to refresh the browser. You can see that the specified port is enabled for compute.

The screenshot shows the Azure Stack Edge Pro R (1 GPU) configuration interface. The left sidebar has a red box around the 'Compute' section. The main area shows a table of network ports:

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.128.44.0	Yes
Port 3	5.5.0.0	No
Port 4	5.5.0.0	No

At the bottom, there are buttons for 'Back to Get started' and 'Next: Web proxy >'. The 'Compute' section header also has a red box around it.

Select **Next: Web proxy** to configure web proxy.

Configure web proxy

This is an optional configuration.

IMPORTANT

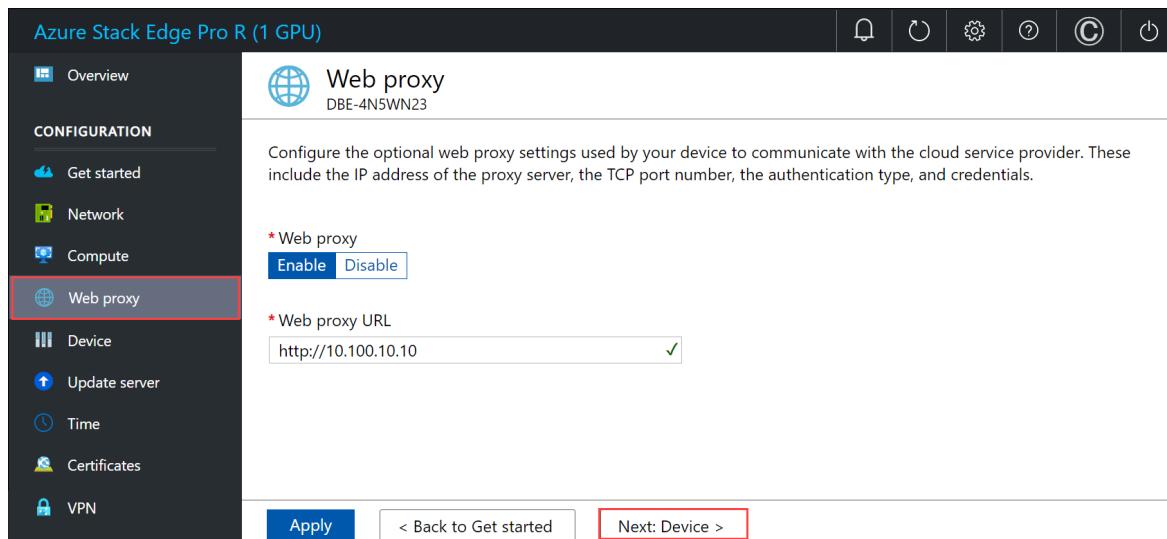
Proxy-auto config (PAC) files are not supported. A PAC file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. Proxies that try to intercept and read all the traffic (then re-sign everything with their own certification) aren't compatible since the proxy's certificate is not trusted. Typically transparent proxies work well with Azure Stack Edge Pro R. Non-transparent web proxies are not supported.

1. On the **Web proxy settings** page, take the following steps:

a. In the **Web proxy URL** box, enter the URL in this format:

`http://host-IP address or FQDN:Port number`. HTTPS URLs are not supported.

b. To validate and apply the configured web proxy settings, select **Apply**.



2. After the settings are applied, select **Next: Device**.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Configure network
- Enable compute network
- Configure web proxy

To learn how to set up your Azure Stack Edge Pro R device, see:

[Configure device settings](#)

Tutorial: Configure the device settings for Azure Stack Edge Pro R

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you configure device related settings for your Azure Stack Edge Pro R device. You can set up your device name, update server, and time server via the local web UI.

The device settings can take around 5-7 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

Prerequisites

Before you configure device related settings on your Azure Stack Edge Pro R device, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro R](#).
 - You've configured network and enabled and configured compute network on your device as detailed in [Tutorial: Configure network for Azure Stack Edge Pro R](#) .

Configure device settings

Follow these steps to configure device related settings:

1. On the **Device** page, take the following steps:
 - a. Enter a friendly name for your device. The friendly name must contain from 1 to 13 characters and can have letter, numbers, and hyphens.
 - b. Provide a **DNS domain** for your device. This domain is used to set up the device as a file server.
 - c. To validate and apply the configured device settings, select **Apply**.

The screenshot shows the Azure Stack Edge Pro R (1 GPU) Device configuration interface. The 'Device' tab is selected in the left sidebar. In the main area, under 'Device name', the 'Name' field is set to 'myasepro1' and the 'DNS domain' field is set to 'wdshcsso.com'. Under 'Device endpoints', there is a table with the following data:

Service	Certificate Required	Endpoint
SMB server	No	\dbe-4n5wn23.microsoftdatabox.com\[Share name]
NFS server	No	\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.dbe-4n5wn23.microsoftdatabox.com
Azure Resource Manager	Yes	https://management.dbe-4n5wn23.microsoftdatabox.com
Blob Storage	Yes	https://[Account name].blob.dbe-4n5wn23.microsoftdatabox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	No	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.

At the bottom, there are buttons for 'Apply', '< Back to Get started', and 'Next: Update server >'.

If you have changed the device name and the DNS domain, the automatically generated self-signed certificates on the device will not work. You need to choose one of the following options when you configure certificates.:.

- Generate and download the device certificates.
- Bring your own certificates for the device including the signing chain.

Warning

If you change the device name or DNS domain, you must upload new certificates for the device to work properly.

Apply

Cancel

- When the device name and the DNS domain are changed, the SMB endpoint is created.
- After the settings are applied, select **Next: Update server**.

Device name
Assign a friendly name and DNS domain for the device.

* Name: myasepro1
* DNS domain: wdshcsso.com

Device endpoints
Use these device endpoints to reach the following services. Some services require a certificate. For those services, certificates must be uploaded for the endpoint to be valid.

Service	Certificate Required	Endpoint
SMB server	No	\myasepro1.wdshcsso.com\Share name
NFS server	No	\Device IP address\Share name
Azure Resource Manager login	Yes	https://login.dbe-4n5wn23.microsoftbox.com
Azure Resource Manager	Yes	https://management.dbe-4n5wn23.microsoftbox.com
Blob Storage	Yes	https://[Account name].blob.dbe-4n5wn23.microsoftbox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	No	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.

Buttons: Apply, < Back to Get started, Next: Update server >

Configure update

- On the **Update** page, you can now configure the location from where to download the updates for your device.
 - You can get the updates directly from the **Microsoft Update server**.

Update server
myasepro1

Configure update server for your device.

* Select update server type
Microsoft Update (default)

Buttons: Apply, < Back to Get started, Next: Time >

You can also choose to deploy updates from the **Windows Server Update services (WSUS)**. Provide the path to the WSUS server.

The screenshot shows the Azure Stack Edge Pro R (1 GPU) configuration interface. On the left, a sidebar lists various configuration options: Overview, Get started, Network, Compute, Web proxy, Device, Update server (which is highlighted with a red border), and Time. The main content area is titled 'Update server' and shows the user 'myasepro1'. It provides instructions to configure the update server for the device. Two fields are highlighted with red boxes: 'Select update server type' (set to 'Windows Server Update Services') and 'Server URI' (containing 'http://FL319.guest.corp.microsoft.com:8530'). A green checkmark is present next to the server URI. At the bottom, there are buttons for 'Apply', '< Back to Get started', and 'Next: Time >'.

NOTE

If a separate Windows Update server is configured and if you choose to connect over *https* (instead of *http*), then signing chain certificates required to connect to the update server are needed. For information on how to create and upload certificates, go to [Manage certificates](#).

For working in a disconnected mode such as your Azure Stack Edge device tiering to Modular Data Center, enable WSUS option. During activation, the device scans for updates and if the server is not set up, then the activation will fail.

2. Select **Apply**.
3. After the update server is configured, select **Next: Time**.

Configure time

Follow these steps to configure time settings on your device.

IMPORTANT

Though the time settings are optional, we strongly recommend that you configure a primary NTP and a secondary NTP server on the local network for your device. If local server is not available, public NTP servers can be configured.

NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

1. On the **Time** page, you can select the time zone, and the primary and secondary NTP servers for your device.
 - a. In the **Time zone** drop-down list, select the time zone that corresponds to the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. In the **Primary NTP server** box, enter the primary server for your device or accept the default value of time.windows.com. Ensure that your network allows NTP traffic to pass from your datacenter to the internet.
 - c. Optionally, in the **Secondary NTP server** box, enter a secondary server for your device.
 - d. To validate and apply the configured time settings, select **Apply**.

The screenshot shows the Azure Stack Edge Pro R configuration interface. On the left, a sidebar lists several configuration options: Overview, Get started, Network, Compute, Web proxy, Device, Update server, Time (which is selected and highlighted with a red box), Certificates, and VPN. The main content area is titled 'Time' and shows the device's current time as '10/16/2020 7:12:34 AM'. It includes fields for 'Time zone' (set to '(UTC-08:00) Pacific Time (US & Canada)'), 'Primary NTP server' (set to 'time.windows.com'), and 'Secondary NTP server' (set to '10.100.10.20'). At the bottom are 'Apply' and 'Next: Certificates >' buttons, with 'Next: Certificates >' also highlighted with a red box.

2. After the settings are applied, select **Next: Certificates**.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

To learn how to configure certificates for your Azure Stack Edge Pro R device, see:

[Configure certificates](#)

Tutorial: Configure certificates for your Azure Stack Edge Pro R

9/21/2022 • 4 minutes to read • [Edit Online](#)

This tutorial describes how you can configure certificates for your Azure Stack Edge Pro R device by using the local web UI.

The time taken for this step can vary depending on the specific option you choose and how the certificate flow is established in your environment.

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device
- Configure VPN
- Configure encryption-at-rest

Prerequisites

Before you configure and set up your Azure Stack Edge Pro R device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro R](#).
- If you plan to bring your own certificates:
 - You should have your certificates ready in the appropriate format including the signing chain certificate. For details on certificate, go to [Manage certificates](#)

Configure certificates for device

1. In the **Certificates** page, you will configure your certificates. Depending on whether you changed the device name or the DNS domain in the **Device** page, you can choose one of the following options for your certificates.
 - If you have not changed the device name or the DNS domain in the earlier step, then you can skip this step and proceed to the next step. The device has automatically generated self-signed certificates to begin with.
 - If you changed the device name or DNS domain, you will see that the status of certificates will show as **Not valid**.

Name	Status	Expiration date	Thumbprint
Node (4N5WN23)	⚠️ Not valid	10/15/2022	DCD42D3536F1E74A615FF97E3AA486C4DBFBFAE9
Azure Resource Manager	⚠️ Not valid	10/15/2022	33F4EA8E382F953380C43C362E72939CEC244D
Blob storage	⚠️ Not valid	10/15/2022	2607EDEB5B884362A7DCCEEB5067014F50FAB337
Local web UI	⚠️ Not valid	10/15/2022	2607EDEB5B884362A7DCCEEB5067014F50FAB337
IoT device root CA	⚠️ Not present	-	-
IoT device CA	⚠️ Not present	-	-
IoT device Key	⚠️ Not present	-	-
Edge container registry certificate	⚠️ Not present	-	-
Edge container registry key	⚠️ Not present	-	-

Select a certificate to view the details of the status.

Local web UI has following errors:-

- Certificate with subject name CN=dbe-4n5wn23.microsoftdatabox.com does not have the correct subject name or subject alternative names for Appliance Endpoint certificate. Check the certificate you have uploaded and if needed bring in a new certificate.

This is because the certificates do not reflect the updated device name and DNS domain (that are used in subject name and subject alternative). To successfully activate your device, you can bring your own signed endpoint certificates and the corresponding signing chains. You first add the signing chain and then upload the endpoint certificates. For more information, go to [Bring your own certificates on your Azure Stack Edge Pro R device](#).

- If you changed the device name or DNS domain, and you do not bring your own certificates, then the activation will be blocked.

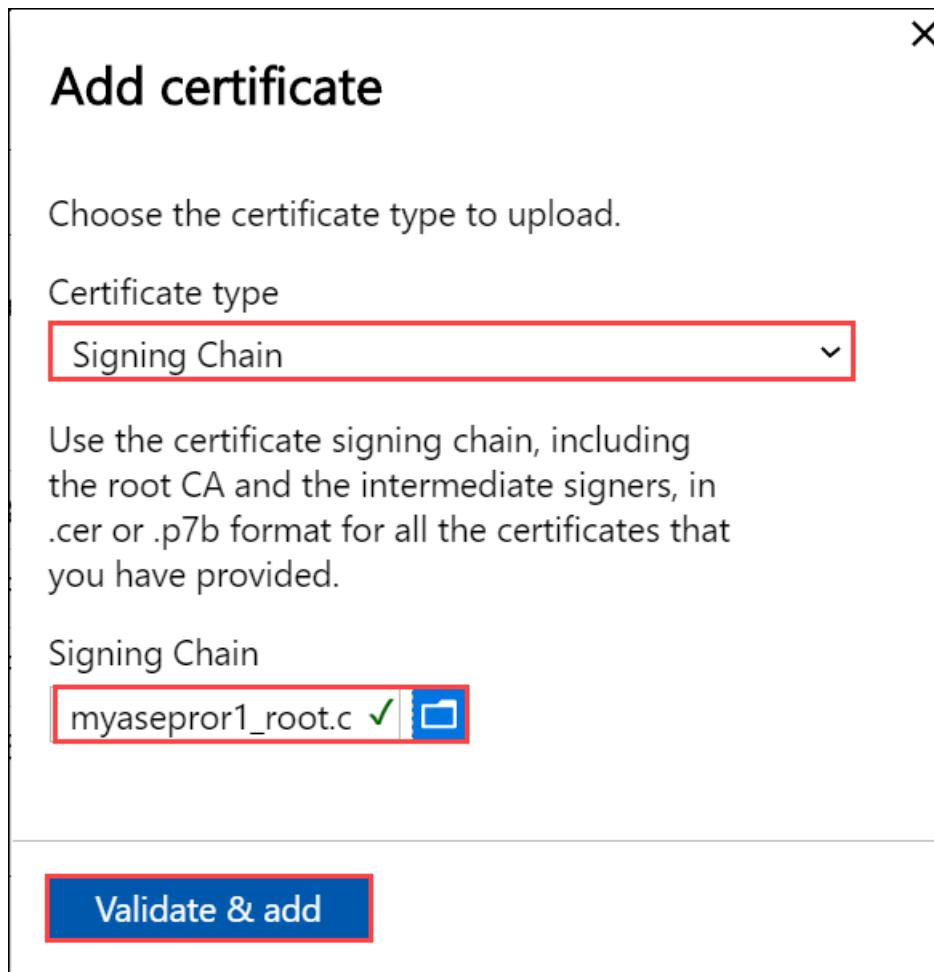
Bring your own certificates

Follow these steps to add your own certificates including the signing chain.

- To upload certificate, on the Certificate page, select + Add certificate.

Name	Status	Expiration date	Thumbprint	Download
Node (4N5WN23)	✓ Valid	10/16/2022	1F010ACDAECCAD9C23D008621142B7B0967959BE	Download
Azure Resource Manager	✓ Valid	10/16/2022	50E614D671BD77D745DASFF7C7549D02287023DA	Download
Blob storage	✓ Valid	10/16/2022	ED07A7142ADA1DBEFF112F005F5B2ADDABD78D1	Download
Local web UI	✓ Valid	10/16/2022	13944E17C1D76E72F1E99B57051C0AA29EC9D4BE	Download
IoT device root CA	⚠️ Not present	-	-	-
IoT device CA	⚠️ Not present	-	-	-
IoT device Key	⚠️ Not present	-	-	-
Edge container registry certificate	⚠️ Not present	-	-	-
Edge container registry key	⚠️ Not present	-	-	-

2. Upload the signing chain first and select **Validate & add**.



3. Now you can upload other certificates. For example, you can upload the Azure Resource Manager and Blob storage endpoint certificates.

X

Add certificate

Choose the certificate type to upload.

Certificate type

Endpoints



Bring your own signed certificates for endpoints for Blob storage and Azure Resource Manager for the device.

Azure Resource Manager Password

myasepror1_wdshc ✓



.....

Blob storage Password

myasepror1_wdshc ✓



.....

Validate & add

You can also upload the local web UI certificate. After you upload this certificate, you will be required to start your browser and clear the cache. You will then need to connect to the device local web UI.

Add certificate

Choose the certificate type to upload.

Certificate type

Local web UI

Use the local web UI certificate to access the website browser via SSL. After the certificate is applied, close and then restart the browser to avoid any SSL cache issues.

Local web UI

Password

myasepro1_wdshc ✓



.....

Validate & add

You can also upload the node certificate.

Add certificate

Choose the certificate type to upload.

Certificate type

Node

Use the node certificates to connect to individual device nodes over a secure channel.

4N5WN23

Password

myasepror1_wdshc ✓



.....

Validate & add

Finally you can upload the VPN certificate.

Add certificate

Choose the certificate type to upload.

Certificate type

Node

Use the node certificates to connect to individual device nodes over a secure channel.

4N5WN23	Password
myasepror1_wdshc ✓

Validate & add

At any time, you can select a certificate and view the details to ensure that these match with the certificate that you uploaded.

The certificate page should update to reflect the newly added certificates.

The screenshot shows the Azure Stack Edge Pro R configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Compute, Web proxy, Device, Update server, Time, Certificates), Maintenance (Power, Hardware health, Software update), and Cloud details. The 'Certificates' section is selected and highlighted with a red border. The main content area is titled 'Certificates' and shows a table of existing certificates. The table columns are Name, Status, Expiration date, Thumbprint, and Download. The table rows include:

Name	Status	Expiration date	Thumbprint	Download
Signing Chain	Valid	10/16/2021	E7867A5123B5688496EACE92C962A019427E3D0	-
Node (4N5WN23)	Valid	10/16/2021	6BE8191F6D0EAF2455B8AD67C4CD4CFE0434A36A	-
Azure Resource Manager	Valid	10/16/2021	6BE8191F6D0EAF2455B8AD67C4CD4CFE0434A36A	-
Blob storage	Valid	10/16/2021	6BE8191F6D0EAF2455B8AD67C4CD4CFE0434A36A	-
Local web UI	Valid	10/16/2021	6BE8191F6D0EAF2455B8AD67C4CD4CFE0434A36A	-
IoT device root CA	Not present	-	-	-
IoT device CA	Not present	-	-	-
IoT device Key	Not present	-	-	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

At the bottom of the table are buttons for '< Back to Get started' and 'Next: Cloud details >'.

NOTE

Except for Azure public cloud, signing chain certificates are needed to be brought in before activation for all cloud configurations (Azure Government or Azure Stack).

4. Select < Back to Get started.

Configure VPN

1. On the **Security** tile, select **Configure** for VPN.

Azure Stack Edge Rugged J-5100a

Overview

CONFIGURATION

- Get started
- Network
- Web proxy
- Device
- Update server
- Time
- Certificates
- VPN**
- Cloud details
- Compute

MAINTENANCE

- Power
- Hardware health
- Software update
- Password change
- Device reset

TROUBLESHOOTING

- Diagnostic tests
- Support

VPN
myasetest1

To add a second layer of encryption to data-in-motion, configure the VPN settings for your device.

VPN state: Disabled

VPN gateway IP: Not configured

PFS group: Not configured

DH group: Not configured

IPsec integrity method: Not configured

IPsec cipher transform constants: Not configured

IPsec authentication transform constants: Not configured

IKE encryption method: Not configured

Configure

Upload VPN route configuration file

Upload VPN route configuration file

Upload

IP address ranges to be accessed using VPN only

IP addresses allowed: Not configured

Configure

[Go back to Get started](#)

To configure VPN, you'll first need to ensure that you have all the necessary configuration done in Azure. For details, see [Configure prerequisites](#) and [Configure Azure resources for VPN](#). Once this is complete, you can do the configuration in the local UI.

- On the VPN page, select **Configure**.
- In the **Configure VPN** blade:
 - Enable **VPN settings**.
 - Provide the **VPN shared secret**. This is the shared key you provided while creating the Azure VPN connection object.
 - Provide the **VPN gateway IP address**. This is the Azure local network gateway IP address.
 - For **PFS group**, select **None**.
 - For **DH group**, select **Group2**.
 - For **IPsec integrity method**, select **SHA256**.
 - For **IPsec cipher transform constants**, select **GCMAES256**.
 - For **IPsec authentication transform constants**, select **GCMAES256**.
 - For **IKE encryption method**, select **AES256**.
 - Select **Apply**.

X

Confaure VPN

* VPN settings

Enable

Disable

VPN shared secret

.....

VPN gateway IP

52.180.162.131



PFS group

None



DH group

Group2



IPsec integrity method

SHA256



IPsec cipher transform constants

GCMAES256



IPsec authentication transform constants

GCMAES256



IKE encryption method

AES256



Apply

- c. To upload the VPN route configuration file, select **Upload**.

The screenshot shows the Azure Stack Edge Rugged J-5100a configuration interface. The left sidebar has a 'VPN' section selected. The main content area is titled 'VPN' and shows the device name 'myasetest1'. It provides a summary of current VPN settings and a 'Configure' button. Below this, there's a section for uploading a route configuration file, with a red box highlighting the 'Upload' button. At the bottom, there's a section for IP address ranges and a 'Configure' button.

- Browse to the VPN configuration *json* file that you downloaded on your local system in the previous step.
- Select the region as the Azure region associated with the device, virtual network, and gateways.
- Select **Apply**.

The dialog box is titled 'Upload VPN route configuration file'. It contains two main sections: 'Upload file' with a 'Select a file' input field and a blue 'Upload' button, and 'Region' with a dropdown menu set to 'centraluseuap'. At the bottom is a large red 'Apply' button.

- d. To add client-specific routes, configure IP address ranges to be accessed using VPN only.
- Under **IP address ranges to be accessed using VPN only**, select **Configure**.
 - Provide a valid IPv4 range and select **Add**. Repeat the steps to add other ranges.
 - Select **Apply**.

IP address ranges to be accessed using VPN only

Specify a range of IP addresses to be included for your VPN connection.

IPv4 range

Example: 10.10.10.10/24

Add

Enter a valid IPv4 range.

10.10.10.10/24

Delete

Apply

2. Select < Back to Get started.

Configure encryption-at-rest

1. On the **Security** tile, select **Configure** for encryption-at-rest. This is a required setting and until this is successfully configured, you can't activate the device.

At the factory, once the devices are imaged, the volume level BitLocker encryption is enabled. After you receive the device, you need to configure the encryption-at-rest. The storage pool and volumes are recreated and you can provide BitLocker keys to enable encryption-at-rest and thus create a second layer of encryption for your data-at-rest.

2. In the **Encryption-at-rest** pane, provide a 32 character long Base-64 encoded key. This is a one-time configuration and this key is used to protect the actual encryption key. You can choose to automatically generate this key or enter one.



Encryption at rest

You can bring your own encryption at rest key or generate one here.

* Select an option

System generated encryption key

.....



This key is saved in the key file on the Cloud details page after the device is activated.

The key is saved in a key file on the **Cloud details** page after the device is activated.

3. Select **Apply**. This operation takes several minutes and the status of operation is displayed on the **Security** tile.

Double encryption at rest.

66 % completed.



4. After the status shows as **Completed**, select < Back to Get started.

Your device is now ready to be activated.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device

- Configure VPN
- Configure encryption-at-rest

To learn how to activate your Azure Stack Edge Pro R device, see:

[Activate Azure Stack Edge Pro R device](#)

Tutorial: Activate Azure Stack Edge Pro R device

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how you can activate your Azure Stack Edge Pro R device by using the local web UI.

The activation process can take around 5 minutes to complete.

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Pro R device, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Pro R](#).
 - You've configured the network and compute network settings as detailed in [Configure network, compute network, web proxy](#)
 - You have uploaded your own or generated the device certificates on your device if you changed the device name or the DNS domain via the **Device** page. If you haven't done this step, you will see an error during the device activation and the activation will be blocked. For more information, go to [Configure certificates](#).
- You have the activation key from the Azure Stack Edge service that you created to manage the Azure Stack Edge Pro R device. For more information, go to [Prepare to deploy Azure Stack Edge Pro R](#).

Activate the device

1. In the local web UI of the device, go to **Get started** page.
2. On the **Activation** tile, select **Activate**.

The screenshot shows the Azure Stack Edge Pro R (1 GPU) configuration interface. On the left, a sidebar lists various configuration options: Overview, Get started (highlighted with a red border), Network, Compute, Web proxy, Device, Update server, Time, Certificates, VPN, and Cloud details. Below these are Maintenance options: Power and Hardware health. The main pane is titled "Get started with standalone device setup" and "myasepro1". It contains four sections: 1. Network (Network: Configured, Compute network: Configured, Web proxy: Not configured). 2. Device setup (Device: Configured, Update: Configured with defaults, Time: Configured with defaults). 3. Security (Certificates: Configured, Encryption at rest: Completed, Encryption at rest key rotation: Rotate keys). 4. Activation (Text: Use the activation key from the Azure portal to activate your device, a blue "Activate" button).

3. In the **Activate** pane:

- a. Enter the **Activation key** that you got in [Get the activation key for Azure Stack Edge Pro R](#).
- b. You can enable proactive log collection to let Microsoft collect logs based on the health status of the device. The logs collected this way are uploaded to an Azure Storage account.
- c. Select **Apply**.

Activate

Activate the device with Azure service. [Learn how to get the activation key](#). After the device is activated, the system checks for and applies any critical updates.

* Activation key

1abC2def3gH4jk56lmnO7pq8rs9tu01vwX==#1abcd2e3456f78 ✓

Proactive log collection

Based on proactive log collection indicators, logs are proactively uploaded to an Azure Storage account to help Microsoft Support troubleshoot issues when they arise. [Learn more](#).

[Enable](#) [Disable](#)

If you click the "Disable" button, you agree to deactivate the proactive log collection. After the proactive log collection is disabled, logs are not uploaded automatically if a proactive log collection indicator is detected.

Learn more about [Microsoft's privacy practices](#).

[Activate](#)

4. First the device is activated. You are then prompted to download the key file.

Device activated

Successfully activated your device. Download the device key file to a secure location. These keys may be needed to facilitate a future system recovery.

[Download and continue](#)

Select **Download and continue** and save the *device-serial-no.json* file in a safe location outside of the device. **This key file contains the recovery keys for the OS disk and data disks on your device.** These keys may be needed to facilitate a future system recovery.

Here are the contents of the *json* file:

```
{  
    "Id": "<Device ID>",  
    "DataVolumeBitLockerExternalKeys": {  
        "hcsinternal": "<BitLocker key for data disk>",  
        "hcsdata": "<BitLocker key for data disk>"  
    },  
    "SystemVolumeBitLockerRecoveryKey": "<BitLocker key for system volume>",  
    "ServiceEncryptionKey": "<Azure service encryption key>"  
}
```

The following table explains the various keys:

FIELD	DESCRIPTION
<code>Id</code>	This is the ID for the device.
<code>DataVolumeBitLockerExternalKeys</code>	These are the BitLockers keys for the data disks and are used to recover the local data on your device.
<code>SystemVolumeBitLockerRecoveryKey</code>	This is the BitLocker key for the system volume. This key helps with the recovery of the system configuration and system data for your device.
<code>ServiceEncryptionKey</code>	This key protects the data flowing through the Azure service. This key ensures that a compromise of the Azure service will not result in a compromise of stored information.

5. Go to the **Overview** page. The device state should show as **Activated**.

The screenshot shows the Azure Stack Edge Pro (1 GPU) Overview page. The left sidebar has a dark theme with white icons and text. The main area has a light background. The top navigation bar includes a search icon, a refresh icon, a gear icon, a help icon, a circular icon with a 'C', and a power icon.

Configuration sidebar items include: Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, Certificates, and Cloud details. The **MAINTENANCE** section is collapsed.

The main content area has three sections:

- System**:
 - Health status : ✓ Healthy
 - Software version : [2.1.1342.1972](#)
 - Total capacity : 4.19 TB
 - Available capacity : 4.15 TB
- Device**:
 - Device serial number : 3Q7LHQ2
 - Node serial number : 3Q7LHQ2
 - State** : ✓ Activated
 - Compute acceleration : 1 * GPU
- Configuration**:
 - Network : Configured
 - Web proxy : Not enabled
 - Cloud connectivity : Fully connected

The device activation is complete. You can now add shares on your device.

If you encounter any issues during activation, go to [Troubleshoot activation and Azure Key Vault errors](#).

Next steps

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

To learn how to transfer data with your Azure Stack Edge Pro R device, see:

[Transfer data with Azure Stack Edge Pro R](#)

Tutorial: Configure compute on Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role and create a Kubernetes cluster on your Azure Stack Edge Pro GPU device.

This procedure can take around 20 to 30 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Get Kubernetes endpoints

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro device:

- Make sure that you've activated your Azure Stack Edge Pro device as described in [Activate Azure Stack Edge Pro](#).
- Make sure that you've followed the instructions in [Enable compute network](#) and:
 - Enabled a network interface for compute.
 - Assigned Kubernetes node IPs and Kubernetes external service IPs.

NOTE

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are on the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

Configure compute

To configure compute on your Azure Stack Edge Pro, you'll create an IoT Hub resource via the Azure portal.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**, and select **IoT Edge**.

The screenshot shows the Azure Stack Edge device overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Your device is running fine!' message. Below it, the 'Deployed edge services' section shows 'No deployed services'. The 'Edge services' section contains three cards: 'Virtual machines' (with a 'New' button), 'IoT Edge' (which is selected and has a red box around its card), and 'Cloud storage gateway'. Each card has a 'How to get started?' link.

2. In **Enable IoT Edge service**, select **Add**.

The screenshot shows the IoT Edge | Overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Enable IoT Edge service' section. This section contains instructions to enable the service by setting up the network and configuring the Azure subscription, followed by a large 'Add' button. Below this is a 'Steps to deploy IoT Edge services' section. At the bottom, there's a 'What's next' section with a link to 'Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services'.

3. On the **Configure Edge compute** blade, input the following information:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.

FIELD	VALUE
IoT Hub	<p>Choose from New or Existing. By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.</p>
Name	Accept the default name or enter a name for your IoT Hub resource.

Home > myasetest > IoT Edge >

Create IoT Edge service ⊕

Azure Stack Edge

[Basics](#) [Review + Create](#)

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription * <small>(1)</small>	Edge Gateway Test
Resource group * <small>(1)</small>	myaserg
IoT Hub * <small>(1)</small>	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing myasetest-iothub ✓

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

*IoT Edge device: myasetest-edge
 IoT Gateway device: myasetest-storagegateway*

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

4. When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

The screenshot shows the IoT Edge Overview page. At the top, there's a search bar and several action buttons: 'Add module', 'Add trigger', 'Refresh configuration', 'Remove', and 'Refresh'. Below the header, a red box highlights the 'Overview' tab. A message box says 'IoT Edge service is running fine!' with the subtext 'Start processing the data using IoT Edge modules. Learn more'. On the left, there are navigation links for 'Modules', 'Triggers', and 'Properties'. The main area has two sections: 'Modules' and 'Triggers'. The 'Modules' section contains a sub-section for 'Edge Shares' with a 'Configure Shares' link, and another for 'Edge Storage account' with a 'Configure Storage account' link. The 'Triggers' section has a 'Add trigger' button. At the bottom, there are three links: 'Edge Shares', 'Edge Storage account', and 'Network bandwidth usage'.

5. To confirm the Edge compute role has been configured, go to **IoT Edge > Properties**.

The screenshot shows the IoT Edge Properties page. At the top, there's a search bar and a 'Refresh' button. Below the header, a red box highlights the 'Properties' tab. The main content area displays device and platform information in a table:

IoT Hub	myasetest-iohub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

When the Edge compute role is set up on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

It can take 20-30 minutes to configure compute because, behind the scenes, virtual machines and a Kubernetes cluster are being created.

After you have successfully configured compute in the Azure portal, a Kubernetes cluster and a default user associated with the IoT namespace (a system namespace controlled by Azure Stack Edge) exist.

Get Kubernetes endpoints

To configure a client to access Kubernetes cluster, you'll need the Kubernetes endpoint. Follow these steps to get Kubernetes API endpoint from the local UI of your Azure Stack Edge Pro device.

1. In the local web UI of your device, go to **Device** page.
2. Under the **Device endpoints**, copy the **Kubernetes API endpoint**. This endpoint is a string in the

following format: [https://compute.<device-name>.<DNS-domain>\[Kubernetes-cluster-IP-address\]](https://compute.<device-name>.<DNS-domain>[Kubernetes-cluster-IP-address]).

The screenshot shows the 'Device' configuration page for a device named 'dl115'. The 'Device endpoints' section is highlighted with a red box. It lists various services with their certificate requirements and endpoints. The 'Kubernetes API service' endpoint is highlighted with a blue box: [https://compute.dl115.teatraining1.com \[10.128.45.200\]](https://compute.dl115.teatraining1.com [10.128.45.200]).

Service	Certificate Required	Endpoint
SMB server	No	\\\dl115.teatraining1.com\Share name]
NFS server	No	\\\[Device IP address]\Share name]
Azure Resource Manager login	Yes	https://login.dl115.teatraining1.com
Azure Resource Manager	Yes	https://management.dl115.teatraining1.com
Blob Storage	Yes	https://[Account name].blob.dl115.teatraining1.com
Kubernetes API service	No	https://compute.dl115.teatraining1.com [10.128.45.200]
Edge IoT hub	Yes	Endpoint not yet created.

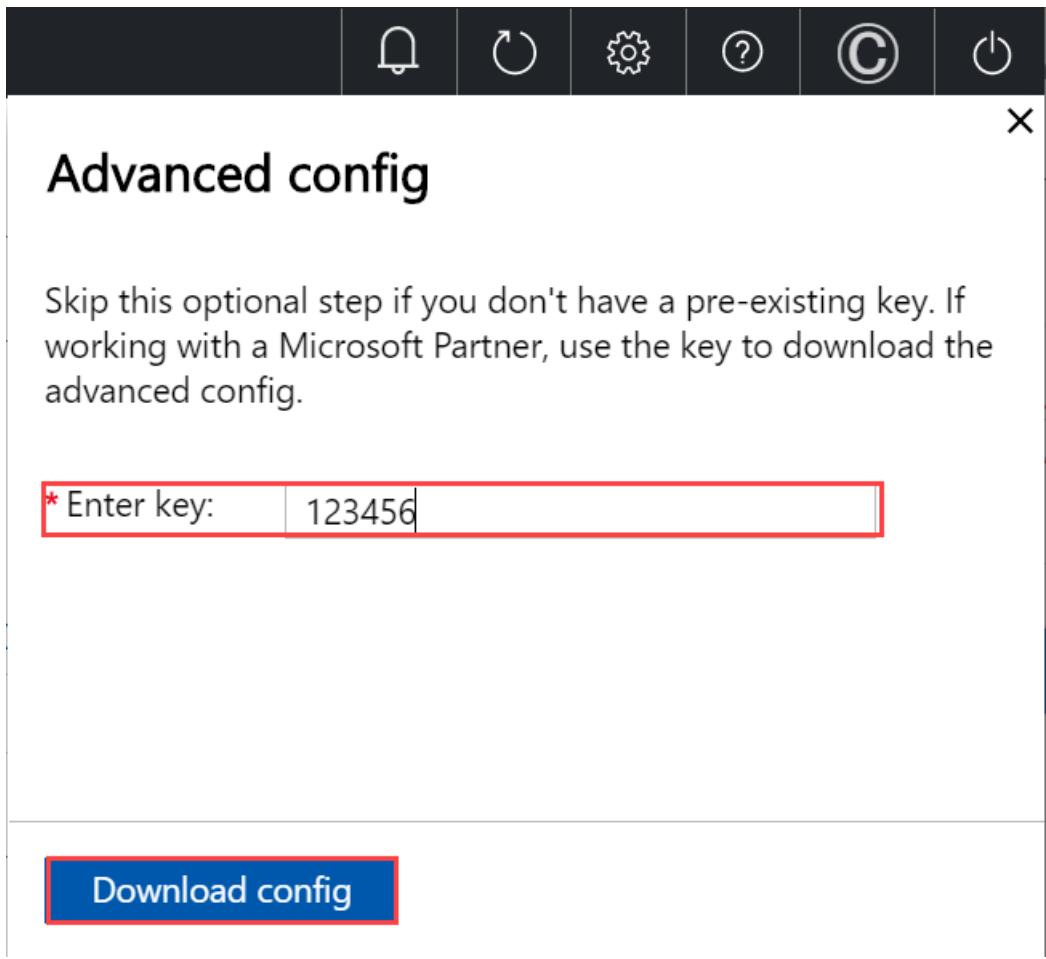
3. Save the endpoint string. You'll use this endpoint string later when configuring a client to access the Kubernetes cluster via kubectl.

4. While you are in the local web UI, you can:

- If you've been provided a key from Microsoft (select users may have a key), go to Kubernetes API, select **Advanced config**, and download an advanced configuration file for Kubernetes.

The screenshot shows the 'Device' configuration page for a device named 'myasegpu1'. The 'Device endpoints' section is highlighted with a red box. The 'Kubernetes API' endpoint is highlighted with a red box and has a 'Advanced config' button next to it. The endpoint URL is [https://compute.myasegpu1.wdshcsso.com \[10.128.44.241\]](https://compute.myasegpu1.wdshcsso.com [10.128.44.241]).

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\Share name]
NFS server	No	\\\[Device IP address]\Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241] Advanced config
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]



- You can also go to **Kubernetes dashboard** endpoint and download an `aseuser` config file.

The screenshot shows the 'Azure Stack Edge' device configuration page. The left sidebar lists various configuration tabs: Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, and Device (which is selected). The main area shows a 'Device' card for 'myasegpu1'. Under 'Device name', the 'Name' is set to 'myasegpu1' and the 'DNS domain' is 'wdshcsso.com'. The 'Device endpoints' section contains a table:

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241]
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]

At the bottom, there are buttons for 'Apply', '< Back to Overview', and 'Next: Update server >'.

You can use this config file to sign into the Kubernetes dashboard or debug any issues in your Kubernetes cluster. For more information, see [Access Kubernetes dashboard](#).

Next steps

In this tutorial, you learned how to:

- Configure compute
- Get Kubernetes endpoints

To learn how to administer your Azure Stack Edge Pro device, see:

[Use local web UI to administer an Azure Stack Edge Pro](#)

Configure VPN on your Azure Stack Edge Mini R device via Azure PowerShell

9/21/2022 • 10 minutes to read • [Edit Online](#)

The VPN option provides a second layer of encryption for the data-in-motion over *TLS* from your Azure Stack Edge Mini R or Azure Stack Edge Pro R device to Azure. You can configure VPN on your Azure Stack Edge Mini R device via the Azure portal or via the Azure PowerShell.

This article describes the steps required to configure a Point-to-Site (P2S) VPN on your Azure Stack Edge Mini R device using an Azure PowerShell script to create the configuration in the cloud. The configuration on the Azure Stack Edge device is done via the local UI.

About VPN setup

A P2S VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer or your Azure Stack Edge Mini R device. You start the P2S connection from the client computer or the device. The P2S connection in this case uses IKEv2 VPN, a standards-based IPsec VPN solution.

The typical work flow includes the following steps:

1. Configure prerequisites.
2. Set up necessary resources on Azure.
 - a. Create and configure a virtual network and required subnets.
 - b. Create and configure an Azure VPN gateway (virtual network gateway).
 - c. Set up Azure Firewall and add network and app rules.
 - d. Create Azure Routing Tables and add routes.
 - e. Enable Point-to-site in VPN gateway.
 - a. Add the client address pool.
 - b. Configure tunnel type.
 - c. Configure authentication type.
 - d. Create certificate.
 - e. Upload certificate.
 - f. Download phone book.
3. Set up VPN in the local web UI of the device.
 - a. Provide phone book.
 - b. Provide Service tags (json) file.

The detailed steps are provided in the following sections.

Configure prerequisites

- You should have access to an Azure Stack Edge Mini R device that is installed as per the instructions in [Install your Azure Stack Edge Mini R device](#). This device will be establishing a P2S connection with Azure.
- You should have access to a valid Azure Subscription that is enabled for Azure Stack Edge service in Azure. Use this subscription to create a corresponding resource in Azure to manage your Azure Stack Edge Mini R device.
- You have access to a Windows client that you'll use to access your Azure Stack Edge Mini R device. You'll

use this client to programmatically create the configuration in the cloud.

1. To install the required version of PowerShell on your Windows client, run the following commands:

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser  
Import-Module Az.Accounts
```

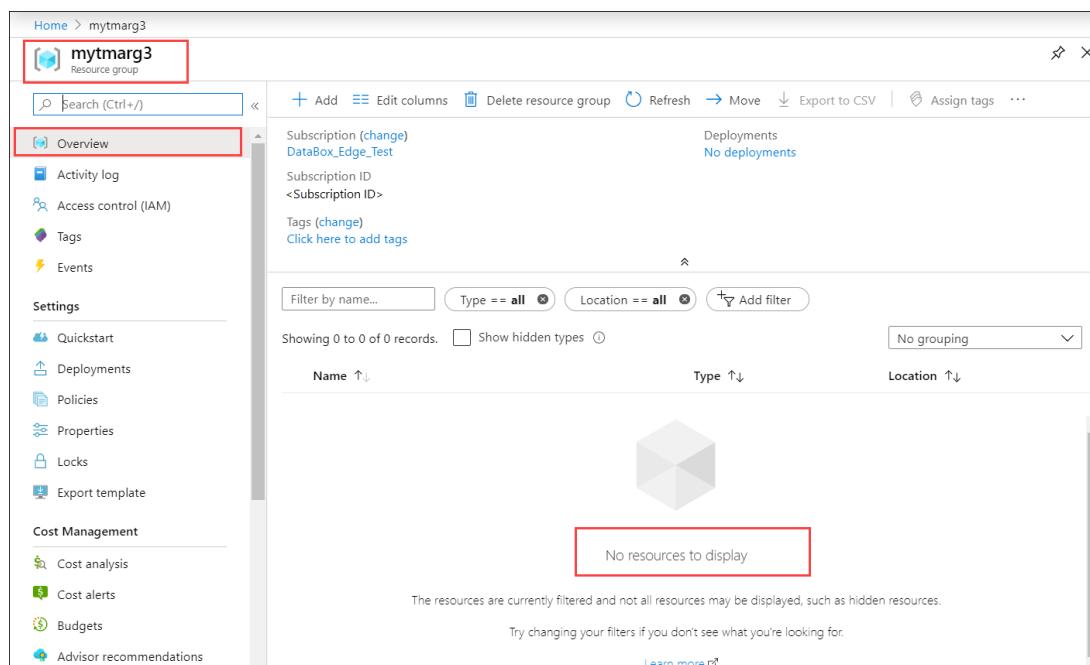
2. To connect to your Azure account and subscription, run the following commands:

```
Connect-AzAccount  
Set-AzContext -Subscription "<Your subscription name>"
```

Provide the Azure subscription name you are using with your Azure Stack Edge Mini R device to configure VPN.

3. [Download the script](#) required to create configuration in the cloud. The script will:

- o Create an Azure Virtual network and the following subnets: *GatewaySubnet*, and *AzureFirewallSubnet*.
 - o Create and configure an Azure VPN gateway.
 - o Create and configure an Azure local network gateway.
 - o Create and configure an Azure VPN connection between the Azure VPN gateway and the local network gateway.
 - o Create an Azure Firewall and add network rules, app rules.
 - o Create an Azure Routing table and add routes to it.
4. Create the resource group in the Azure portal under which you want the Azure resources to be created. Go to the list of services in Azure portal, select **Resource group** and then select + Add. Provide the subscription information and the name for your resource group and then select **Create**. If you go to this resource group, it should not have any resources under it at this time.



5. You will need to have a Base 64 encoded certificate in `.cer` format for your Azure Stack Edge Mini R device. This certificate should be uploaded to your Azure Stack Edge device as `pfx` with a private key. This certificate also needs to be installed in the trusted root of the store on the client that is trying to establish the P2S connection.

Use the script

First you modify the `parameters-p2s.json` file to input your parameters. Next, you run the script using the modified json file.

Each of these steps is discussed in the following sections.

Download service tags file

You may already have a `ServiceTags.json` file in the folder where you downloaded the script. If not, you can download the service tags file.

Download the service tags from the Azure to your local client and save as a `json` file in the same folder that contains the scripts: <https://www.microsoft.com/download/details.aspx?id=56519>.

This file is uploaded in the local web UI at a later step.

Modify parameters file

The first step would be to modify the `parameters-p2s.json` file and save the changes.

For the Azure resources that you create, you'll provide the following names:

PARAMETER NAME	DESCRIPTION
virtualNetworks_vnet_name	Azure Virtual Network name
azureFirewalls_firewall_name	Azure Firewall name
routeTables_routetable_name	Azure Route table name
publicIPAddresses_VNGW_public_ip_name	Public IP address name for your Virtual network gateway
virtualNetworkGateways_VNGW_name	Azure VPN gateway (virtual network gateway) name
publicIPAddresses_firewall_public_ip_name	Public IP address name for your Azure Firewall
location	This is the region in which you want to create your virtual network. Select the same region as the one associated with your device.
RouteTables_routetable_onprem_name	This is the name of the additional route table to help the firewall route packets back to Azure Stack Edge device. The script creates two additional routes and associates <code>default</code> and <code>GatewaySubnet</code> with this route table.

Provide the following IP addresses and address spaces for the Azure resources that are created including the virtual network and associated subnets (`default`, `firewall`, `GatewaySubnet`).

PARAMETER NAME	DESCRIPTION
VnetIPv4AddressSpace	This is the address space associated with your virtual network. Provide Vnet IP range as private IP range (https://en.wikipedia.org/wiki/Private_network#Private_IPv4_addresses).
DefaultSubnetIPv4AddressSpace	This is the address space associated with the <code>Default</code> subnet for your virtual network.

PARAMETER NAME	DESCRIPTION
FirewallSubnetIPv4AddressSpace	This is the address space associated with the <code>Firewall</code> subnet for your virtual network.
GatewaySubnetIPv4AddressSpace	This is the address space associated with the <code>GatewaySubnet</code> for your virtual network.
GatewaySubnetIPv4bgpPeeringAddress	This is the IP address that is reserved for BGP communication and is based off the address space associated with the <code>GatewaySubnet</code> for your virtual network.
ClientAddressPool	This IP address is used for the address pool in the P2S configuration in Azure portal.
PublicCertData	Public certificate data is used by the VPN Gateway to authenticate P2S clients connecting to it. To get the certificate data, install the root certificate. Make sure the certificate is Base-64 encoded with a .cer extension. Open this certificate and copy the text in the certificate between ==BEGIN CERTIFICATE== and ==END CERTIFICATE== in one continuous line.

Run the script

Follow these steps to use the modified `parameters-p2s.json` and run the script to create Azure resources.

1. Run PowerShell. Switch to the directory where the script is located.
2. Run the script.

```
.\AzDeployVpn.ps1 -Location <Location> -AzureAppRuleFilePath "appRule.json" -AzureIPRangesFilePath "<Service tag json file>" -ResourceGroupName "<Resource group name>" -AzureDeploymentName "<Deployment name>" -NetworkRuleCollectionName "<Name for collection of network rules>" -Priority 115 -AppRuleCollectionName "<Name for collection of app rules>"
```

NOTE

In this release, the script works in East US location only.

You will need to input the following information when you run the script:

PARAMETER	DESCRIPTION
Location	This is the region in which the Azure resources must be created.
AzureAppRuleFilePath	This is the file path for <code>appRule.json</code> .
AzureIPRangesFilePath	This is the Service Tag json file that you downloaded in the earlier step.
ResourceGroupName	This is the name of the resource group under which all the Azure resources are created.
AzureDeploymentName	This is the name for your Azure deployment.

PARAMETER	DESCRIPTION
NetworkRuleCollectionName	This is the name for the collection of all the network rules that are created and add to your Azure Firewall.
Priority	This is the priority assigned to all the network and application rules that are created.
AppRuleCollectionName	This is the name for the collection of all the application rules that are created and added to your Azure Firewall.

A sample output is shown below.

```
PS C:\Offline docs\AzureVpnConfigurationScripts> .\AzDeployVpn.ps1 -Location eastus -AzureAppRuleFilePath "appRule.json" -AzureIPRangesFilePath ".\ServiceTags_Public_20200203.json" -ResourceGroupName "mytmargin3" -AzureDeploymentName "tmap2stestdeploy1" -NetworkRuleCollectionName "testnrc1" -Priority 115 -AppRuleCollectionName "testarc2"
    validating vpn deployment parameters
    Starting vpn deployment
    C:\Offline docs\AzureVpnConfigurationScripts\parameters-p2s.json
    C:\Offline docs\AzureVpnConfigurationScripts\template-p2s.json
    vpn deployment: tmap2stestdeploy1 started and status: Running
    Waiting for vpn deployment completion....
==== CUT ===== CUT =====
Adding route 191.236.0.0/18 for AzureCloud.eastus
Adding route 191.237.0.0/17 for AzureCloud.eastus
Adding route 191.238.0.0/18 for AzureCloud.eastus
Total Routes:294, Existing Routes: 74, New Routes Added: 220
Additional routes getting added
```

IMPORTANT

- The script takes approximately 90 minutes to run. Make sure to sign into your network right before the script starts.
- If for any reason there is a failed session with the script, make sure to delete the resource group to delete all the resources created under it.

After the script is complete, a deployment log is generated in the same folder where the script resides.

Verify the Azure resources

After you've successfully run the script, verify that all the resources were created in Azure. Go to the resource group that you created. You should see the following resources:

Subscription (change)
DataBox_Edge_Test

Subscription ID
<Subscription ID>

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 7 of 7 records. Show hidden types No grouping

Name	Type	Location
firewall5	Firewall	East US
firewallpublicip5	Public IP address	East US
routetable5	Route table	East US
routetableonprem5	Route table	East US
vnet5	Virtual network	East US
vngw5	Virtual network gateway	East US
vngwpublicip5	Public IP address	East US

< Previous Page 1 of 1 Next >

Download phone book for VPN profile

In this step, you will download the VPN profile for your device.

1. In the Azure portal, go to the resource group and then select the virtual network gateway that you created in the earlier step.

Subscription (change)
DataBox_Edge_Test

Subscription ID
<Subscription ID>

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 7 of 7 records. Show hidden types No grouping

Name	Type	Location
firewall5	Firewall	East US
firewallpublicip5	Public IP address	East US
routetable5	Route table	East US
routetableonprem5	Route table	East US
vnet5	Virtual network	East US
<input checked="" type="checkbox"/> vngw5	Virtual network gateway	East US
vngwpublicip5	Public IP address	East US

< Previous Page 1 of 1 Next >

2. Go to **Settings > Point-to-site configuration**. Select **Download VPN client**.

3. Save the zipped profile and extract on your Windows client.

4. Go to *WindowsAmd64* folder and then extract the `.exe` : *VpnClientSetupAmd64.exe*.

5. Create a temporary path. For example:

```
C:\NewTemp\vnet\tmp
```

6. Run PowerShell and go to the directory where the `.exe` is located. To execute the `.exe`, type:

```
.\VpnClientSetupAmd64.exe /Q /C /T:"C:\NewTemp\vnet\tmp"
```

7. The temporary path will have new files. Here is a sample output:

```

PS C:\windows\system32> cd "C:\Users\Ase\Downloads\vngw5\WindowsAmd64"
PS C:\Users\Ase\Downloads\vngw5\WindowsAmd64> .\VpnClientSetupAmd64.exe /Q /C
/T:"C:\NewTemp\vnet\tmp"
PS C:\Users\Ase\Downloads\vngw5\WindowsAmd64> cd "C:\NewTemp\vnet"
PS C:\NewTemp\vnet> ls .\tmp

Directory: C:\NewTemp\vnet\tmp

Mode                LastWriteTime       Length Name
----                -----          -----
-a----   2/6/2020  6:18 PM           947 8c670077-470b-421a-8dd8-8cedb4f2f08a.cer
-a----   2/6/2020  6:18 PM           155 8c670077-470b-421a-8dd8-8cedb4f2f08a.cmp
-a----   2/6/2020  6:18 PM          3564 8c670077-470b-421a-8dd8-8cedb4f2f08a.cms
-a----   2/6/2020  6:18 PM          11535 8c670077-470b-421a-8dd8-8cedb4f2f08a.inf
-a----   2/6/2020  6:18 PM          2285 8c670077-470b-421a-8dd8-8cedb4f2f08a.pbk
-a----   2/6/2020  6:18 PM          5430 azurebox16.ico
-a----   2/6/2020  6:18 PM          4286 azurebox32.ico
-a----   2/6/2020  6:18 PM          138934 azurevpnbanner.bmp
-a----   2/6/2020  6:18 PM          46064 cmroute.dll
-a----   2/6/2020  6:18 PM          196 routes.txt

PS C:\NewTemp\vnet>

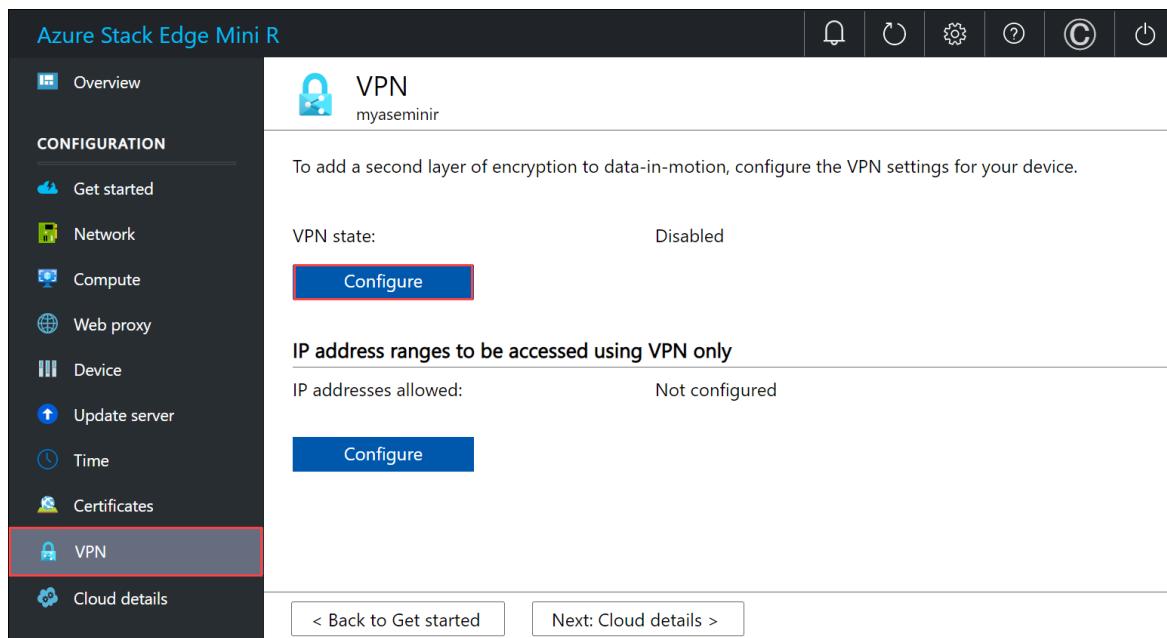
```

- The .pbk file is the phone book for the VPN profile. You will use this in the local UI.

VPN configuration on the device

Follow these steps on the local UI of your Azure Stack Edge device.

- In the local UI, go to **VPN** page. Under VPN state, select **Configure**.



- In the **Configure VPN** blade:

- In the Upload phone book file, point to the .pbk file that you created in the earlier step.
- In the Upload public IP list config file, provide Azure Data Center IP range JSON file as input. You downloaded this file in an earlier step from: <https://www.microsoft.com/download/details.aspx?id=56519>.
- Select **eastus** as the region and select **Apply**.

Configure VPN

* VPN settings

* Upload phone book file

8c670077-470b-421a-8dd8-8cedb4f2f08 ✓

* Upload public IP List config file

ServiceTags_Public_20200203.json ✓

Region

eastus ▾

If the phone book file (.pbk) and the public IP list config file (.json) are already uploaded, uploading those again will override the previous copies.

3. In the IP address ranges to be accessed using VPN only section, enter the Vnet IPv4 range that you had chosen for your Azure Virtual Network.

IP address ranges to be accessed using VPN only

Specify a range of IP addresses to be included for your VPN connection.

IPv4 range

Example: 10.10.10.10/24

Add

172.28.0.0/16

Delete

Apply

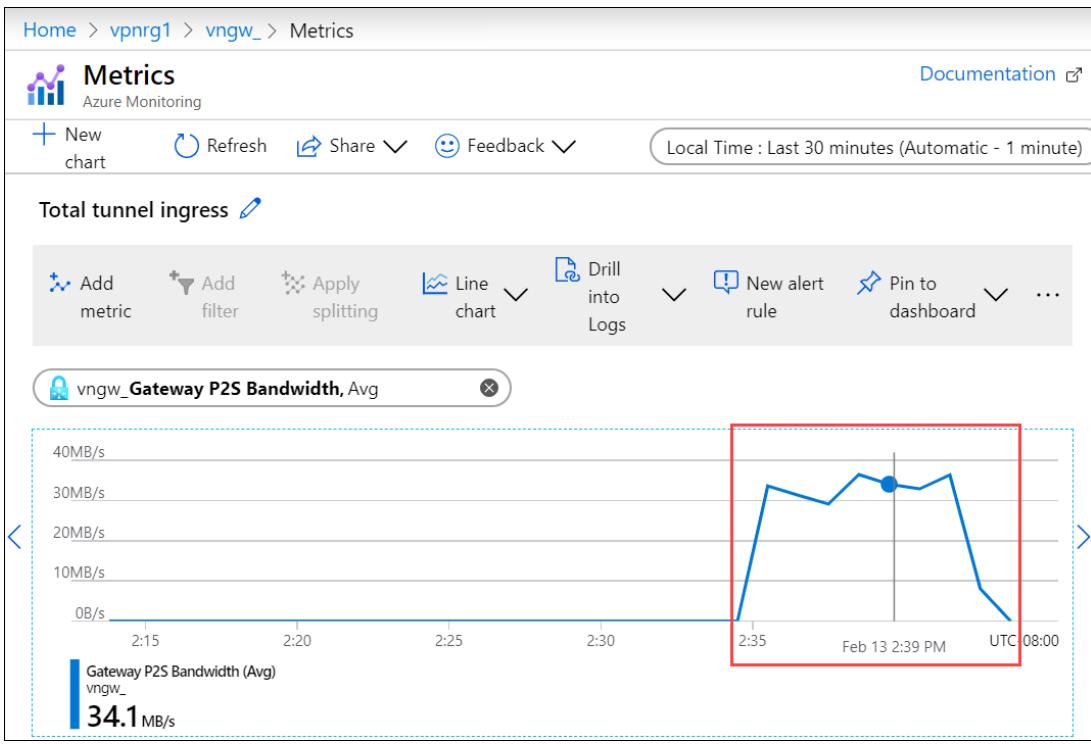
Verify client connection

1. In the Azure portal, go to the VPN gateway.
2. Go to **Settings > Point-to-site configuration**. Under **Allocated IP addresses**, the IP address of your Azure Stack Edge device should show up.

Validate data transfer through VPN

To confirm that VPN is working, copy data to an SMB share. Follow the steps in [Add a share](#) on your Azure Stack Edge device.

1. Copy a file, for example \data\pictures\waterfall.jpg to the SMB share that you mounted on your client system.
2. To validate that the data is going through VPN, while the data is being copied:
 - a. Go to the VPN gateway in the Azure portal.
 - b. Go to **Monitoring > Metrics**.
 - c. In the right-pane, choose the **Scope** as your VPN gateway, **Metric** as Gateway P2S bandwidth, and **Aggregation** as Avg.
 - d. As the data is being copied, you will see an increase in the bandwidth utilization and when the data copy is complete, the bandwidth utilization will drop.



3. Verify that this file shows up in your storage account on the cloud.

Debug issues

To debug any issues, use the following commands:

```
Get-AzResourceGroupDeployment -DeploymentName $deploymentName -ResourceGroupName $ResourceGroupName
```

The sample output is shown below:

```
PS C:\Projects\TZA\VPN\Azure-VpnDeployment> Get-AzResourceGroupDeployment -DeploymentName "tznvpngr14_deployment" -ResourceGroupName "tznvpngr14"
```

```

DeploymentName      : tznvpngr14_deployment
ResourceGroupName   : tznvpngr14
ProvisioningState   : Succeeded
Timestamp          : 1/21/2020 6:23:13 PM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name           Type       Value
    ======  ======  ======
    virtualNetworks_vnet_name     String
tznvpngr14_vnet      :
    azureFirewalls_firewall_name String
tznvpngr14_firewall  :
    routeTables_routetable_name String
tznvpngr14_routetable  :
    publicIPAddresses_VNGW_public_ip_name String
tznvpngr14_vngwpublicip  :
    virtualNetworkGateways_VNGW_name String
tznvpngr14_vngw      :
    publicIPAddresses_firewall_public_ip_name String
tznvpngr14_fwpip     :
    localNetworkGateways_LNGW_name String
tznvpngr14_lngw      :
    connections_vngw_lngw_name String
tznvpngr14_connection  :
    location          String
    vnetIPv4AddressSpace String
    East US
172.24.0.0/16        :
    defaultSubnetIPv4AddressSpace String
172.24.0.0/24        :
    firewallSubnetIPv4AddressSpace String
172.24.1.0/24        :
    gatewaySubnetIPv4AddressSpace String
172.24.2.0/24        :
    gatewaySubnetIPv4bgpPeeringAddress String
172.24.2.254         :
    customerNetworkAddressSpace String
10.0.0.0/18          :
    customerPublicNetworkAddressSpace String
207.68.128.0/24      :
    dbeIOTNetworkAddressSpace String
10.139.218.0/24      :
    azureVPNsharedKey      String
    dbE-Gateway-ipaddress  String
    1234567890
207.68.128.113       :

Outputs             :
    Name           Type       Value
    ======  ======  ======
    virtualNetwork     Object
    {
        "provisioningState": "Succeeded",
        "resourceGuid": "dcf673d3-5c73-4764-b077-77125eda1303",
        "addressSpace": {
            "addressPrefixes": [
                "172.24.0.0/16"
            ]
        }
    }
===== CUT ===== CUT =====
```

```
Get-AzResourceGroupDeploymentOperation -ResourceGroupName $ResourceGroupName -DeploymentName
$AzureDeploymentName
```

Next steps

Configure VPN via the local UI on your Azure Stack Edge device.

Configure business continuity and disaster recovery for Azure Stack Edge VPN

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to configure business continuity and disaster recovery (BCDR) on a virtual private network (VPN) configured on an Azure Stack Edge device.

This article applies to both Azure Stack Edge Pro R and Azure Stack Edge Mini R device.

Configure failover to a paired region

Your Azure Stack Edge device uses other Azure services, for example Azure Storage. You can configure BCDR on any specific Azure service that is used by the Azure Stack Edge device. If an Azure service used by Azure Stack Edge fails over to its paired region, the Azure Stack Edge device will now connect to the new IP addresses and the communication will not be doubly encrypted.

The Azure Stack Edge device uses split tunneling and all the data and services that are configured in the home region (the region associated with your Azure Stack Edge device) go over the VPN tunnel. If the Azure services fail over to a paired region which is outside of the home region, then the data will no longer go over VPN and hence is not doubly encrypted.

In this scenario, typically only a handful of Azure services are impacted. To address this issue, the following changes should be made in the Azure Stack Edge VPN configuration:

1. Add the failover Azure service IP range(s) in the inclusive routes for VPN on Azure Stack Edge. The services will then start getting routed through the VPN.

To add the inclusive routes, you need to download the json file that has the service specific routes. Make sure to update this file with the new routes.

2. Add the corresponding Azure service IP range(s) in Azure Route table.
3. Add the routes to the firewall.

NOTE

1. The failover of an Azure VPN gateway and Azure Virtual Network (VNET) is addressed in section [Recover from an Azure region that failed due to disaster](#).
2. IP ranges added in the Azure route table could cross the limit of 400. If this occurs, you will need to follow the guidance in section, [Move from one Azure region to another Azure region](#).

Recover from a failed Azure region

In the event that the entire Azure region fails over due to a catastrophic event such as earthquake, all the Azure services in that region including the Azure Stack Edge service will fail over. Since there are multiple services, the inclusive routes could easily range into a few hundreds. Azure has a limitation of 400 routes.

When the region fails over, the virtual network (Vnet) also fails over to the new region and so does the Virtual network gateway (VPN gateway). To address this change, make the following changes in your Azure Stack Edge

VPN configuration:

1. Move your Vnet to the target region. For more information, see: [Move an Azure virtual network to another region via the Azure portal](#).
2. Deploy a new Azure VPN gateway in the target region where you moved the Vnet. For more information, see [Create a virtual network gateway](#).
3. Update Azure Stack Edge VPN configuration to use the above VPN gateway in the VPN connection and then select the target region to add routes that use the VPN gateway.
4. Update the incoming Azure route table if the client address pool also changes.

Move from an Azure region to another

You can move your Azure Stack Edge device from one location to another location. To use a region closest to where your device is deployed, you will need to configure the device for a new home region. Make the following changes:

1. You can update Azure Stack Edge VPN configuration to use a new region's VPN gateway and select the new region to add routes that use VPN gateway.

Next steps

[Back up your Azure Stack Edge device](#).

What is the Azure Stack Edge Mini R?

9/21/2022 • 5 minutes to read • [Edit Online](#)

Azure Stack Edge Mini R is an ultra portable, rugged, edge computing device designed for use in harsh environments. Azure Stack Edge Mini R is delivered as a hardware-as-a-service solution. Microsoft ships you a cloud-managed device that acts as network storage gateway and has a built-in Vision Processing Unit (VPU) that enables accelerated AI-inferencing.

This article provides you an overview of the Azure Stack Edge Mini R solution, key capabilities, and the scenarios where you can deploy this device.

Key capabilities

Azure Stack Edge Mini R has the following capabilities:

CAPABILITY	DESCRIPTION
Rugged hardware	Rugged hardware designed for harsh environments.
Ultra portable	Ultra portable, battery-operated form factor.
Cloud-managed	Device and service are managed via the Azure portal.
Edge compute workloads	Allows analysis, processing, filtering of data. Supports VMs and containerized workloads. <ul style="list-style-type: none">• For information on VM workloads, see VM overview on Azure Stack Edge.• For containerized workloads, see Kubernetes overview on Azure Stack Edge
Accelerated AI inferencing	Enabled by the Intel Movidius Myriad X VPU.
Wired and wireless	Allows wired and wireless data transfers.
Data access	Direct data access from Azure Storage Blobs and Azure Files using cloud APIs for additional data processing in the cloud. Local cache on the device is used for fast access of most recently used files.
Disconnected mode	Deploy, run, manage applications in offline mode. Disconnected mode supports offline upload scenarios.
Supported file transfer protocols	Supports standard SMB, NFS, and REST protocols for data ingestion. For more information on supported versions, go to Azure Stack Edge Mini R system requirements .
Data refresh	Ability to refresh local files with the latest from cloud. For more information, see Refresh a share on your Azure Stack Edge .

CAPABILITY	DESCRIPTION
Double encryption	Use of self-encrypting drive provides the first layer of encryption. VPN provides the second layer of encryption. BitLocker support to locally encrypt data and secure data transfer to cloud over <i>https</i> . For more information, see Configure VPN on your Azure Stack Edge Pro R device .
Bandwidth throttling	Throttle to limit bandwidth usage during peak hours. For more information, see Manage bandwidth schedules on your Azure Stack Edge .
Easy ordering	Bulk ordering and tracking of the device via Azure Edge Hardware Center. For more information, see Order a device via Azure Edge Hardware Center .

Use cases

Here are the various scenarios where Azure Stack Edge Mini R can be used for rapid Machine Learning (ML) inferencing at the edge and preprocessing data before sending it to Azure.

- **Inference with Azure Machine Learning** - With Azure Stack Edge Mini R, you can run ML models to get quick results that can be acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models. For more information on how to use the Azure ML hardware accelerated models on the Azure Stack Edge Mini R device, see [Deploy Azure ML hardware accelerated models on Azure Stack Edge Mini R](#).
- **Preprocess data** - Transform data via compute options such as containers or virtual machines before sending it to Azure to create a more actionable dataset. Preprocessing can be used to:
 - Aggregate data.
 - Modify data, for example to remove personal data.
 - Subset data to optimize storage and bandwidth, or for further analysis.
 - Analyze and react to IoT Events.
- **Transfer data over network to Azure** - Use Azure Stack Edge Mini R to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

Components

The Azure Stack Edge Mini R solution comprises of an Azure Stack Edge resource, Azure Stack Edge Mini R rugged, ultra portable physical device, and a local web UI.

- **Azure Stack Edge Mini R physical device** - An ultra portable, rugged, compute and storage device supplied by Microsoft. The device has an onboard battery and weighs less than 7 lbs.



To procure a device, go to the Azure Edge Hardware Center and place an order. Azure Edge Hardware Center service lets you choose from a variety of Azure Stack Edge SKUs as per your business need. You can order multiple units of a device type, ship multiple devices to different locations, save addresses for future orders, and also track the status of your orders.

Once the order is delivered, you can configure your device and create an Azure Stack Edge resource to manage the device.

For more information, go to [Create an order for your Azure Stack Edge Mini R device](#).

- **Azure Stack Edge resource** – A resource in the Azure portal that lets you manage a rugged, Azure Stack Edge Mini R device from a web interface that you can access from different geographical locations. Use the Azure Stack Edge resource to create and manage resources, view, and manage devices and alerts, and manage shares.
- **Azure Stack Edge Mini R local web UI** - A browser-based local user interface on your Azure Stack Edge Mini R device primarily intended for the initial configuration of the device. Use the local web UI also to run diagnostics, shut down and restart the Azure Stack Edge Pro device, view copy logs, and contact Microsoft Support to file a service request.

The local web UI on the device currently supports the following languages with their corresponding language codes:

LANGUAGE	CODE	LANGUAGE	CODE	LANGUAGE	CODE
English {default}	en	Czech	cs	German	de
Spanish	es	French	fr	Hungarian	hu
Italian	it	Japanese	ja	Korean	ko
Dutch	nl	Polish	pl	Portuguese - Brazil	pt-br
Portuguese - Portugal	pt-pt	Russian	ru	Swedish	sv

LANGUAGE	CODE	LANGUAGE	CODE	LANGUAGE	CODE
Turkish	tr	Chinese - simplified	zh-hans	Chinese - traditional	zh-hant

Region availability

Azure Stack Edge Mini R physical device, Azure resource, and target storage account to which you transfer data do not all have to be in the same region.

- **Resource availability** - For a list of all the regions where the Azure Stack Edge resource is available, go to [Azure products available by region](#).
- **Device availability** - For a list of all the countries where the Azure Stack Edge Mini R device is available, go to Availability section in the Azure Stack Edge Mini R tab for [Azure Stack Edge Mini R pricing](#).
- **Destination Storage accounts** - The storage accounts that store the data are available in all Azure regions. The regions where the storage accounts store Azure Stack Edge Mini R data should be located close to where the device is located for optimum performance. A storage account located far from the device results in long latencies and slower performance.

Azure Stack Edge service is a non-regional service. For more information, see [Regions and Availability Zones in Azure](#). Azure Stack Edge service does not have dependency on a specific Azure region, making it resilient to zone-wide outages and region-wide outages.

For a discussion of considerations for choosing a region for the Azure Stack Edge service, device, and data storage, see [Choosing a region for Azure Stack Edge](#).

Next steps

- Review the [Azure Stack Edge Mini R system requirements](#).

Azure Stack Edge Mini R safety instructions

9/21/2022 • 11 minutes to read • [Edit Online](#)



READ SAFETY AND HEALTH INFORMATION

Read all the safety information in this article before you use your Azure Stack Edge Mini R device, a composition of one battery pack, one AC/DC plugged power supply, one module power adapter, and one server module. Failure to follow instructions could result in fire, electric shock, injuries, or damage to your properties. Read all safety information below before using Azure Stack Edge Mini R.

Safety icon conventions

The following signal words for hazard alerting signs are:

ICON	DESCRIPTION
	DANGER: Indicates a hazardous situation that, if not avoided, will result in death or serious injury. WARNING: Indicates a hazardous situation that, if not avoided, could result in death or serious injury. CAUTION: Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

The following hazard icons are to be observed when setting up and running your Azure Stack Edge Mini R device:

ICON	DESCRIPTION
	Read All Instructions First
	NOTICE: Indicates information considered important, but not hazard-related.
	Hazard Symbol
	Electric Shock Hazard
	Indoor Use Only
	No User Serviceable Parts. Do not access unless properly trained.

ICON	DESCRIPTION

Handling precautions and site selection

The Azure Stack Edge Mini R device has the following handling precautions and site selection criteria:



CAUTION:

- Inspect the *as-received* device for damages. If the device enclosure is damaged, [contact Microsoft Support](#) to obtain a replacement. Do not attempt to operate the device.
- If you suspect the device is malfunctioning, [contact Microsoft Support](#) to obtain a replacement. Do not attempt to service the device.
- The device contains no user-serviceable parts. Hazardous voltage, current, and energy levels are present inside. Do not open. Return the device to Microsoft for servicing.



CAUTION:

It is recommended to operate the system:

- Away from sources of heat including direct sunlight and radiators.
- In locations not exposed to moisture or rain.
- Located in a space that minimizes vibration and physical shock. The system is designed for shock and vibration according to MIL-STD-810G.
- Isolated from strong electromagnetic fields produced by electrical devices.
- Do not allow any liquid or any foreign object to enter the System. Do not place beverages or any other liquid containers on or near the system.



CAUTION:

- This equipment contains a lithium battery. Do not attempt to service the battery pack. Batteries in this equipment are not user serviceable. Risk of Explosion if battery is replaced by an incorrect type.



CAUTION:

Only charge the battery pack when it is a part of the Azure Stack Edge Mini R device, do not charge as a separate device.



CAUTION:

- The ON/OFF switch on the battery pack is for discharging the battery to the server module only. If the power adapter is plugged into the battery pack, power is passed to the server module even if the switch is in the OFF position.



CAUTION:

- Do not burn or short circuit the battery pack. It must be recycled or disposed of properly.



CAUTION:

- In lieu of using the provided AC/DC power supply, this system also has the option to use a field provided Type 2590 Battery. In this case, the end user shall verify that it meets all applicable safety, transportation, environmental, and any other national/local regulations.
- When operating the system with Type 2590 Battery, operate the battery within the conditions of use specified by the battery manufacturer.



CAUTION:

This device has two SFP+ ports, which may be used with optical transceivers. To avoid hazardous laser radiation, only use with Class 1 transceivers.

Electrical precautions

The Azure Stack Edge Mini R device has the following electrical precautions:



WARNING:

When used with the power supply adaptor:

- Provide a safe electrical earth connection to the power supply cord. The alternating current (AC) cord has a three-wire grounding plug (a plug that has a grounding pin). This plug fits only a grounded AC outlet. Do not defeat the purpose of the grounding pin.
- Given that the plug on the power supply cord is the main disconnect device, ensure that the socket outlets are located near the device and are easily accessible.
- Unplug the power cord(s) (by pulling the plug, not the cord) and disconnect all cables if any of the following conditions exist:
 - The power cord or plug becomes frayed or otherwise damaged.
 - The device is exposed to rain, excess moisture, or other liquids.
 - The device has been dropped and the device casing has been damaged.
 - You suspect the device needs service or repair.
- Permanently unplug the unit before you move it or if you think it has become damaged in any way.
- Provide a suitable power source with electrical overload protection to meet the following power specifications:
 - Voltage: 100 - 240 Volts AC
 - Current: 1.7 Amperes
 - Frequency: 50 to 60 Hz



WARNING:

- Do not attempt to modify or use AC power cord(s) other than the ones provided with the equipment.



WARNING:

- Power supply labeled with this symbol is rated for indoor use only.

Regulatory information

The following contains regulatory information for Azure Stack Edge Mini R device, regulatory model number: TMA01.

The Azure Stack Edge Mini R device is designed for use with NRTL Listed (UL, CSA, ETL, etc.), and IEC/EN 60950-1 or IEC/EN 62368-1 compliant (CE marked) Information Technology equipment.

In countries other than the USA and Canada, network cables (not provided with the equipment) shall not be installed with this equipment if their length is greater than 3 meters.

The equipment is designed to operate in the following environments:

ENVIRONMENT	SPECIFICATIONS
System temperature specifications	<ul style="list-style-type: none"> Storage temperature: -20°C–50°C (-4°F–122°F) Continuous operation: 0°C–40°C (32°F–104°F)
Relative humidity (RH) specifications	<ul style="list-style-type: none"> Storage: 5% to 95% relative humidity Operating: 10% to 90% relative humidity
Maximum altitude specifications	<ul style="list-style-type: none"> Operating: 15,000 feet (4,572 meters) Non-operating: 40,000 feet (12,192 meters)

! **NOTICE:** Changes or modifications made to the equipment not expressly approved by Microsoft may void the user's authority to operate the equipment.

CANADA and USA:

! **NOTICE:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

The Netgear A6150 WiFi USB Adapter provided with this equipment is intended to be operated close to the human body are tested for body-worn Specific Absorption Rate (SAR) compliance. The SAR limit set by the FCC is 1.6 W/kg when averaged over 1 g of tissue. When carrying the product or using it while worn on your body, maintain a distance of 10 mm from the body to ensure compliance with RF exposure requirements.

The Netgear A6150 WiFi USB Adapter complies with ANSI/IEEE C95.1-1999 and was tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C.

Netgear A6150 Specific Absorption Rate (SAR): 1.18 W/kg averaged over 1 g of tissue

The Netgear A6150 WiFi USB Adapter is to be used with approved antennas only. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multitransmitter product procedures. For products available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users are advised that high-power radars are allocated as primary users (priority users) of the bands 5250–5350 MHz and 5650–5850 MHz, and these radars could cause interference and/or damage to LE-LAN devices.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For more information about interference issues, go to the FCC website at fcc.gov/cgb/consumerfacts/interference.html. You can also call the FCC at 1-888-CALL FCC to request Interference and Telephone Interference fact sheets.

Additional information about radiofrequency safety can be found on the FCC website at <https://www.fcc.gov/general/radio-frequency-safety-0> and the Industry Canada website at <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01904.html>.

This product has demonstrated EMC compliance under conditions that included the use of compliant peripheral devices and shielded cables between system components. It is important that you use compliant peripheral devices and shielded cables between system components to reduce the possibility of causing interference to radios, television sets, and other electronic devices.

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3(A)/NMB-3(A)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA

United States: (800) 426-9400

Canada: (800) 933-4750

Netgear A6150 WiFi USB Adapter FCC ID: PY318300429

Netgear A6150 WiFi USB Adapter IC ID: 4054A-18300429

The Netgear A6150 WiFi USB Adapter provided with this equipment is compliant with SAR for general population/uncontrolled exposure limits in IC RSS-102 and has been tested in accordance with the measurement methods and procedures specified in IEEE 1528. Maintain at least 10-mm distance for body-worn condition.

The Netgear A6150 WiFi USB Adapter complies with the Canada portable RF exposure limit set forth for an uncontrolled environment and is safe for intended operation as described in its manual. Further RF exposure reduction can be achieved by keeping the product as far as possible from your body or by setting the device to a lower output power if such a function is available.

A table with the Specific Absorption Rate (SAR) averaged over 1 g for each product can be seen in the USA section above.

L'adaptateur USB WiFi Netgear A6150 fourni avec cet équipement est conforme de SAR pour la population générale / limites d'exposition incontrôlée de CNR-102 et a été testé en conformité avec les méthodes et procédures de mesure spécifiées dans la norme IEEE 1528. Maintenir au moins 10mm à distance pour la condition physique-garde.

L'adaptateur USB WiFi Netgear A6150 est conforme à la limite d'exposition aux RF portable Canada établies pour un environnement non contrôlé et sont sans danger pour le fonctionnement prévu comme décrit dans le manuel. Poursuite de la réduction de l'exposition aux RF peut être réalisé en gardant le produit autant que possible de votre corps ou par le réglage du dispositif à une puissance de sortie inférieure si une telle fonction est disponible.

Un tableau avec le taux d'absorption spécifique (SAR) en moyenne plus de 1g pour chaque produit peut être vu dans la section Des USA ci-dessus.

EUROPEAN UNION:

Request a copy of the EU Declaration of Conformity for this equipment. Send email to CSI_Compliance@microsoft.com.

The Netgear A6150 WiFi USB Adapter provided with this equipment is in compliance with Directive 2014/53/EU and can also be provided on request.



WARNING:

This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Disposal of waste batteries and electrical and electronic equipment:



This symbol on the product or its batteries or its packaging means that this product and any batteries it contains must not be disposed of with your household waste. Instead, it is your responsibility to hand this over to an applicable collection point for the recycling of batteries and electrical and electronic equipment. This separate collection and recycling will help to conserve natural resources and prevent potential negative consequences for human health and the environment due to the possible presence of hazardous substances in batteries and electrical and electronic equipment, which could be caused by inappropriate disposal. For more information about where to drop off your batteries and electrical and electronic waste, please contact your local city/municipality office, your household waste disposal service, or the shop where you purchased this product. Contact erecycle@microsoft.com for additional information on WEEE.

This product contains coin cell battery(ies).

The Netgear A6150 WiFi USB Adapter provided with this equipment is intended to be operated close to the human body and is tested for body-worn Specific Absorption Rate (SAR) compliance (see below values). When carrying the product or using it while worn on your body, maintain a distance of 10mm from the body to ensure compliance with RF exposure requirements.

Netgear A6150 Specific Absorption Rate (SAR): 0.54 W/kg averaged over 10g of tissue

This device may operate in all member states of the EU. Observe national and local regulations where the device is used. This device is restricted to indoor use only when operating in the 5150-5350 MHz frequency range in the following countries:

AT	BE	BG	HR	CY	CZ	DK	
EE	FI	FR	DE	EL	HU	IE	
IT	LV	LT	LU	MT	NL	PL	
PT	RO	SK	SI	ES	SE	UK(NI)	

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of Netgear wireless products for sale in the EU:

WiFi

FREQUENCY RANGE (MHZ)	CHANNELS USED	MAX TRANSMIT POWER (DBM/MW)
2400-2483.5	1-13	ODFM: 19.9 dBm (97.7 mW) CCK: 17.9 dBm (61.7 mW)
5150-5320	36-48	22.9 dBm (195 mW)
5250-5350	52-64	22.9 dBm (195 mW) with TPC 19.9 dBm (97.7 mW) non-TPC
5470-5725	100-140	29.9 dBm (977 mW) with TPC 29.6 dBm (490 mW) non-TPC

Microsoft Ireland Sandyford Ind Est Dublin D18 KX32 IRL

Telephone number: +353 1 295 3826

Fax number: +353 1 706 4110

SINGAPORE:

The Netgear A6150 WiFi USB Adapter provided with this equipment complies with IMDA standards.

Next steps

- [Prepare to deploy Azure Stack Edge Mini R](#)

Azure Stack Edge Mini R system requirements

9/21/2022 • 8 minutes to read • [Edit Online](#)

This article describes the important system requirements for your Microsoft Azure Stack Edge Mini R solution and for the clients connecting to Azure Stack Edge Mini R. We recommend that you review the information carefully before you deploy your Azure Stack Edge Mini R. You can refer back to this information as necessary during the deployment and subsequent operation.

The system requirements for the Azure Stack Edge Mini R include:

- **Software requirements for hosts** - describes the supported platforms, browsers for the local configuration UI, SMB clients, and any additional requirements for the clients that access the device.
- **Networking requirements for the device** - provides information about any networking requirements for the operation of the physical device.

Supported OS for clients connected to device

Here is a list of the supported operating systems for clients or hosts connected to your device. These operating system versions were tested in-house.

OPERATING SYSTEM/PLATFORM	VERSIONS
Windows Server	2016 2019
Windows	10
SUSE Linux	Enterprise Server 12 (x86_64)
Ubuntu	16.04.3 LTS
CentOS	7.0
Mac OS	10.14.1

Supported protocols for clients accessing device

Here are the supported protocols for clients accessing your device.

PROTOCOL	VERSIONS	NOTES
SMB	2.X, 3.X	SMB 1 isn't supported.
NFS	3.0, 4.1	Mac OS is not supported with NFS v4.1.

Supported storage accounts

Here is a list of the supported storage accounts for your device.

STORAGE ACCOUNT	NOTES
Classic	Standard
General Purpose	Standard; both V1 and V2 are supported. Both hot and cool tiers are supported.

Supported Edge storage accounts

The following Edge storage accounts are supported with REST interface of the device. The Edge storage accounts are created on the device. For more information, see [Edge storage accounts](#)

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob	

*Page blobs and Azure Files are currently not supported.

Supported local Azure Resource Manager storage accounts

These storage accounts are via the device local APIs when you are connected to the local Azure Resource Manager. The following storage accounts are supported:

TYPE	STORAGE ACCOUNT	COMMENTS
Standard	GPv1: Block Blob, Page Blob	SKU type is Standard_LRS
Premium	GPv1: Block Blob, Page Blob	SKU type is Premium_LRS

Supported storage types

Here is a list of the supported storage types for the device.

FILE FORMAT	NOTES
Azure block blob	
Azure page blob	
Azure Files	

Supported browsers for local web UI

Here is a list of the browsers supported for the local web UI for the virtual device.

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Google Chrome	Latest version	
Microsoft Edge	Latest version	

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Internet Explorer	Latest version	If enhanced security features are enabled, you may not be able to access local web UI pages. Disable enhanced security, and restart your browser.
FireFox	Latest version	
Safari on Mac	Latest version	

Networking port requirements

Port requirements for Azure Stack Edge Mini R

The following table lists the ports that need to be opened in your firewall to allow for SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access to your device. *Out* or *outbound* refers to the direction in which your Azure Stack Edge Mini R device sends data externally, beyond the deployment, for example, outbound to the internet.

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	NOTES
TCP 80 (HTTP)	Out	WAN	No	Outbound port is used for internet access to retrieve updates. The outbound web proxy is user configurable.
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable.
UDP 123 (NTP)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based NTP server.
UDP 53 (DNS)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based DNS server. We recommend using a local DNS server.
TCP 5985 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTP.

Port No.	In or Out	Port Scope	Required	Notes
TCP 5986 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTPS.
UDP 67 (DHCP)	Out	LAN	In some cases See notes	This port is required only if you're using a local DHCP server.
TCP 80 (HTTP)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. Accessing the local UI over HTTP will automatically redirect to HTTPS.
TCP 443 (HTTPS)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. This port is also used to connect Azure Resource Manager to the device local APIs, to connect Blob storage via REST APIs, and to the Security token service (STS) to authenticate via access and refresh tokens.
TCP 445 (SMB)	In	LAN	In some cases See notes	This port is required only if you are connecting via SMB.
TCP 2049 (NFS)	In	LAN	In some cases See notes	This port is required only if you are connecting via NFS.

Port requirements for IoT Edge

Azure IoT Edge allows outbound communication from an on-premises Edge device to Azure cloud using supported IoT Hub protocols. Inbound communication is only required for specific scenarios where Azure IoT Hub needs to push down messages to the Azure IoT Edge device (for example, Cloud To Device messaging).

Use the following table for port configuration for the servers hosting Azure IoT Edge runtime:

Port No.	In or Out	Port Scope	Required	Guidance
----------	-----------	------------	----------	----------

Port No.	In or Out	Port Scope	Required	Guidance
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound open for IoT Edge provisioning. This configuration is required when using manual scripts or Azure IoT Device Provisioning Service (DPS).

For complete information, go to [Firewall and port configuration rules for IoT Edge deployment](#).

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your Azure Stack Edge Mini R device and the service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. These changes require the network administrator to monitor and update firewall rules for your Azure Stack Edge Mini R as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on Azure Stack Edge Mini R fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

NOTE

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for gateway feature

URL Pattern	Component or functionality
https://*.databoxedge.azure.com/* https://*.servicebus.windows.net/* https://login.microsoftonline.com https://login.microsoftonline.net	Azure Stack Edge service Azure Service Bus Authentication Service - Azure Active Directory
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.windows.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt https://management.azure.com/	Azure storage accounts and monitoring

URL PATTERN	COMPONENT OR FUNCTIONALITY
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
<code>https://azureprofilerfrontdoor.cloudapp.net</code>	Azure Traffic Manager
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
<code>http://<vault-name>.vault.azure.net:443</code>	Key Vault

URL patterns for compute feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscl.io	
https://*.azuredcr.io	Personal and third-party container registries (optional)
https://*.azure-devices.net	IoT Hub access (required)
https://*.docker.com	StorageClass (required)

URL patterns for gateway for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.us/* https://*.servicebus.usgovcloudapi.net/* https://login.microsoftonline.us	Azure Data Box Edge/ Azure Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.us	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.usgovcloudapi.net/* https://*.data.microsoft.com http://*.msftncsi.com https://www.msftconnecttest.com/connecttest.txt	Azure storage accounts and monitoring

URL PATTERN	COMPONENT OR FUNCTIONALITY
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
https://(vault-name).vault.usgovcloudapi.net:443	Key Vault

URL patterns for compute for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.msccr.com	
https://*.azure-devices.us	IoT Hub access (required)
https://*.azuredcrus	Personal and third-party container registries (optional)

Internet bandwidth

The devices are designed to continue to operate when your internet connection is slow or gets interrupted. In normal operating conditions, we recommend that you use:

- A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
- A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Use WAN throttling to limit your WAN throughput to 64 Mbps or higher.

Compute sizing considerations

Use your experience while developing and testing your solution to ensure there is enough capacity on your Azure Stack Edge Mini R device and you get the optimal performance from your device.

Factors you should consider include:

- **Container specifics** - Think about the following.
 - What is your container footprint? How much memory, storage, and CPU is your container consuming?

- How many containers are in your workload? You could have a lot of lightweight containers versus a few resource-intensive ones.
- What are the resources allocated to these containers versus what are the resources they are consuming (the footprint)?
- How many layers do your containers share? Container images are a bundle of files organized into a stack of layers. For your container image, determine how many layers and their respective sizes to calculate resource consumption.
- Are there unused containers? A stopped container still takes up disk space.
- In which language are your containers written?
- **Size of the data processed** - How much data will your containers be processing? Will this data consume disk space or the data will be processed in the memory?
- **Expected performance** - What are the desired performance characteristics of your solution?

To understand and refine the performance of your solution, you could use:

- The compute metrics available in the Azure portal. Go to your Azure Stack Edge resource and then go to **Monitoring > Metrics**. Look at the **Edge compute - Memory usage** and **Edge compute - Percentage CPU** to understand the available resources and how are the resources getting consumed.
- The monitoring commands available via the PowerShell interface of the device such as:
 - `dkr stats` to get a live stream of container(s) resource usage statistics. The command supports CPU, memory usage, memory limit, and network IO metrics.
 - `dkr system df` to get information regarding the amount of disk space used.
 - `dkr image [prune]` to clean up unused images and free up space.
 - `dkr ps --size` to view the approximate size of a running container.

For more information on the available commands, go to [Debug Kubernetes issues](#).

Finally, make sure that you validate your solution on your dataset and quantify the performance on Azure Stack Edge Mini R before deploying in production.

Next step

- [Deploy your Azure Stack Edge Mini R](#)

Azure Stack Edge Mini R limits

9/21/2022 • 3 minutes to read • [Edit Online](#)

Consider these limits as you deploy and operate your Azure Stack Edge Mini R solution.

Azure Stack Edge service limits

- The storage account should be physically closest to the region where the device is deployed (can be different from where the service is deployed).
- Moving a Azure Stack Edge resource to a different subscription or resource group is not supported. For more details, go to [Move resources to new resource group or subscription](#).

Azure Stack Edge Mini R device limits

The following table describes the limits for the Azure Stack Edge Mini R device.

DESCRIPTION	LIMIT
No. of files per device	100 million
No. of shares per container	1
Maximum no. of share endpoints and REST endpoints per device	24
Maximum no. of tiered storage accounts per device	24
Maximum file size written to a share	500 GB
Maximum number of resource groups per device	800

Azure storage limits

This section describes the limits for Azure Storage service, and the required naming conventions for Azure Files, Azure block blobs, and Azure page blobs, as applicable to the Azure Stack Edge service. Review the storage limits carefully and follow all the recommendations.

For the latest information on Azure storage service limits and best practices for naming shares, containers, and files, go to:

- [Naming and referencing containers](#)
- [Naming and referencing shares](#)
- [Block blobs and page blob conventions](#)

IMPORTANT

If there are any files or directories that exceed the Azure Storage service limits, or do not conform to Azure Files/Blob naming conventions, then these files or directories are not ingested into the Azure Storage via the Azure Stack Edge service.

Data upload caveats

Following caveats apply to data as it moves into Azure.

- We suggest that more than one device should not write to the same container.
- If you have an existing Azure object (such as a blob or a file) in the cloud with the same name as the object that is being copied, device will overwrite the file in the cloud.
- An empty directory hierarchy (without any files) created under share folders is not uploaded to the blob containers.
- You can copy the data using drag and drop with File Explorer or via command line. If the aggregate size of files being copied is greater than 10 GB, we recommend you use a bulk copy program such as Robocopy or rsync. The bulk copy tools retry the copy operation for intermittent errors and provide additional resiliency. If using Blob storage via REST, AzCopy or Azure Storage Explorer can be used.
- If the share associated with the Azure storage container uploads blobs that do not match the type of blobs defined for the share at the time of creation, then such blobs are not updated. For example, you create a block blob share on the device. Associate the share with an existing cloud container that has page blobs. Refresh that share to download the files. Modify some of the refreshed files that are already stored as page blobs in the cloud. You will see upload failures.
- After a file is created in the shares, renaming of the file isn't supported.
- Deletion of a file from a share does not delete the entry in the storage account.
- If using rsync to copy data, then `rsync -a` option is not supported.

Azure storage account size and object size limits

Here are the limits on the size of the data that is copied into storage account. Make sure that the data you upload conforms to these limits. For the most up-to-date information on these limits, go to [Azure blob storage scale targets](#) and [Azure Files scale targets](#).

SIZE OF DATA COPIED INTO AZURE STORAGE ACCOUNT	DEFAULT LIMIT
Block Blob and page blob	500 TB per storage account

Azure object size limits

Here are the sizes of the Azure objects that can be written. Make sure that all the files that are uploaded conform to these limits.

AZURE OBJECT TYPE	UPLOAD LIMIT
Block Blob	4.75 TB
Page Blob	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.
Azure Files	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

IMPORTANT

Creation of files (irrespective of the storage type) is allowed up to 5 TB. However, if you create a file whose size is greater than the upload limit defined in the preceding table, the file does not get uploaded. You have to manually delete the file to reclaim the space.

Next steps

- [Prepare to deploy Azure Stack Edge](#)

Azure Stack Edge Mini R technical specifications

9/21/2022 • 3 minutes to read • [Edit Online](#)

The hardware components of your Microsoft Azure Stack Edge Mini R device adhere to the technical specifications and regulatory standards outlined in this article. The technical specifications describe the CPU, memory, power supply units (PSUs), storage capacity, enclosure dimensions, and weight.

Compute, memory

The Azure Stack Edge Mini R device has the following specifications for compute and memory:

SPECIFICATION	VALUE
CPU type	Intel Xeon-D 1577
CPU: raw	16 total cores, 32 total vCPUs
CPU: usable	24 vCPUs
Memory type	16 GB 2400 MT/s SODIMM
Memory: raw	48 GB RAM (3 x 16 GB)
Memory: usable	32 GB RAM

Compute acceleration

A Vision Processing Unit (VPU) is included on every Azure Stack Edge Mini R device that enables Kubernetes, deep neural network and computer vision based applications.

SPECIFICATION	VALUE
Compute Acceleration card	Intel Movidius Myriad X VPU For more information, see Intel Movidius Myriad X VPU

Storage

The Azure Stack Edge Mini R device has 1 data disk and 1 boot disk (that serves as operating system storage). The following table shows the details for the storage capacity of the device.

SPECIFICATION	VALUE
Number of solid-state drives (SSDs)	2 X 1 TB disks One data disk and one boot disk
Single SSD capacity	1 TB
Total capacity (data only)	1 TB

SPECIFICATION	VALUE
Total usable capacity*	~ 750 GB

Some space is reserved for internal use.

Network

The Azure Stack Edge Mini R device has the following specifications for the network:

SPECIFICATION	VALUE
Network interfaces	2 x 10 Gbps SFP+ Shown as PORT 3 and PORT 4 in the local UI
Network interfaces	2 x 1 Gbps RJ45 Shown as PORT 1 and PORT 2 in the local UI
Wi-Fi	802.11ac

Routers and switches

The following routers and switches are compatible with the 10 Gbps SFP+ network interfaces (Port 3 and Port 4) on your Azure Stack Edge Mini R devices:

ROUTER/SWITCH	NOTES
VoyagerESR 2.0	Cisco ESS3300 Switch component
VoyagerSW26G	
VoyagerVM 3.0	
TDC Switch	
TRX R2 (8-Core)	
SW12GG	

Transceivers, cables

The following copper SFP+ (10 Gbps) transceivers and cables are strongly recommended for use with Azure Stack Edge Mini R devices. Compatible fiber-optic cables can be used with SFP+ network interfaces (Port 3 and Port 4) but have not been tested.

SFP+ TRANSCEIVER TYPE	SUPPORTED CABLES	NOTES

SFP+ TRANSCEIVER TYPE	SUPPORTED CABLES	NOTES
SFP+ Direct-Attach Copper (10GSFP+Cu)	<ul style="list-style-type: none"> • FS SFP-10G-DAC (Available in industrial temperature -40°C to +85°C as custom order) • 10Gtek CAB-10GSFP-P0.5M • Cisco SFP-H10GB-CU1M 	<ul style="list-style-type: none"> • Also known as SFP+ Twinax DAC cables. • Recommended option because it has lowest power usage and is simplest. • Autonegotiation is not supported. • Connecting an SFP device to an SFP+ device is not supported.

Power supply unit

The Azure Stack Edge Mini R device includes an external 85 W AC adapter to supply power and charge the onboard battery.

The following table shows the power supply unit specifications:

SPECIFICATION	VALUE
Maximum output power	85 W
Frequency	50/60 Hz
Voltage range selection	Auto ranging: 100-240 V AC

Included battery

The Azure Stack Edge Mini R device also includes an onboard battery that is charged by the power supply.

An additional [Type 2590 battery](#) can be used along with the onboard battery to extend the use of the device between the charges. This battery should be compliant with all the safety, transportation, and environmental regulations applicable in the country of use.

SPECIFICATION	VALUE
Onboard battery capacity	73 Wh

Enclosure dimensions and weight

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The following table lists the dimensions of the device and the USP with the rugged case in millimeters and inches.

ENCLOSURE	MILLIMETERS	INCHES
Height	68	2.68

ENCLOSURE	MILLIMETERS	INCHES
Width	208	8.19
Length	259	10.20

Enclosure weight

The following table lists the weight of the device including the battery.

ENCLOSURE	WEIGHT
Total weight of the device	7 lbs

Enclosure environment

This section lists the specifications related to the enclosure environment, such as temperature, humidity, and altitude.

SPECIFICATIONS	DESCRIPTION
Temperature range	0 – 40° C (operational)
Vibration	MIL-STD-810 Method 514.7* Procedure I CAT 4, 20
Shock	MIL-STD-810 Method 516.7* Procedure IV, Logistic
Altitude	Operational: 15,000 feet Non-operational: 40,000 feet

*All references are to MIL-STD-810G Change 1 (2014)

Next steps

- [Deploy your Azure Stack Edge Mini R](#)

Deployment checklist for your Azure Stack Edge Mini R device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This article describes the information that can be gathered ahead of the actual deployment of your Azure Stack Edge Mini R device.

Use the following checklist to ensure you have this information after you have placed an order for an Azure Stack Edge Mini R device and before you have received the device.

Deployment checklist

STAGE	PARAMETER	DETAILS
Device management	<ul style="list-style-type: none">Azure subscriptionResource providers registeredAzure Storage account	<ul style="list-style-type: none">Enabled for Azure Stack Edge Mini R/Data Box Gateway, owner or contributor access.In Azure portal, go to Home > Subscriptions > Your-subscription > Resource providers. Search for Microsoft.DataBoxEdge and register. Repeat for Microsoft.Devices if deploying IoT workloads.Need access credentials.
Device installation	Power cables in the package. For US, an SVE 18/3 cable rated for 125 V and 15 Amps with a NEMA 5-15P to C13 (input to output) connector is shipped.	For more information, see the list of Supported power cords by country .
	<ul style="list-style-type: none">At least 1 X 1-GbE RJ-45 network cable for Port 1At least 1 X 25-GbE SFP+ copper cable for Port 3, Port 4, Port 5, or Port 6	Customer needs to procure these cables. For a full list of supported network cables, switches, and transceivers for device network cards, see Cavium FastlinQ 41000 Series Interoperability Matrix and Mellanox dual port 25G ConnectX-4 channel network adapter compatible products .
Network readiness	Check to see how ready your network is for the deployment of an Azure Stack Edge device.	Use the Azure Stack Network Readiness Checker to test all needed connections.
First-time device connection	Laptop whose IPv4 settings can be changed. This laptop connects to Port 1 via a switch or a USB to Ethernet adaptor.	

Stage	Parameter	Details
Device sign-in	Device administrator password, between 8 and 16 characters, including three of the following character types: uppercase, lowercase, numeric, and special characters.	Default password is <i>Password1</i> , which expires at first sign-in.
Network settings	<p>Device comes with 2 x 1-GbE, 4 x 25-GbE network ports.</p> <ul style="list-style-type: none"> Port 1 is used to configure management settings only. One or more data ports can be connected and configured. At least one data network interface from among Port 2 - Port 6 needs to be connected to the Internet (with connectivity to Azure). DHCP and static IPv4 configuration supported. 	Static IPv4 configuration requires IP, DNS server, and default gateway.
Compute network settings	<ul style="list-style-type: none"> Require 2 free, static, contiguous IPs for Kubernetes nodes, and 1 static IP for IoT Edge service. Require 1 additional IP for each extra service or module that you'll deploy. 	Only static IPv4 configuration is supported.
(Optional) Web proxy settings	<ul style="list-style-type: none"> Web proxy server IP/FQDN, port Web proxy username, password 	
Firewall and port settings	If using firewall, make sure the listed URLs patterns and ports are allowed for device IPs.	
(Recommended) Time settings	Configure time zone, primary NTP server, secondary NTP server.	Configure primary and secondary NTP server on local network. If local server is not available, public NTP servers can be configured.
(Optional) Update server settings	Require update server IP address on local network, path to WSUS server.	By default, public Windows update server is used.
Device settings	<ul style="list-style-type: none"> Device fully qualified domain name (FQDN) DNS domain 	

STAGE	PARAMETER	DETAILS
(Optional) Certificates	To test non-production workloads, use Generate certificates option . If you bring your own certificates including the signing chain(s), Add certificates in appropriate format.	Configure certificates only if you change the device name and/or DNS domain.
Activation	Require activation key from the Azure Stack Edge resource.	Once generated, the key expires in 3 days.

Next steps

- Prepare to deploy your [Azure Stack Edge Mini R device](#).
- Use the [Azure Stack Edge Network Readiness Tool](#) to verify your network settings.

Tutorial: Prepare to deploy Azure Stack Edge Mini R

9/21/2022 • 13 minutes to read • [Edit Online](#)

This tutorial is the first in the series of deployment tutorials that are required to completely deploy an Azure Stack Edge Mini R device. This tutorial describes how to prepare the Azure portal to deploy an Azure Stack Edge resource.

You need administrator privileges to complete the setup and configuration process. The portal preparation takes less than 10 minutes.

In this tutorial, you learn how to:

- Create a new resource
- Get the activation key

Get started

To deploy Azure Stack Edge Mini R, refer to the following tutorials in the prescribed sequence.

STEP	DESCRIPTION
Preparation	These steps must be completed in preparation for the upcoming deployment.
Deployment configuration checklist	Use this checklist to gather and record information before and during the deployment.
Deployment prerequisites	These prerequisites validate that the environment is ready for deployment.
Deployment tutorials	These tutorials are required to deploy your Azure Stack Edge Mini R device in production.
1. Prepare the Azure portal for device	Create and configure your Azure Stack Edge resource before you install the physical device.
2. Install the device	Inspect and cable your physical device.
3. Connect to the device	Once the device is installed, connect to device local web UI.
4. Configure network settings	Configure network including the compute network and web proxy settings for your device.
5. Configure device settings	Assign a device name and DNS domain, configure update server and device time.
6. Configure security settings	Configure certificates using your own certificates, set up VPN, and configure encryption-at-rest for your device.
7. Activate the device	Use the activation key from service to activate the device. The device is ready to set up SMB or NFS shares or connect via REST.

STEP	DESCRIPTION
8. Configure compute	Configure the compute role on your device. A Kubernetes cluster is also created.

You can now begin to set up the Azure portal.

Deployment configuration checklist

Before you deploy your device, you need to collect information to configure the software on your Azure Stack Edge Mini R device. Preparing some of this information ahead of time helps streamline the process of deploying the device in your environment. Use the [Azure Stack Edge Mini R deployment configuration checklist](#) to note down the configuration details as you deploy your device.

Prerequisites

Following are the configuration prerequisites for your Azure Stack Edge resource, your Azure Stack Edge device, and the datacenter network.

For the Azure Stack Edge resource

Before you begin, make sure that:

- Your Microsoft Azure subscription is enabled for an Azure Stack Edge resource. Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#).
- You have owner or contributor access at resource group level for the Azure Stack Edge, IoT Hub, and Azure Storage resources.
- To create an order in the Azure Edge Hardware Center, you need to make sure that the Microsoft.EdgeOrder provider is registered. For information on how to register, go to [Register resource provider](#).
- To create any Azure Stack Edge resource, you should have permissions as a contributor (or higher) scoped at resource group level. You also need to make sure that the `Microsoft.DataBoxEdge` provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create any IoT Hub resource, make sure that Microsoft.Devices provider is registered. For information on how to register, go to [Register resource provider](#).
 - To create a Storage account resource, again you need contributor or higher access scoped at the resource group level. Azure Storage is by default a registered resource provider.
- You have admin or user access to Azure Active Directory Graph API. For more information, see [Azure Active Directory Graph API](#).
- You have your Microsoft Azure storage account with access credentials.

For the Azure Stack Edge device

Before you deploy a physical device, make sure that:

- You've run the [Azure Stack Network Readiness Checker tool](#) to check network readiness for your Azure Stack Edge device. You can use the tool to check whether your firewall rules are blocking access to any essential URLs for the service and verify custom URLs, among other tests. For more information, see [Check network readiness for your Azure Stack Edge device](#).
- You've reviewed the safety information for this device at [Safety guidelines for your Azure Stack Edge device](#).

- You have received the physical device.
- You have access to a flat, stable, and level work surface where the device can rest safely.
- The site where you intend to set up the device has standard AC power from an independent source or a rack power distribution unit (PDU).

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured per the networking requirements for your Azure Stack Edge device. For more information, see [Azure Stack Edge Mini R system requirements](#).
- For normal operating conditions of your Azure Stack Edge, you have:
 - A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
 - A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Create a new resource

If you have an existing Azure Stack Edge resource to manage your physical device, skip this step and go to [Get the activation key](#).

- [Azure Edge Hardware Center \(Preview\)](#)
- [Azure CLI](#)

Azure Edge Hardware Center (Preview) lets you explore and order a variety of hardware from the Azure hybrid portfolio including Azure Stack Edge Pro devices.

When you place an order through the Azure Edge Hardware Center, you can order multiple devices, to be shipped to more than one address, and you can reuse ship to addresses from other orders.

Ordering through Azure Edge Hardware Center will create an Azure resource that will contain all your order-related information. One resource each will be created for each of the units ordered. You will have to create an Azure Stack Edge resource after you receive the device to activate and manage it.

To place an order through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.
2. Select **+ Create a resource**. Search for and select **Azure Edge Hardware Center**. In the Azure Edge Hardware Center, select **Create**.

Home > Create a resource > Marketplace >

Azure Edge Hardware Center

Microsoft



Azure Edge Hardware Center

Microsoft
☆☆☆☆ 0.0 (0 ratings)

[Create](#)

Overview Plans Usage Information + Support Reviews

Use Azure Edge Hardware Center to order first-party Azure hardware that lets you build and run hybrid apps across datacenters, edge locations, remote offices and the cloud.

Azure Edge Hardware Center lets you choose from a variety of hardware as per your business need and helps you keep track of all the ordered hardware at a single place.

More offers from Microsoft [See All](#)

 Workspace Microsoft Virtual Machine Azure Virtual Desktop resource	 Microsoft HPC Pack 2012 R2 Microsoft Virtual Machine Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux workloads.	 Windows 10 IoT Core Services Microsoft Azure Service Commercialize your project with enterprise-grade security and support	 Web App + SQL Microsoft Azure Service Enjoy secure and flexible development, deployment, and scaling options for your web app
--	--	--	--

[Create](#) [Create](#) [Create](#) [Create](#)

3. Select a subscription, and then select **Next**.

Home > Create a resource > Marketplace > Azure Edge Hardware Center >

Get started ...

Get started [...](#) [X](#)

Info Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select a subscription

Select a subscription to manage deployed resources and costs.

Subscription [Contoso_USEast](#)

[Next](#)

4. To start your order, select **Order** beside the product family that you want to order - for example, **Azure Stack Edge**. If you don't see the product family, you may need to use a different subscription; select **Try selecting a different subscription**.

Get started

X

 Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select product family

Showing 1 product families for selected subscription: ExpressPod BVT (Creates order in BVT env)

Azure Stack Edge

Azure managed physical edge compute device

[Order](#)

Can't see the product family you are looking for? [Try selecting a different subscription.](#)

5. Select the shipping destination for your order.

Azure Edge Hardware Center

X

 Azure Edge Hardware Center lets you order a variety of hardware from the Azure hybrid portfolio and serves all order related information at one place. [What's new?](#)

Select shipping destination

Azure Stack Edge

Order to be billed against subscription: Contoso_USWest ([Change](#))

Select the country/region where you would like your device to be shipped. *

▼

[Next](#)

6. On the **Select Hardware** page, use the **Select** button to select the hardware product to order. For example, here **Azure Stack Edge Pro - GPU** was selected.

 Select Hardware ... X

Hardware family: Azure Stack Edge ([Change](#)) Subscription: Contoso_USWest Ship to country/region: United States

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Device specifications	<ul style="list-style-type: none"> • 1U rack mount device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Azure Private Edge Zones enabled 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Pro R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Portable, server class device with network data transfer capabilities • Hardware accelerated ML using Nvidia T4 GPU • Specialized rugged casing tailored for harsh environments 	Starting from \$\$\$ USD	Select
 Azure Stack Edge Mini R  Double encryption enabled Device specifications	<ul style="list-style-type: none"> • Ultra-portable, WiFi enabled device with battery • Hardware accelerated ML using VPU • Specialized rugged casing tailored for harsh environments 	\$\$\$ USD	Select

After you select a hardware product, you'll select the device configuration to order. For example, if you chose Azure Stack Edge Pro - GPU, you can choose from Azure Stack Edge Pro - 1 GPU and Azure Stack Edge Pro - 2 GPU models.

7. Select the device configuration, and then choose **Select**. The available configurations depend on the hardware you selected. The screen below shows available configurations for Azure Stack Edge Pro - GPU devices.

If you're ordering Azure Stack Edge Mini R devices, which all have the same configuration, you won't see this screen.

Home >
Select Hardware ...

Hardware family: Azure Stack Edge ([Change](#)) Azure managed physical edge compute device

Showing 3 hardware products

 Azure Stack Edge Pro - GPU Hardware specifications	<p>Azure Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. The device is powered with NVIDIA T4 GPUs to provide accelerated AI inferencing at the edge. You can choose from the available configurations with one or two GPUs basis your business need</p> <p>Select a configuration</p> <table border="1"> <thead> <tr> <th>Model</th> <th>Usable compute</th> <th>Usable memory</th> <th>Usable storage</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> <tr> <td><input type="radio"/> Azure Stack Edge Pro - 2 GPU</td> <td>40 vCPU</td> <td>102 GB</td> <td>4.2 TB</td> </tr> </tbody> </table> <p>Learn more Azure Stack Edge Pro - GPU documentation</p>				Model	Usable compute	Usable memory	Usable storage	<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB	<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB
Model	Usable compute	Usable memory	Usable storage													
<input checked="" type="radio"/> Azure Stack Edge Pro - 1 GPU	40 vCPU	102 GB	4.2 TB													
<input type="radio"/> Azure Stack Edge Pro - 2 GPU	40 vCPU	102 GB	4.2 TB													

Select

The **Create order** wizard opens.

8. On the **Basics** tab, provide an **Order name**, **Resource group**, and **Region**. Then select **Next: Shipping + quantity >**.

Create order



Basics Shipping + quantity Notifications Tags Review + create

Hardware details

Azure Stack Edge Pro - 1 GPU

Usable compute : 40 vCPU Usable memory : 102 GB

Usable storage : 4.2 TB

Order details

Order name *

Pro1GPUdevices

The selected subscription will be used to manage deployed resources and billing. Select or create a new resource group to organize and manage all your resources.

Subscription *

Contoso_USEast

Resource group *

USEast_ASE



[Create new](#)

Region *

East US



Review + create

< Previous

Next : Shipping + quantity >

Next, you'll add each ship to address you want to send devices to and then specify how many devices to send to each address. You can order up to 20 units (devices) per order.

9. On the **Shipping + quantity** tab, add each ship to address to send devices to:

- To add a new ship to address, select **Add a new address**.

A required **Address alias** field on the **New address** screen identifies the address for later use.

Select **Add** when you finish filling in the address fields. Then use **Select address(es)** to add the address to your order.

- To use a ship to address from a previous order, or to use an address that you just added, choose **Select address(es)**. Then, on the **Select address(es)** screen, select one or more addresses, and choose **Select**.

<input type="checkbox"/>	Contact person	Address
<input checked="" type="checkbox"/>	Gus Poland 4255555555 gusp@contoso.com Contoso LE	contoso-redmond One Microsoft Way Building 52 Redmond WA 98152 United States
<input type="checkbox"/>	Gus Poland 4085555555 gusp@contoso.com Contoso LE	contoso-sunnyvale 1020 Enterprise Way Building 2 Sunnyvale CA 94089 United States
<input checked="" type="checkbox"/>	Claudia Olivares 4085555555 gusp@contoso.com Contoso LE	SVBldg2 1020 Enterprise Way Building 2 Sunnyvale

The **Shipping + quantity** tab now has a separate item for each ship to address.

Each order item name includes a name prefix (the order name followed by the address alias), with an item number for each device that is shipped to that address.



Create order

...

Basics **Shipping + quantity**

Notifications

Tags

Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Su CA 94089 US	1	Pro1GPUDevicesSVBldg2-01 Order name Address alias Item #
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01

[Review + create](#) [< Previous](#) [Next : Notifications >](#)

- For each address, enter the **Quantity** of devices to ship on the **Shipping + quantity** tab.

When you enter a quantity of more than one, a **+n more** label appears after the order item name.



Create order

...

Basics **Shipping + quantity**

Notifications

Tags

Review + create

You can order up to 20 hardware units and set up multiple shipping addresses in a single order. A unique order item name is generated automatically for each hardware unit. You can edit the order item name.

Ship to address	Quantity	Order item name
SVBldg2 1020 Enterprise Way, Building 2, Sunnyva CA 94089 US	3	Pro1GPUDevicesSVBldg2-... +2 more [Delete]
gusp 1020 Enterprise Way, Sunnyvale CA 94089 US	1	Pro1GPUDevicesgusp-01 [Delete]

[Add a new address](#) [Select address\(es\)](#)

- If you want to change the names of order items, select and click the order item name to open the **Rename order item** pane. If you're shipping more than one item to an address, select **+n more**.

You can make two types of name change:

- To use a different name prefix for all of the order items, edit the **Name prefix** and then select

Apply, as shown on the following screen.

- You can also edit the name of each order item individually.

When you finish, select **Done**.

Select **Next: Notifications** > to continue.

12. If you want to receive status notifications as your order progresses, enter the email address for each recipient on the **Notifications** tab.

To add an email address, enter the address, and select **Add**. You can add up to 20 email addresses.

Home > Select Hardware >

Create order ... X

Basics Shipping + quantity **Notifications** Tags Review + create

We will update you regarding your order progress. You can specify up to 20 email address(es) to receive updates for your order status. Your subscription owner and admin will receive email notifications by default.

Email

claudiao@contoso.com Add

gusp@contoso.com Remove

OpsMgmt@contoso.com Remove

Review + create < Previous Next : Tags >

When you finish, select **Review + create** to continue.

13. On the **Review + create** tab:

- Review your order. The order is automatically validated when you open this screen. If you see a **Validation failed** banner, you'll have to fix the issues before you create the order.
- Review the **Privacy terms**, and select the check box to agree to them.
- Select **Create**.



Validation passed.

Basics Shipping + quantity Notifications Tags Review + create

Order name Pro1GPUdevices

Total hardware units 4

Total monthly service fee <Fee>

Total shipping fee <Fee>

Hardware details

Azure Stack Edge Pro - 1 GPU

Usable compute 40 vCPU

Usable memory 102 GB

Usable storage 4.2 TB

Terms and conditions

Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Basics

Subscription Contoso_USEast

Resource Group USEast_ASE

Region East US

Notifications

Emails gusp@contoso.com, OpsMgmt@contoso.com

Shipping + quantity

▽ Total hardware units (4)

Shipping address	Order item name
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-01
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-02
SVBldg2, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicesSunnyvale2-03
contoso-sunnyvale, 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US	Pro1GPUdevicescontoso-su-01

Create

< Previous

Next >

During deployment, the order opens in the portal, with the status of each order item displayed. After deployment completes, you may need to click the Down arrow by **Deployment details** to see the status of individual items.

Resource	Type	Status	Operation details
SVBldg2	Microsoft.EdgeOrder/addresses	OK	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-01	Microsoft.EdgeOrder/orderItems	OK	Operation details
Pro1GPUDevicesSunnyvale2-02	Microsoft.EdgeOrder/orderItems	Accepted	Operation details
Pro1GPUDevicesSunnyvale2-03	Microsoft.EdgeOrder/orderItems	OK	Operation details

14. To view details for an order item, shown below, select the item in the **Resource** column of the deployment details.

Resource group (change)	Order name	Order item name
USEast_ASE	Pro1GPUdevices	Pro1GPUdevicesSunnyvale2-03

Order item confirmed
Your order item is now confirmed and is being prepared for shipment. Shipping details will be sent via email once the item is dispatched.

Order item information		
Placed on	: 8/6/2021	Shipping address 1020 Enterprise Way, Building 2, Sunnyvale CA 94089 US
Order name	: Pro1GPUdevices	Contact information Claudia Olivares 4085550111, claudiao@contoso.com
View Updates		

Hardware information		
<ul style="list-style-type: none"> Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage 		
<ul style="list-style-type: none"> While your hardware arrives, configure your infrastructure. Learn more 		

15. After a device ships (**Shipped** tag is green), a **Configure hardware** option is added to the item details. Select that option to create a management resource for the device in Azure Stack Edge.

The screenshot shows the Azure Edge Hardware Center interface for an order named 'DemoOrderASAdd1-03'. The 'Overview' tab is selected. Key details shown include:

- Resource group: USEast_ASE
- Location: eastus2euap
- Subscription: Contoso_USEast
- Subscription ID: 1a23bc45-678d-90f1-2ghi-j34klm6n678o
- Tags: Ordered, Shipped (highlighted with a red box), Delivered
- Order name: Pro1GPUDevices
- Order item name: Pro1GPUDevicesSunnyvale2-02 -03
- Placed on: 6/24/2021
- Order name: DemoOrderAS
- Shipping address: abc street, xyz city, pqr state 7698798 US
- Contact information: Anam Shaher, 8768789798, ashaher@hotmail.com
- Hardware information: Azure Stack Edge Pro - 1 GPU: 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage
- Configure hardware button (highlighted with a red box)

The subscription, resource group, and deployment area are filled in from the order, but you can change them.

The screenshot shows the 'Create management resource' wizard for an Azure Stack Edge device. The 'Basics' tab is selected. The device details are:

Device	Order resource name	Status
Azure Stack Edge Pro - 1 GPU	DemoOrderASAdd1-03	Delivered

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * ⓘ: Contoso_USEast

Resource group * ⓘ: USEast_ASE

INSTANCE DETAILS

Name * ⓘ: (empty input field)

Deploy Azure resource in * ⓘ: (US) East US

Buttons at the bottom: Review + create, Previous, Next: Tags

After you activate the device, you'll be able to open the management resource from the item, and open the order item from the management resource.

Create a management resource for each device

To manage devices that are ordered through the Azure Edge Hardware Center, you'll create a management resource for each device in Azure Stack Edge. When the device is activated, the management resource is associated with an order item. You'll be able to open the order item from the management resource and open

the management resource from the order item.

After a device is delivered, a **Configure hardware** link is added to the order item detail, giving you a direct way to open a wizard for creating a management resource. You can also use the **Create management resource** option in Azure Stack Edge.

To create a management resource for a device ordered through the Azure Edge Hardware Center, do these steps:

1. Use your Microsoft Azure credentials to sign in to the Azure portal at this URL: <https://portal.azure.com>.

2. There are two ways to get started creating a new management resource:

- Through the Azure Edge Hardware Center: Search for and select **Azure Edge Hardware Center**.

In the Hardware Center, display **All order items**. Select the item **Name**. In the item **Overview**, select **Configure hardware**.

The **Configure hardware** option appears after a device is shipped.



- In Azure Stack Edge: Search for and select **Azure Stack Edge**. Select **+ Create**. Then select **Create management resource**.



The **Create management resource** wizard opens.

3. On the **Basics** tab, enter the following settings:

SETTING	VALUE
Select a subscription ¹	Select the subscription to use for the management resource.
Resource group ¹	Select the resource group to use for the management resource.
Name	Provide a name for the management resource.
Deploy Azure resource in	Select the country or region where the metadata for the management resource will reside. The metadata can be stored in a different location than the physical device.

¹ An organization may use different subscriptions and resource groups to order devices than they use to manage them.

Create management resource

X

Azure Stack Edge

i After you've created this resource, you can activate an Azure Stack Edge device and manage it through this resource. If you don't have a physical device, you can order it through the [Azure Edge Hardware Center](#).

Basics Tags Review + create**PROJECT DETAILS**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Select a subscription * ⓘ

DataBox_Edge_Test

Resource group * ⓘ

myaserg

Create new

INSTANCE DETAILS

Name * ⓘ

myasetestorder

Deploy Azure resource in * ⓘ

(US) East US

Review + create

Previous

Next: Tags

Select **Review + create** to continue.

4. On the **Review + create** tab, review basic settings for the management resource and the terms of use. Then select **Create**.

If you started this procedure by clicking **Configure hardware** for a delivered item in an Azure Edge Hardware Center order, the device, order resource name, and order status are listed at the top of the screen.

Home > Azure Edge Hardware Center > nidhitest1nidhiaddr-04 >

Create management resource

Azure Stack Edge

All validations have passed.

Basics Tags Review + create

Device	Order resource name	Status
Azure Stack Edge Pro - 2 GPU	nidhitest1nidhiaddr-04	Delivered

Terms and conditions
Your use of the Azure service is governed by the terms and conditions of the agreement under which you obtained the service. For more information see [Terms of use](#).

Basics

Subscription	ExpressPod BVT (Creates order in BVT env)
Resource group	nidhitest
Name	myNewDevice
Region	(US) East US

Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.

Create Previous Next

The **Create** button isn't available until all validation checks have passed.

5. When the process completes, the Overview pane for new resource opens.

Home > Sunnyvale-ASE1GPUdevices-01 | Overview

Deployment

Search (Ctrl+ /) <> Delete Cancel Redeploy Refresh

Overview We'd love your feedback! ↗

Your deployment is complete

Deployment name: Sunnyvale-ASE1GPUdevices-01 Start time: 6/29/2021, 6:04:02 PM
Subscription: Azure Data Box testing Correlation ID: bee14110-d803-4ff4-82a5-6f7e1420d216
Resource group: ContosoEastRG

Deployment details (Download)

Resource	Type	Status	Operation details
Sunnyvale-ASE1GPUdevice	Microsoft.DataBoxEdge/...	OK	Operation details

Next steps Go to resource

Security Center Secure your apps and infrastructure [Go to Azure security center >](#)

Free Microsoft tutorials Start learning today >

Work with an expert Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

Get the activation key

After the Azure Stack Edge resource is up and running, you'll need to get the activation key. This key is used to activate and connect your Azure Stack Edge Mini R device with the resource. You can get this key now while you are in the Azure portal.

- Select the resource you created, and select **Overview**.

The screenshot shows the Azure Stack Edge device management interface. On the left, a sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring (Device events, Alerts, Metrics). The 'Overview' tab is highlighted with a red box. The main content area displays a message: 'Device is not activated. Review the steps to configure and activate your device.' Below this, it says 'Your order is being processed!' and provides a status update: 'Microsoft is reviewing your order. We will inform you via email once the device is shipped. Your billing starts 14 days after the shipment.' A section titled 'While your device arrives...' contains two steps: '1 Configure your infrastructure to activate your device. See configuration steps.' and '2 After activation, deploy services on your device to speed up data processing time.' To the right, there's a 'Edge services' section with three cards: 'Virtual machines' (New), 'IoT Edge', and 'Cloud storage gateway'. Each card has a brief description and a 'How to get started?' link.

2. On the **Activate** tile, provide a name for the Azure Key Vault, or accept the default name. The key vault name can be between 3 and 24 characters.

A key vault is created for each Azure Stack Edge resource that is activated with your device. The key vault lets you store and access secrets. For example, the Channel Integrity Key (CIK) for the service is stored in the key vault.

Once you've specified a key vault name, select **Generate activation key** to create an activation key.

This screenshot shows the same Azure Stack Edge interface as the previous one, but the 'Activate' step is now active. In the main content area, under the 'Your device is on your way...' section, there is a form for generating an activation key. It includes a field labeled 'Azure key vault name *' with the value 'ase-myasetest-ed30d9ee38' and a blue button labeled 'Generate activation key'. Below the form, a note says 'Ensure that your infrastructure is configured. Refer [steps to configure](#)'. The rest of the interface remains the same, with the sidebar and other service cards visible.

Wait a few minutes while the key vault and activation key are created. Select the copy icon to copy the key and save it for later use.

IMPORTANT

- The activation key expires three days after it is generated.
- If the key has expired, generate a new key. The older key is not valid.

Next steps

In this tutorial, you learned about Azure Stack Edge topics such as:

- Create a new resource
- Get the activation key

Advance to the next tutorial to learn how to install Azure Stack Edge.

[Install Azure Stack Edge](#)

Tutorial: Install Azure Stack Edge Mini R

9/21/2022 • 5 minutes to read • [Edit Online](#)

This tutorial describes how to install an Azure Stack Edge Mini R physical device. The installation procedure involves cabling the device.

The installation can take around 30 minutes to complete.

In this tutorial, you learn how to:

- Inspect the device
- Cable the device

Prerequisites

The prerequisites for installing a physical device as follows:

For the Azure Stack Edge resource

Before you begin, make sure that:

- You've completed all the steps in [Prepare to deploy Azure Stack Edge Mini R](#).
 - You've created an Azure Stack Edge resource to deploy your device.
 - You've generated the activation key to activate your device with the Azure Stack Edge resource.

For the Azure Stack Edge Mini R physical device

Before you deploy a device:

- Make sure that the device rests safely on a flat, stable, and level work surface.
- Verify that the site where you intend to set up has:
 - Standard AC power from an independent source -OR-
 - A rack power distribution unit (PDU).

For the network in the datacenter

Before you begin:

- Review the networking requirements for deploying Azure Stack Edge Mini R, and configure the datacenter network per the requirements. For more information, see [Azure Stack Edge networking requirements](#).
- Make sure that the minimum Internet bandwidth is 20 Mbps for the optimal functioning of the device.

Inspect the device

This device is shipped as a single unit. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the device case for any damage. Open the case and inspect the device. If the case or the device appears to be damaged, contact Microsoft Support to help you assess whether the device is in good working order.
3. After the case is opened, make sure that you have:
 - One portable Azure Stack Edge Mini R device with side bumpers attached
 - One battery and the back cover attached to the device.

- One power cord to connect the battery to power source

If you didn't receive all of the items listed here, contact Azure Stack Edge support. The next step is to cable your device.

Cable the device

The following procedures explain how to cable your Azure Stack Edge device for power and network.

Before you start cabling your device, you need the following:

- Your Azure Stack Edge Mini R physical device on the installation site.
- One power cable.
- At least one 1-GbE RJ-45 network cable to connect to the management interface. There are two 1-GbE network interfaces, one management and one data, on the device.
- One 10-GbE SFP+ cable for each data network interface to be configured. At least one data network interface from PORT 3 or PORT 4 needs to be connected to the Internet (with connectivity to Azure).

Use of the highest-performing copper SFP+ (10 Gbps) transceiver is strongly recommended. Compatible fiber-optic transceivers can be used but have not been tested. For more information, see [transceiver and cable specifications](#) for Azure Stack Edge Mini R.

- Access to one power distribution unit (recommended).

NOTE

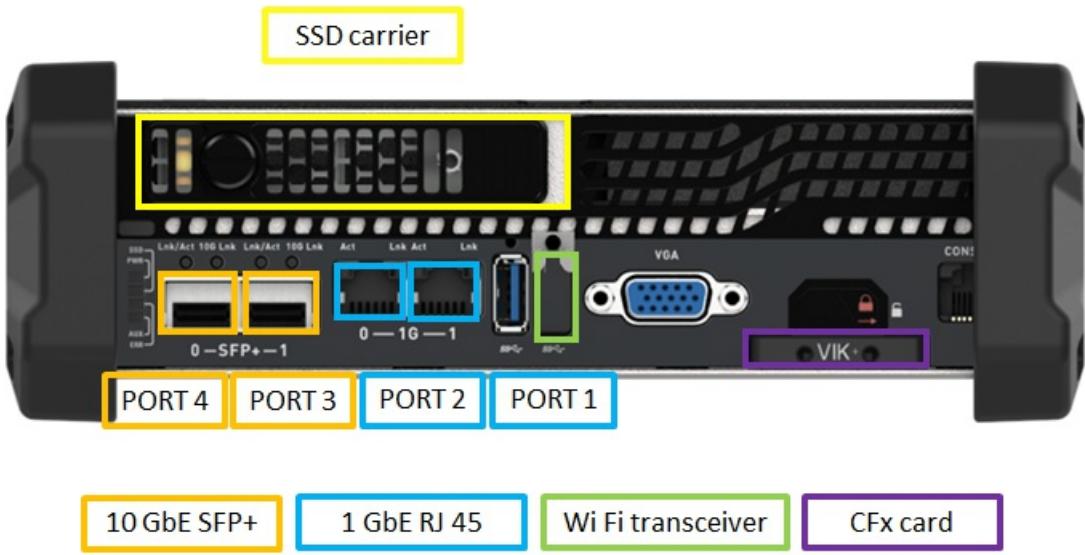
- If you are connecting only one data network interface, we recommend that you use a 10-GbE network interface such as PORT 3 or PORT 4 to send data to Azure.
- For best performance and to handle large volumes of data, consider connecting all the data ports.
- The Azure Stack Edge device should be connected to the datacenter network so that it can ingest data from data source servers.

On your Azure Stack Edge device:

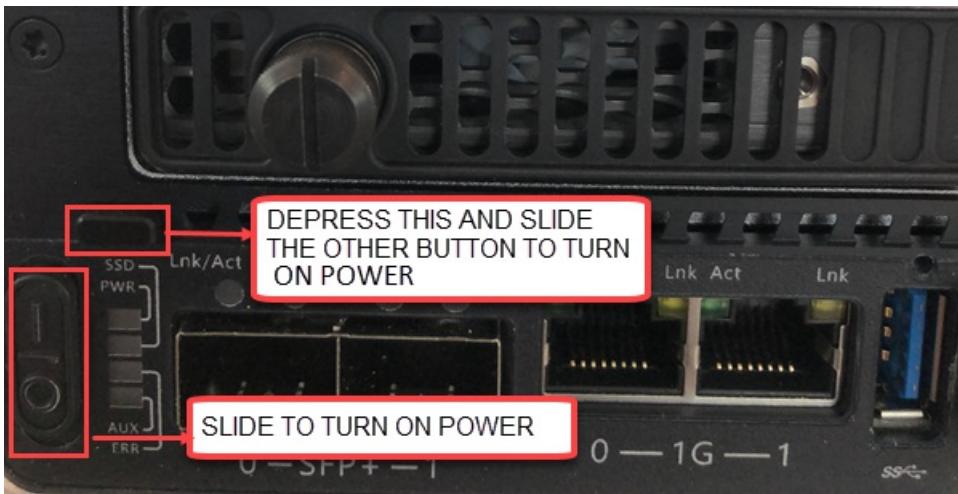
- The front panel has an SSD carrier.
 - The device has 1 SSD disk in the slot.
 - The device also has a CFx card that serves as storage for the operating system disk.
- The front panel has network interfaces and access to Wi-Fi.
 - 2 X 1 GbE RJ 45 network interfaces (PORT 1 and PORT 2 on the local UI of the device)
 - 2 X 10 GbE SFP+ network interfaces (PORT 3 and PORT 4 on the local UI of the device)
 - One Wi-Fi port with a Wi-Fi transceiver attached to it.
- The front panel also has a power button.
- The back panel includes a battery and a cover that are installed on the device.

Take the following steps to cable your device for power and network.

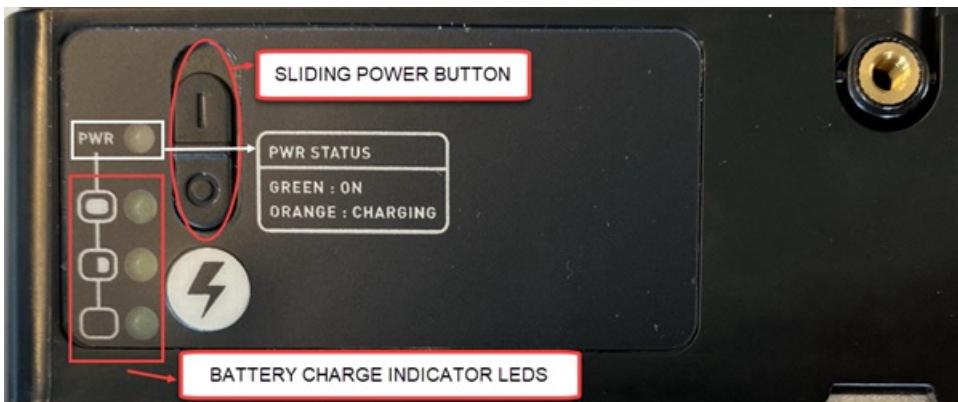
1. Identify the various network and storage components on the front plane of your device.



2. Locate the power button on the bottom-left corner of the front of the device.



3. The battery is connected to the back plane of your device. Identify the second power button located on the battery.



Connect one end of the power cord to the battery and the other to the power outlet.



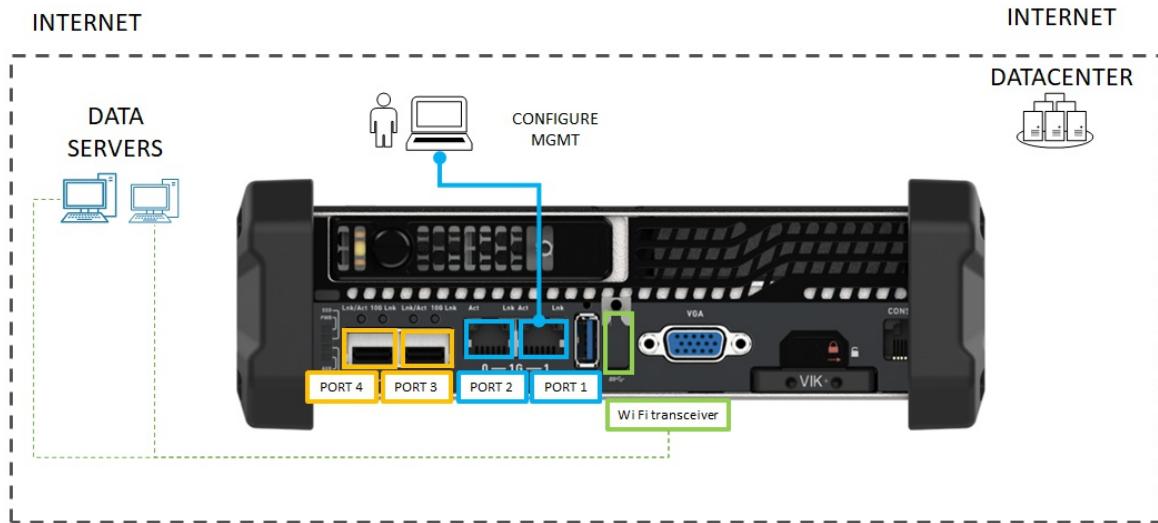
When running only on battery (battery is not connected to the source of power), both the power switch on the front and the switch on the battery should be toggled to ON position. When the battery is connected to a power source, only the power button on the front of the device should be toggled to ON position.

4. Press the power button in the front plane to turn on the device.

NOTE

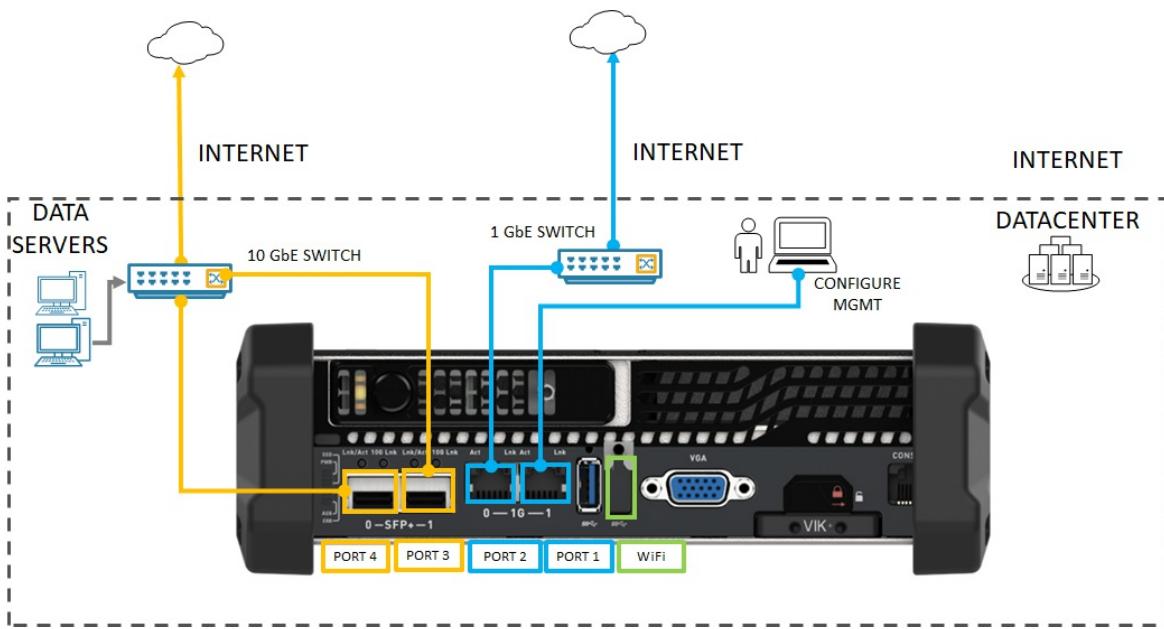
To turn on or turn off the power to the device, you have to depress the black button on top of the power button and then toggle the power button to ON or OFF position.

5. If configuring Wi-Fi on this device, use the following cabling diagram:



- Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. PORT 1 is the dedicated management interface.

If using a wired configuration for this device, use the following diagram:



- Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. PORT 1 is the dedicated management interface.
- Connect one or more of PORT 2, PORT 3, or PORT 4 to the datacenter network/Internet.
 - If connecting PORT 2, use the RJ-45 network cable.
 - For the 10-GbE network interfaces, use the SFP+ copper cables.

NOTE

Using USB ports to connect any external device, including keyboards and monitors, is not supported for Azure Stack Edge devices.

Next steps

In this tutorial, you learned about Azure Stack Edge topics such as how to:

- Unpack the device
- Cable the device

Advance to the next tutorial to learn how to connect, set up, and activate your device.

[Connect and set up Azure Stack Edge](#)

Tutorial: Connect to Azure Stack Edge Mini R

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how you can connect to your Azure Stack Edge Mini R device by using the local web UI.

The connection process can take around 5 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Connect to a physical device

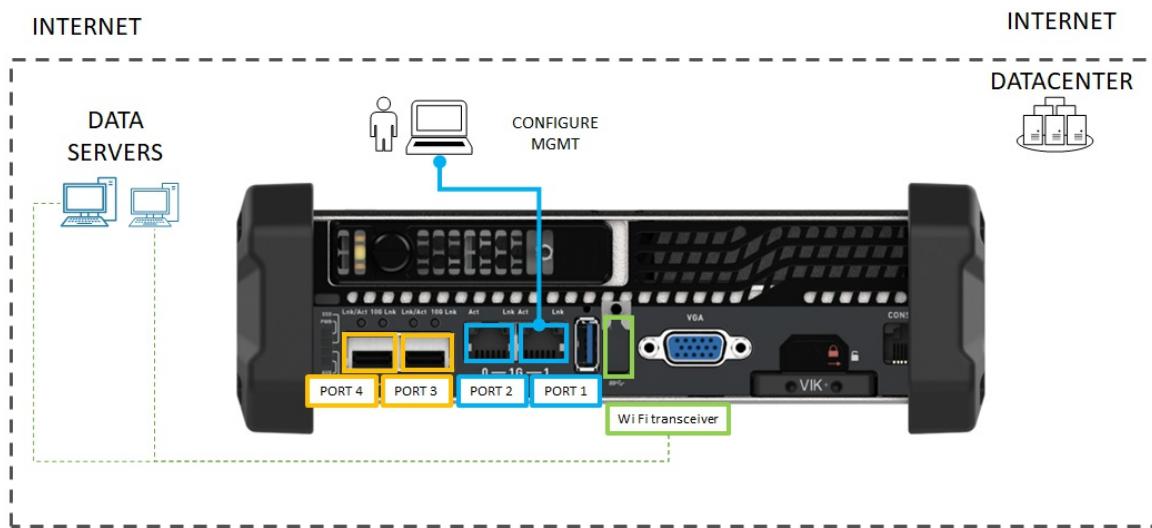
Prerequisites

Before you configure and set up your Azure Stack Edge device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge](#).
- You've run the Azure Stack Network Readiness Checker tool to verify that your network meets Azure Stack Edge requirements. For instructions, see [Check network readiness for Azure Stack Edge devices](#).

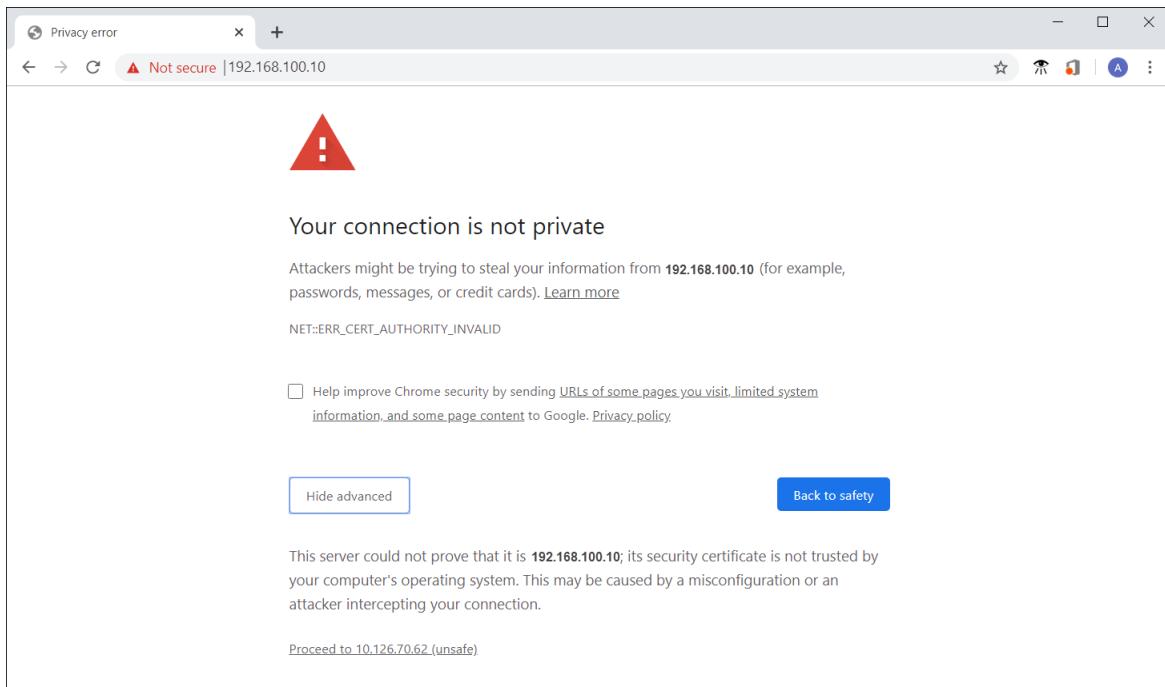
Connect to the local web UI setup

1. Configure the Ethernet adapter on your computer to connect to the Azure Stack Edge Pro device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
2. Connect the computer to PORT 1 on your device. If connecting the computer to the device directly (without a switch), use an Ethernet crossover cable or a USB Ethernet adapter. Use the following illustration to identify PORT 1 on your device.

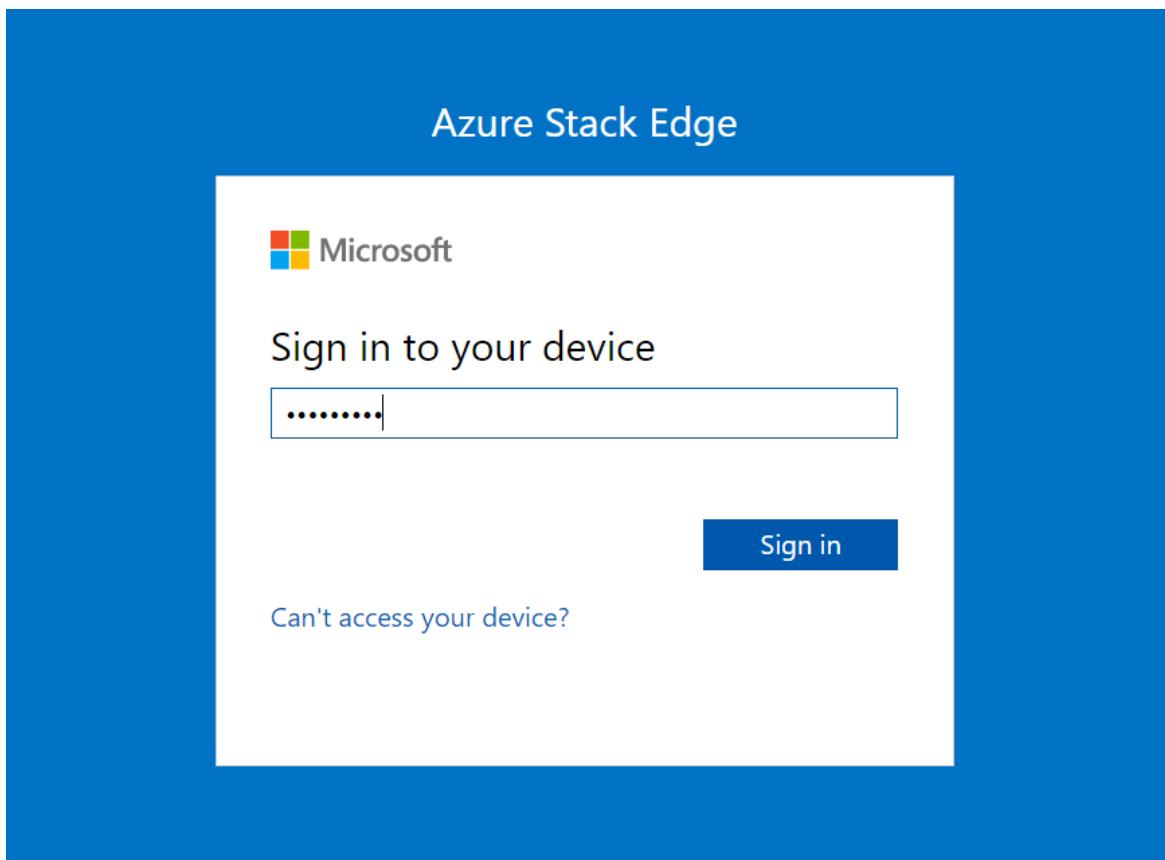


1. Open a browser window and access the local web UI of the device at <https://192.168.100.10>. This action may take a few minutes after you've turned on the device.

You see an error or a warning indicating that there is a problem with the website's security certificate.



2. Select **Continue to this webpage**. These steps might vary depending on the browser you're using.
3. Sign in to the web UI of your device. The default password is *Password1*.



4. At the prompt, change the device administrator password.
The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters.
- You're now at the **Overview** page of your device. The next step is to configure the network settings for your device.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Connect to a physical device

To learn how to configure network settings on your device, see:

[Configure network](#)

Tutorial: Configure network for Azure Stack Edge Mini R

9/21/2022 • 6 minutes to read • [Edit Online](#)

This tutorial describes how to configure network for your Azure Stack Edge Mini R device with an onboard GPU by using the local web UI.

The connection process can take around 20 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure network
- Enable compute network
- Configure web proxy

Prerequisites

Before you configure and set up your Azure Stack Edge Mini R device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Mini R](#).
- You've connected to the local web UI of the device as detailed in [Connect to Azure Stack Edge Mini R](#)

Configure network

Your **Get started** page displays the various settings that are required to configure and register the physical device with the Azure Stack Edge service.

Follow these steps to configure the network for your device.

1. In the local web UI of your device, go to the **Get started** page.
2. If a zero day update is needed, you can do that here by configuring a data port with a wired connection. For more instructions on how to set up a wired connection for this device, see [Cable your device](#). After the update is over, you can remove the wired connection.
3. Create certificates for Wi-Fi and signing chain. Both the signing chain and the Wi-Fi certificates must be DER format with a *.cer* file extension. For instructions, see [Create certificates](#). This step is optional if you're using a Wi-Fi profile instead of certificates for authentication.

NOTE

If you're using password-based authentication on your personal Wi-Fi network, you can skip the certificate steps. Just configure the Wi-Fi port and then upload your Wi-Fi profile.

To find out about Wi-Fi profiles for a WPA2 - Personal network and learn how to export your Wi-Fi profile, see [Use Wi-Fi profiles](#).

4. Add the certificates to your device:

- a. In the local web UI, go to **Get started**. On the **Security** tile, select **Certificates** and then select **Configure**.

Get started with standalone device setup
DVM-TMA-00095

1 Network

Network	:	Configured
Compute network	:	Not configured
Web proxy	:	Not configured

2 Device setup

Device	:	⚠ Needs setup
Update	:	Configured with defaults
Time	:	Configured with defaults

3 Security

Certificates	:	Configured with defaults
VPN	:	Configure
Encryption at rest	:	Configure

4 Activation

Use the activation key from the Azure portal to activate your device.

Activate

b. Select + Add certificate.

Certificates
DVM-TMA-00095

+ Add certificate

To communicate over a secure channel, bring your own signed certificates. You can also download and use the self-signed certificates generated by the device.

Name	Status	Expiration date	Thumbprint
Node (VM-TMA-00095)	Valid	10/19/2022	45DCCA97AC6C4AC08AD9A8322AEC73A54486DBE
Azure Resource Manager	Valid	10/19/2022	ACFC56FE1CF930C225BADCCB91CC91D7EE0AOA7
Blob storage	Valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
Local web UI	Valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
IoT device root CA	⚠ Not present	-	-
IoT device CA	⚠ Not present	-	-
IoT device Key	⚠ Not present	-	-
Edge container registry certificate	⚠ Not present	-	-
Edge container registry key	⚠ Not present	-	-
Vpn certificate	⚠ Not present	-	-
Wifi certificate	⚠ Not present	-	-

< Back to Get started | Next: VPN >

c. Upload the signing chain and select Apply.

Add certificate

Choose the certificate type to upload.

Certificate type

Signing Chain

Use the certificate signing chain, including the root CA and the intermediate signers, in .cer or .p7b format for all the certificates that you have provided.

Signing Chain

myaseminir_root.c ✓

Validate & add

d. Repeat the procedure with the Wi-Fi certificate.

Add certificate

Choose the certificate type to upload.

Certificate type

Wifi certificate

Bring in your device certificate for Wifi connections.

Wifi certificate Password

myaseminir_wdshc ✓ |

Validate & add

e. The new certificates should be displayed on the Certificates page.

Azure Stack Edge Mini R			
Overview	Certificates		
CONFIGURATION	DVM-TMA-00095		
<input type="button" value="Get started"/>	<input type="button" value="Add certificate"/>		
To communicate over a secure channel, bring your own signed certificates. You can also download and use the self-signed certificates generated by the device.			
Name	Status	Expiration date	Thumbprint
Signing Chain	✓ Valid	10/20/2021	4F263851EE6B6288E583F80A87CCC96EDF79225B
Node (VM-TMA-00095)	✓ Valid	10/19/2022	45DCCA97AC6C4AC08AD9A8322AE73A54486DBE
Azure Resource Manager	✓ Valid	10/19/2022	ACFC56FE1CF930C225BADCCB91CC91D7EE0A0A7
Blob storage	✓ Valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
Local web UI	✓ Valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
IoT device root CA	⚠ Not present	-	-
IoT device CA	⚠ Not present	-	-
IoT device Key	⚠ Not present	-	-
Edge container registry certificate	⚠ Not present	-	-
Edge container registry key	⚠ Not present	-	-
Vpn certificate	⚠ Not present	-	-
Wifi certificate	✓ Valid	10/20/2021	C0D77E2B72D0081B499FB1C5643ED06D26100F2F

- f. Go back to **Get started**.
5. Configure the Wi-Fi port. On the **Network** tile, select **Configure**.

On your physical device, there are five network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3 and PORT 4 are all 10-Gbps network interfaces. The fifth port is the Wi-Fi port.

The screenshot shows the Azure Stack Edge Mini R configuration interface. The left sidebar has sections for Overview, Configuration (with Network selected), Compute, Web proxy, Device, Update server, Time, Certificates, VPN, and Cloud details. The Maintenance section includes Power, Hardware health, Software update, Password change, and Device reset. The main area is titled 'Network' and shows the device ID 'DVM-TMA-00095'. A message at the top says 'Link on the following port(s) is not active: Port WiFi.' Below this is a table for 'Network interfaces' with columns for Name, IP addresses, Subnet mask, Gateway, and MAC addresses. It lists Port 1 (IP 192.168.100.10, MAC 00-13-F2-18-05-E1), Port 2 (IP 192.168.100.10, MAC 00-13-F2-18-05-E0), Port 3 (IP 192.168.100.10, MAC 00-13-95-39-2B-0E), Port 4 (IP 192.168.100.10, MAC 00-13-95-39-2B-0D), and Port WiFi (IP -, MAC 3C-37-86-8B-4F-9A). The row for Port WiFi is highlighted with a red box. Below this is a section for 'Wifi profiles settings' with a table for connection status, signal strength, and download. Buttons for 'Add Wifi profile', 'Connect Wifi Profile', and 'Delete Wifi profile' are available. At the bottom are links for '< Back to Get started' and 'Next: Compute >'.

Select the Wi-Fi port and configure the port settings.

IMPORTANT

We strongly recommend that you configure a static IP address for the Wi-Fi port.

Network settings (Port WiFi)

* IP settings

DHCP Static **Static**

* Subnet mask
255.255.252.0 ✓

Gateway
10.128.44.1 ✓

Primary DNS
10.50.50.50 ✓

Secondary DNS
10.50.10.50 ✓

Serial number	IP address	MAC address
VM-TMA-00095	10.128.44.249 ✓	3C-37-86-8B-4F-9A

Apply

The Network page updates after you apply the Wi-Fi port settings.

Azure Stack Edge Mini R

Network DVM-TMA-00095

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

WiFi profiles settings

For the WiFi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
TEA_Cisco_AP	Disconnected	-	Download profile

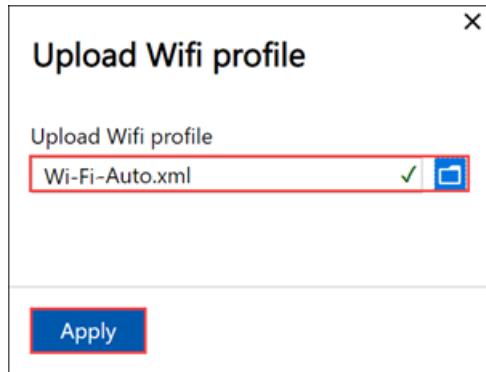
Add WiFi profile Connect WiFi Profile Delete WiFi profile

< Back to Get started Next: Compute >

- Select Add WiFi profile and upload your WiFi profile.

The screenshot shows the Azure Stack Edge Mini R configuration interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Compute, Web proxy, Device, Update server, Time, Certificates, VPN, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and a bottom section for Back to Get started and Next: Compute >. The main area is titled 'Network' and shows 'DVM-TMA-00095'. A message at the top says 'Link on the following port(s) is not active: Port WiFi.' Below this is a table for 'Network interfaces' with columns Name, IP addresses, Subnet mask, Gateway, and MAC addresses. The table lists five entries: Port 1 (IP 192.168.100.10, Mask 255.255.255.0, Gateway -, MAC 00-13-F2-18-05-E1), Port 2 (IP 192.168.100.11, Mask 255.255.255.0, Gateway -, MAC 00-13-F2-18-05-E0), Port 3 (IP 192.168.100.12, Mask 255.255.255.0, Gateway -, MAC 00-13-95-39-2B-0E), Port 4 (IP 192.168.100.13, Mask 255.255.255.0, Gateway -, MAC 00-13-95-39-2B-0D), and Port WiFi (IP 10.128.44.249, Mask 255.255.252.0, Gateway 10.128.44.1, MAC 3C-37-86-8B-4F-9A). Below the table is a section for 'Wifi profiles settings' with a table for connection status, signal strength, and download. Buttons for Add Wifi profile, Connect Wifi Profile, and Delete Wifi profile are shown. At the bottom are links for < Back to Get started and Next: Compute >.

A wireless network profile contains the SSID (network name), password key, and security information to be able to connect to a wireless network. You can get the Wi-Fi profile for your environment from your network administrator.



After the profile is added, the list of Wi-Fi profiles updates to reflect the new profile. The profile should show the **Connection status** as **Disconnected**.

Azure Stack Edge Mini R

Network DVM-TMA-00095

CONFIGURATION

- Get started
- Network**
- Compute
- Web proxy
- Device
- Update server
- Time
- Certificates
- VPN
- Cloud details

MAINTENANCE

- Power
- Hardware health
- Software update
- Password change
- Device reset

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Wifi profiles settings

For the Wifi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
Aruba	Disconnected	-	Download profile

[Add Wifi profile](#) [Connect Wifi Profile](#) [Delete Wifi profile](#)

[< Back to Get started](#) [Next: Compute >](#)

7. After the wireless network profile is successfully loaded, connect to this profile. Select **Connect to Wi-Fi profile**.

Azure Stack Edge Mini R

Network DVM-TMA-00095

CONFIGURATION

- Get started
- Network**
- Compute
- Web proxy
- Device
- Update server
- Time
- Certificates
- VPN
- Cloud details

MAINTENANCE

- Power
- Hardware health
- Software update
- Password change
- Device reset

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Wifi profiles settings

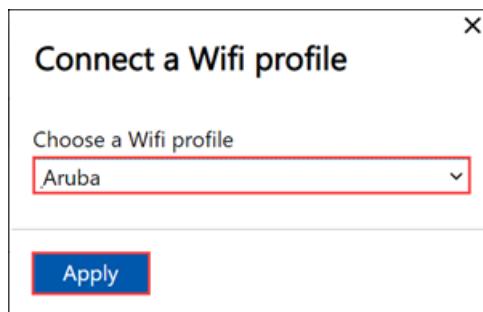
For the Wifi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
Aruba	Disconnected	-	Download profile

[Add Wifi profile](#) [Connect Wifi Profile](#) [Delete Wifi profile](#)

[< Back to Get started](#) [Next: Compute >](#)

8. Select the Wi-Fi profile that you added in the previous step, and select **Apply**.



The Connection status should update to Connected. The signal strength updates to indicate the quality of the signal.

Name	Connection Status	Signal strength	Download
Aruba	Connected	Moderate	Download profile

NOTE

To transfer large amounts of data, we recommend that you use a wired connection instead of the wireless network.

9. Disconnect PORT 1 on the device from the laptop.

10. As you configure the network settings, keep in mind:

- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.
- If DHCP isn't enabled, you can assign static IPs if needed.
- You can configure your network interface as IPv4.
- Network Interface Card (NIC) Teaming or link aggregation is not supported with Azure Stack Edge.
- Serial number for any port corresponds to the node serial number. For a K-series device, only one serial number is displayed.

NOTE

- We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has registered with the service, and then change. You can then view the IPs of all the adapters in the **Device properties** in the Azure portal for your service.
- If you need to connect to your device from an outside network, see [Enable device access from outside network](#) for additional network settings.

After you have configured and applied the network settings, select **Next: Compute** to configure compute network.

Enable compute network

Follow these steps to enable compute and configure compute network.

1. In the **Compute** page, select a network interface that you want to enable for compute.

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.128.24.0	No
Port 3	5.5.0.0	No
Port 4	5.5.0.0	No
Port WiFi	10.128.44.0	No

2. In the **Network settings** dialog, select **Enable**. When you enable compute, a virtual switch is created on your device on that network interface. The virtual switch is used for the compute infrastructure on the device.
3. Assign **Kubernetes node IPs**. These static IP addresses are for the compute VM.

For an n -node device, a contiguous range of a minimum of $n+1$ IPv4 addresses (or more) are provided for the compute VM using the start and end IP addresses. Given Azure Stack Edge is a 1-node device, a minimum of 2 contiguous IPv4 addresses are provided.

IMPORTANT

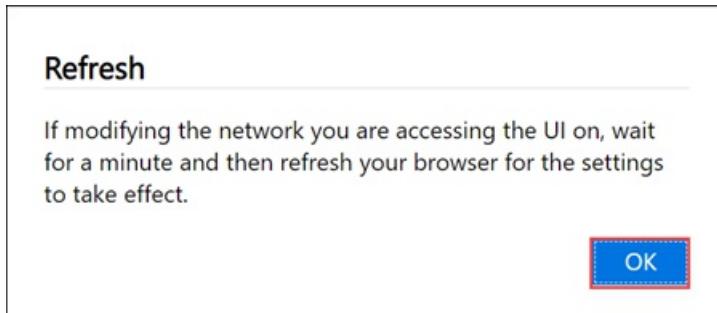
Kubernetes on Azure Stack Edge uses 172.27.0.0/16 subnet for pod and 172.28.0.0/16 subnet for service. Make sure that these are not in use in your network. If these subnets are already in use in your network, you can change these subnets by running the `Set-HcsKubeClusterNetworkInfo` cmdlet from the PowerShell interface of the device. For more information, see [Change Kubernetes pod and service subnets](#).

4. Assign **Kubernetes external service IPs**. These are also the load-balancing IP addresses. These contiguous IP addresses are for services that you want to expose outside the Kubernetes cluster and you specify the static IP range depending on the number of services exposed.

IMPORTANT

We strongly recommend that you specify a minimum of 1 IP address for Azure Stack Edge Mini R Hub service to access compute modules. You can then optionally specify additional IP addresses for other services/IoT Edge modules (1 per service/module) that need to be accessed from outside the cluster. The service IP addresses can be updated later.

5. Select **Apply**.



6. The configuration takes a couple minutes to apply and you may need to refresh the browser. You can see that the specified port is enabled for compute.

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.128.24.0	No
Port 3	5.5.0.0	No
Port 4	5.5.0.0	No
Port WiFi	10.128.44.0	Yes

Select **Next: Web proxy** to configure web proxy.

Configure web proxy

This is an optional configuration.

IMPORTANT

Proxy-auto config (PAC) files are not supported. A PAC file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. Proxies that try to intercept and read all the traffic (then re-sign everything with their own certification) aren't compatible since the proxy's certificate is not trusted. Typically transparent proxies work well with Azure Stack Edge Mini R. Non-transparent web proxies are not supported.

1. On the **Web proxy settings** page, take the following steps:

- a. In the **Web proxy URL** box, enter the URL in this format:

`http://host-IP address or FQDN:Port number`. HTTPS URLs are not supported.

b. To validate and apply the configured web proxy settings, select **Apply**.

The screenshot shows the Azure Stack Edge Mini R configuration interface. The left sidebar has a 'CONFIGURATION' section with options: Get started, Network, Compute, Web proxy (which is selected and highlighted in blue), Device, Update server, Time, Certificates, and VPN. The main panel title is 'Web proxy' with the identifier 'DVM-TMA-00095'. It contains a descriptive text about configuring optional web proxy settings. Below that is a section for 'Web proxy' status with 'Enable' and 'Disable' buttons, where 'Enable' is selected. A 'Web proxy URL' input field contains 'http://10.100.10.10' with a green checkmark icon. At the bottom are three buttons: 'Apply' (highlighted in blue), '< Back to Get started', and 'Next: Device >'.

2. After the settings are applied, select **Next: Device**.

Next steps

In this tutorial, you learned about:

- Prerequisites
- Configure network
- Enable compute network
- Configure web proxy

To learn how to set up your Azure Stack Edge Mini R device, see:

[Configure device settings](#)

Tutorial: Configure the device settings for Azure Stack Edge Mini R

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how you configure device related settings for your Azure Stack Edge Mini R device with an onboard GPU. You can set up your device name, update server, and time server via the local web UI.

The device settings can take around 5-7 minutes to complete.

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

Prerequisites

Before you configure device related settings on your Azure Stack Edge Mini R device with GPU, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Mini R](#).
 - You've configured network and enabled and configured compute network on your device as detailed in [Tutorial: Configure network for Azure Stack Edge Mini R with GPU](#).

Configure device settings

Follow these steps to configure device related settings:

1. On the **Device** page, take the following steps:
 - a. Enter a friendly name for your device. The friendly name must contain from 1 to 13 characters and can have letter, numbers, and hyphens.
 - b. Provide a **DNS domain** for your device. This domain is used to set up the device as a file server.
 - c. To validate and apply the configured device settings, select **Apply**.

The screenshot shows the Azure Stack Edge Mini R configuration interface. On the left, there's a sidebar with various configuration options like Get started, Network, Compute, Web proxy, Device (which is selected and highlighted with a red box), Update server, Time, Certificates, VPN, and Cloud details. Under MAINTENANCE, there are Power, Hardware health, Software update, Password change, and Device reset. Under TROUBLESHOOTING, there are Diagnostic tests and Support. The main right panel shows the 'Device' configuration. It has a warning message: 'To complete this step, you will need to apply the desired device name and DNS domain.' Below it, there's a 'Device name' section where the user can assign a friendly name and DNS domain. The 'Name' field contains 'myaseminir' and the 'DNS domain' field contains 'wdshcssd.com', both of which are highlighted with a red border. There's also a 'Device endpoints' table listing various services and their endpoints. At the bottom, there are 'Apply', '< Back to Get started', and 'Next: Update server >' buttons.

If you have changed the device name and the DNS domain, the self-signed certificates that existed on the device will not work.

Warning

If you change the device name or DNS domain, you must upload new certificates for the device to work properly.

Apply

Cancel

You need to choose one of the following options when you configure certificates:

- Generate and download the device certificates.
 - Bring your own certificates for the device including the signing chain.
- d. When the device name and the DNS domain are changed, the SMB endpoint is created.

Service	Certificate Required	Endpoint
SMB server	No	\myaseminir.wdshcsso.com\[Share name]
NFS server	No	\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.dvm-tma-00095.microsoftdatabox.com
Azure Resource Manager	Yes	https://management.dvm-tma-00095.microsoftdatabox.com
Blob Storage	Yes	https://[Account name].blob.dvm-tma-00095.microsoftdatabox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	No	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.

- e. After the settings are applied, select **Next: Update server**.

Configure update

- On the **Update** page, you can now configure the location from where to download the updates for your device.
- You can get the updates directly from the **Microsoft Update server**.

You can also choose to deploy updates from the **Windows Server Update services (WSUS)**. Provide the path to the WSUS server.

Azure Stack Edge Mini R

CONFIGURATION

- Get started
- Network
- Compute
- Web proxy
- Device
- Update server**
- Time
- Certificates

Update server

Configure update server for your device.

* Select update server type
Windows Server Update Services

* Server URI
http://FL319.guest.corp.microsoft.com:8530 ✓

Apply < Back to Get started Next: Time >

NOTE

If a separate Windows Update server is configured and if you choose to connect over *https* (instead of *http*), then signing chain certificates required to connect to the update server are needed. For information on how to create and upload certificates, go to [Manage certificates](#). For working in a disconnected mode such as your Azure Stack Edge device tiering to Modular Data Center, enable WSUS option. During activation, the device scans for updates and if the server is not set up, then the activation will fail.

2. Select **Apply**.
3. After the update server is configured, select **Next: Time**.

Configure time

Follow these steps to configure time settings on your device.

IMPORTANT

Though the time settings are optional, we strongly recommend that you configure a primary NTP and a secondary NTP server on the local network for your device. If local server is not available, public NTP servers can be configured.

NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

1. On the **Time** page, you can select the time zone, and the primary and secondary NTP servers for your device.
 - a. In the **Time zone** drop-down list, select the time zone that corresponds to the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
 - b. In the **Primary NTP server** box, enter the primary server for your device or accept the default value of time.windows.com.
Ensure that your network allows NTP traffic to pass from your datacenter to the internet.
 - c. Optionally, in the **Secondary NTP server** box, enter a secondary server for your device.
 - d. To validate and apply the configured time settings, select **Apply**.

The screenshot shows the Azure Stack Edge Mini R configuration interface. On the left, a sidebar lists various configuration options under 'CONFIGURATION' and 'MAINTENANCE'. The 'Time' option is highlighted with a red box. The main panel displays the 'Time' settings page, titled 'Time' with the user name 'myaseminir'. It includes a brief description of time synchronization settings, the current device time ('10/21/2020 2:19:27 PM'), and three configuration fields: 'Time zone' (set to '(UTC-08:00) Pacific Time (US & Canada)'), 'Primary NTP server' (set to 'time.windows.com'), and 'Secondary NTP server' (set to '10.100.10.20'). At the bottom are 'Apply', '< Back to Get started', and 'Next: Certificates >' buttons.

2. After the settings are applied, select **Next: Certificates**.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure device settings
- Configure update
- Configure time

To learn how to configure certificates for your Azure Stack Edge Mini R device, see:

[Configure certificates](#)

Tutorial: Configure certificates, VPN, encryption for your Azure Stack Edge Mini R

9/21/2022 • 4 minutes to read • [Edit Online](#)

This tutorial describes how you can configure certificates, VPN, and encryption-at-rest for your Azure Stack Edge Mini R device by using the local web UI.

The time taken for this step can vary depending on the specific option you choose and how the certificate flow is established in your environment.

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device
- Configure VPN
- Configure encryption at rest

Prerequisites

Before you configure and set up your Azure Stack Edge Mini R device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Mini R](#).
- If you plan to bring your own certificates:
 - You should have your certificates ready in the appropriate format including the signing chain certificate. For details on certificate, go to [Manage certificates](#)
 - If your device is deployed in Azure Government or Azure Government Secret or Azure Government top secret cloud and not deployed in Azure public cloud, a signing chain certificate is required before you can activate your device. For details on certificate, go to [Manage certificates](#).

Configure certificates for device

1. In the **Certificates** page, you will configure your certificates. Depending on whether you changed the device name or the DNS domain in the **Device** page, you can choose one of the following options for your certificates.
 - If you have not changed the default device name or the default DNS domain in the earlier step and do not wish to bring your own certificates, then you can skip this step and proceed to the next step. The device has automatically generated self-signed certificates to begin with.
 - If you changed the device name or DNS domain, you will see that the status of certificates will show as **Not valid**.

Name	Status	Expiration date	Thumbprint
Signing Chain	Valid	10/20/2021	4F263851EE6B6288E583F80A87CCC96EDF79225B
Node (VM-TMA-00095)	Not valid	10/19/2022	45DCCA97AC6C4AC08AD9A8322AE73A54486DBE
Azure Resource Manager	Not valid	10/19/2022	ACFC56FE1CF930C225BADCCB91CC91D7EE0A0A7
Blob storage	Not valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
Local web UI	Not valid	10/19/2022	A5901AF5C04B8182AE7943906EA7EE04E788DE24
IoT device root CA	Not present	-	-
IoT device CA	Not present	-	-
IoT device Key	Not present	-	-
Edge container registry certificate	Not present	-	-
Edge container registry key	Not present	-	-
Vpn certificate	Not present	-	-
Wifi certificate	Valid	10/20/2021	C0D77E2B72D0081B499FB1C5643ED06D26100F2F

Select a certificate to view the details of the status.

The certificate status is **Not valid** because the certificates do not reflect the updated device name and DNS domain (that are used in subject name and subject alternative). To successfully activate your device, you can bring your own signed endpoint certificates and the corresponding signing chains. You first add the signing chain and then upload the endpoint certificates. For more information, go to [Bring your own certificates on your Azure Stack Edge Mini R device](#).

- If you changed the device name or DNS domain, and you do not bring your own certificates, then the **activation will be blocked**.

Bring your own certificates

You already added the signing chain in an earlier step on this device. You can now upload the endpoint certificates, node certificate, local UI certificate and the VPN certificate. Follow these steps to add your own certificates.

1. To upload certificate, on the Certificate page, select **+ Add certificate**.

2. You can upload other certificates. For example, you can upload the Azure Resource Manager and Blob storage endpoint certificates.



Add certificate

Choose the certificate type to upload.

Certificate type

Endpoints

Bring your own signed certificates for endpoints for Blob storage and Azure Resource Manager for the device.

Azure Resource Manager Password

myaseminir_wdshc	✓	
------------------	---	--	-------

Blob storage Password

myaseminir_wdshc	✓	
------------------	---	--	-------

Validate & add

3. You can also upload the local web UI certificate. After you upload this certificate, you will be required to start your browser and clear the cache. You will then need to connect to the device local web UI.



Add certificate

Choose the certificate type to upload.

Certificate type

Local web UI



Use the local web UI certificate to access the website browser via SSL. After the certificate is applied, close and then restart the browser to avoid any SSL cache issues.

Local web UI

Password

myaseminir_wdshc ✓



.....

Validate & add

4. You can also upload the node certificate.



Add certificate

Choose the certificate type to upload.

Certificate type

Node



Use the node certificates to connect to individual device nodes over a secure channel.

VM-TMA-00095

Password

myaseminir_wdshc ✓



.....

Validate & add

- Finally, you can upload the VPN certificate.

Add certificate

Choose the certificate type to upload.

Certificate type

Vpn certificate

Bring in your device certificate for VPN connections.

Vpn certificate	Password
myaseminir_wdshc ✓	••••••••

Validate & add

- At any time, you can select a certificate and view the details to ensure that these match with the certificate that you uploaded.

Azure Stack Edge Mini R

Name	Status	Expiration date
Signing Chain	Valid	10/21/2021
Node (VM-TMA-00095)	Valid	10/21/2021
Azure Resource Manager	Valid	10/21/2021
Blob storage	Valid	10/21/2021
Local web UI	Valid	10/21/2021
IoT device root CA	Not present	-
IoT device CA	Not present	-
IoT device Key	Not present	-
Edge container registry certificate	Not present	-
Edge container registry key	Not present	-
Vpn certificate	Valid	10/21/2021
Wifi certificate	Valid	10/20/2021

< Back to Get started Next: VPN >

The certificate page should update to reflect the newly added certificates.

Name	Status	Expiration date	Thumbprint
Signing Chain	Valid	10/21/2021	BBA4B599CBE0CAEFFE9DCCC9AFA395F030E60B94
Node (VM-TMA-00095)	Valid	10/21/2021	427D008A5CBF1EFA2A39E44AFA4A8BC5ABE9BD67
Azure Resource Manager	Valid	10/21/2021	427D008A5CBF1EFA2A39E44AFA4A8BC5ABE9BD67
Blob storage	Valid	10/21/2021	427D008A5CBF1EFA2A39E44AFA4A8BC5ABE9BD67
Local web UI	Valid	10/21/2021	427D008A5CBF1EFA2A39E44AFA4A8BC5ABE9BD67
IoT device root CA	Not present	-	-
IoT device CA	Not present	-	-
IoT device Key	Not present	-	-
Edge container registry certificate	Not present	-	-
Edge container registry key	Not present	-	-
Vpn certificate	Valid	10/21/2021	427D008A5CBF1EFA2A39E44AFA4A8BC5ABE9BD67
Wifi certificate	Valid	10/20/2021	C0D77E2B72D0081B499FB1C5643ED06D26100F2F

NOTE

Except for Azure public cloud, signing chain certificates are needed to be brought in before activation for all cloud configurations (Azure Government or Azure Stack Hub).

Configure VPN

- On the **Security** tile, select **Configure** for VPN.

To configure VPN, you'll first need to ensure that you have all the necessary configuration done in Azure. For details, see [Configure VPN via PowerShell for your Azure Stack Edge Mini R device](#). Once this is complete, you can do the configuration in the local UI.

- On the VPN page, select **Configure**.

- In the **Configure VPN** blade:

- Provide the phone book as input.
- Provide Azure Data Center IP range JSON file as input. Download this file from:
<https://www.microsoft.com/download/details.aspx?id=56519>.
- Select **eastus** as the region.

d. Select Apply.

Configure VPN

* VPN settings

* Upload phone book file (.pbk)

myaseminir.pbk

* Upload Service Tags file (.json)

ServiceTags_Public_20201019.json

Region

eastus

If the phone book file (.pbk) and the public IP list config file (.json) are already uploaded, uploading those again will override the previous copies.

c. Configure IP address ranges to be accessed using VPN only.

- Under **IP address ranges to be accessed using VPN only**, select **Configure**.
- Enter the VNET IPv4 range that you had chosen for your Azure Virtual Network.
- Select **Apply**.



IP address ranges to be accessed using VPN only

Specify a range of IP addresses to be included for your VPN connection.

IPv4 range

Example: 10.10.10.10/24

Add

10.10.10.10/24

Delete

Apply

Your device is now ready to be encrypted. Configure encryption at rest.

Enable encryption

1. On the **Security** tile, select **Configure** for encryption-at-rest. This is a required setting and until this is successfully configured, you can't activate the device.

The screenshot shows the Azure Stack Edge Mini R configuration interface. The left sidebar has sections for Overview, Configuration (with Get started highlighted), Network, Compute, Web proxy, Device, Update server, Time, Certificates, VPN, and Cloud details. The Maintenance section includes Power, Hardware health, Software update, Password change, and Device reset. The main area displays four steps: 1. Network (Network: Configured, Compute network: Configured, Web proxy: Not configured). 2. Device setup (Device: Configured, Update: Configured with defaults, Time: Configured with defaults). 3. Security (Certificates: Configured, VPN: Configured, Encryption at rest: Configure, highlighted with a red border). 4. Activation (Instructions to use an activation key from the Azure portal). A blue 'Activate' button is located at the bottom right of the activation section.

At the factory, once the devices are imaged, the volume level BitLocker encryption is enabled. After you receive the device, you need to configure the encryption-at-rest. The storage pool and volumes are recreated and you can provide BitLocker keys to enable encryption-at-rest and thus create a second layer of encryption for your data-at-rest.

2. In the **Encryption-at-rest** pane, enter a 32 character long (AES-256 bit) Base-64 encoded key. This is a one-time configuration and this key is used to protect the actual encryption key.

Encryption at rest

You can bring your own encryption at rest key or generate one here.

* Select an option

Bring your own key

* To provide your own key, enter a Base-64 encoded AES-256 bit encryption key.

.....

* Enter the encryption key again.

.....

i This key is saved in the key file on the Cloud details page after the device is activated.

Apply

You can choose to automatically generate this key as well.



Encryption at rest

You can bring your own encryption at rest key or generate one here.

* Select an option

Use system generated key ▾

System generated encryption key

.....



This key is saved in the key file on the Cloud details page after the device is activated.

Apply

3. Select **Apply**. This operation takes several minutes and the status of operation is displayed on the **Security** tile.



Encryption at rest

You can bring your own encryption at rest key or generate one here.

* Select an option

Use system generated key ▾

System generated encryption key

.....



This key is saved in the key file on the Cloud details page after the device is activated.

Apply

4. After the status shows as **Completed**, go back to **Get started**.

Your device is now ready to be activated.

Next steps

In this tutorial, you learn about:

- Prerequisites
- Configure certificates for the physical device
- Configure VPN
- Configure encryption at rest

To learn how to activate your Azure Stack Edge Mini R device, see:

[Activate Azure Stack Edge Mini R device](#)

Tutorial: Activate Azure Stack Edge Mini R

9/21/2022 • 2 minutes to read • [Edit Online](#)

This tutorial describes how you can activate your Azure Stack Edge Mini R device by using the local web UI.

The activation process can take around 15 minutes to complete.

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

Prerequisites

Before you configure and set up your Azure Stack Edge Mini R device, make sure that:

- For your physical device:
 - You've installed the physical device as detailed in [Install Azure Stack Edge Mini R](#).
 - You've configured the network and compute network settings as detailed in [Configure network, compute network, web proxy](#)
 - You have uploaded your own certificates on your device if you changed the device name or the DNS domain via the **Device** page. These steps are detailed in [Configure certificates, VPN, and encryption-at-rest](#). If you haven't done this step, activation will be blocked.
 - You have configured the encryption-at-rest for your device. If you haven't done this step, you will see an error during the device activation and the activation will be blocked. For more information, go to [Configure certificates, VPN, and encryption-at-rest](#).
- You have the activation key from the Azure Stack Edge service that you created to manage the Azure Stack Edge Mini R device. For more information, go to [Prepare to deploy Azure Stack Edge Mini R](#).

Activate the device

1. In the local web UI of the device, go to **Get started** page.
2. On the **Activation** tile, select **Activate**.

The screenshot shows the Azure Stack Edge Mini R configuration interface. On the left, a sidebar lists various configuration options under 'CONFIGURATION' and 'MAINTENANCE'. The 'Get started' option is selected. The main area is titled 'Get started with standalone device setup' and shows four numbered steps:

- 1 Network**:

Network	:	Configured
Compute network	:	Configured
Web proxy	:	Not configured
- 2 Device setup**:

Device	:	Configured
Update	:	Configured with defaults
Time	:	Configured with defaults
- 3 Security**:

Certificates	:	Configured
VPN	:	Configured
Encryption at rest	:	Completed
Encryption at rest key rotation	:	Rotate keys
- 4 Activation**:

Use the activation key from the Azure portal to activate your device.

Activate

3. In the **Activate** pane:

- Enter the **Activation key** that you got in [Get the activation key for Azure Stack Edge Pro R](#).
- You can enable proactive log collection to let Microsoft collect logs based on the health status of the device. The logs collected this way are uploaded to an Azure Storage account.
- Select **Apply**.



Activate

Activate the device with Azure service. Learn how to [get the activation key](#). After the device is activated, the system checks for and applies any critical updates.

* Activation key

<Activation key>



Proactive log collection

Based on system health indicators, logs are proactively uploaded to an Azure Storage account to help Microsoft Support troubleshoot issues when they arise. [Learn more](#).

[Enable](#) [Disable](#)

Click the “Enable” button. By enabling this option, you agree to the proactive log collection, as described [here](#). To learn more about Microsoft’s privacy practices, see the [Microsoft Privacy Statement](#).

[Activate](#)

4. First the device is activated. You are then prompted to download the key file.

Device activated

Successfully activated your device. Download the device key file to a secure location. These keys will be needed to facilitate a future system recovery.

[Download and continue](#)

Select **Download and continue** and save the *device-serial-nojson* file in a safe location outside of the device. **This key file contains the recovery keys for the OS disk and data disks on your device.** These keys may be needed to facilitate a future system recovery.

Here are the contents of the *json* file:

```
{  
  "Id": "<Device ID>",  
  "DataVolumeBitLockerExternalKeys": {  
    "hcsinternal": "<BitLocker key for data disk>",  
    "hcsdata": "<BitLocker key for data disk>"  
  },  
  "SystemVolumeBitLockerRecoveryKey": "<BitLocker key for system volume>",  
  "SEDEncryptionExternalKey": "xZM/vC7GxjqHZ3VMo7xSs/wH9rRsF/PNM+mOsZ+GaL0=",  
  "ServiceEncryptionKey": "<Azure service encryption key>"  
}
```

The following table explains the various keys:

FIELD	DESCRIPTION
<code>Id</code>	This is the ID for the device.
<code>DataVolumeBitLockerExternalKeys</code>	These are the BitLocker keys for the data disks and are used to recover the local data on your device.
<code>SystemVolumeBitLockerRecoveryKey</code>	This is the BitLocker key for the system volume. This key helps with the recovery of the system configuration and system data for your device.
<code>SEDEncryptionExternalKey</code>	This user provided or system generated key is used to protect the self-encrypting data drives that have a built in encryption.
<code>ServiceEncryptionKey</code>	This key protects the data flowing through the Azure service. This key ensures that a compromise of the Azure service will not result in a compromise of stored information.

5. Go to the **Overview** page. The device state should show as **Activated**.

The screenshot shows the Azure Stack Edge Mini R Overview page. On the left, a navigation sidebar lists sections like Configuration, Maintenance, and Device. The main area displays two boxes: 'System' and 'Device'. The 'System' box shows 'Health status' as Healthy, 'Software version' as 2.2.1388.2229, 'State' as Activated (which is highlighted with a red box), and 'Azure portal' as myaseminir. The 'Device' box shows 'Device serial number' as VM-TMA-00095, 'Node serial number' as VM-TMA-00095, 'Available capacity' as 743.11 GB, and 'Compute acceleration' as 1 * VPU. Below these is a 'Configuration' box showing 'Network' as Configured, 'Web proxy' as Not enabled, and 'Cloud connectivity' as Fully connected.

The device activation is complete. You can now add shares on your device.

If you encounter any issues during activation, go to [Troubleshoot activation and Azure Key Vault errors](#).

Next steps

In this tutorial, you learned about:

- Prerequisites
- Activate the physical device

To learn how to transfer data with your Azure Stack Edge Mini R device, see:

[Transfer data with Azure Stack Edge Mini R](#)

Tutorial: Configure compute on Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role and create a Kubernetes cluster on your Azure Stack Edge Pro GPU device.

This procedure can take around 20 to 30 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Get Kubernetes endpoints

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro device:

- Make sure that you've activated your Azure Stack Edge Pro device as described in [Activate Azure Stack Edge Pro](#).
- Make sure that you've followed the instructions in [Enable compute network](#) and:
 - Enabled a network interface for compute.
 - Assigned Kubernetes node IPs and Kubernetes external service IPs.

NOTE

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are on the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

Configure compute

To configure compute on your Azure Stack Edge Pro, you'll create an IoT Hub resource via the Azure portal.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**, and select **IoT Edge**.

The screenshot shows the Azure Stack Edge device overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Your device is running fine!' message. Below it, the 'Deployed edge services' section shows 'No deployed services'. The 'Edge services' section contains three cards: 'Virtual machines' (with a 'New' button), 'IoT Edge' (which is selected and has a red box around its card), and 'Cloud storage gateway'. Each card has a 'How to get started?' link.

2. In **Enable IoT Edge service**, select **Add**.

The screenshot shows the IoT Edge | Overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Enable IoT Edge service' section. This section contains instructions to enable the service by setting up the network and configuring the Azure subscription, followed by a large 'Add' button. Below this is a 'Steps to deploy IoT Edge services' section. At the bottom, there's a 'What's next' section with a link to 'Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services'.

3. On the **Configure Edge compute** blade, input the following information:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.

FIELD	VALUE
IoT Hub	<p>Choose from New or Existing. By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.</p>
Name	Accept the default name or enter a name for your IoT Hub resource.

Home > myasetest > IoT Edge >

Create IoT Edge service ⊕

Azure Stack Edge

[Basics](#) [Review + Create](#)

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription * <small>(i)</small>	<input type="text" value="Edge Gateway Test"/>
Resource group * <small>(i)</small>	<input type="text" value="myaserg"/>
IoT Hub * <small>(i)</small>	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing <input type="text" value="myasetest-iothub"/>

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

*IoT Edge device: myasetest-edge
 IoT Gateway device: myasetest-storagegateway*

Only Linux container image types are supported.

[Review + Create](#) [Previous](#) [Next: Review + Create](#)

4. When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

The screenshot shows the IoT Edge | Overview page for an Azure Stack Edge device named 'myasetest'. The top navigation bar includes 'Home > myasetest > IoT Edge | Overview' and standard UI controls like search, add module, add trigger, refresh, and remove. A red box highlights the 'Overview' tab. A message box states 'IoT Edge service is running fine!' with the subtext 'Start processing the data using IoT Edge modules. Learn more'. Below this are sections for 'Modules' (with an 'Add module' button), 'Triggers' (with an 'Add trigger' button), and 'Edge Shares', 'Edge Storage account', and 'Network bandwidth usage' configuration options.

5. To confirm the Edge compute role has been configured, go to **IoT Edge > Properties**.

The screenshot shows the IoT Edge | Properties page for the same device. The 'Properties' tab is highlighted with a red box. The main content area displays device configurations in a table:

IoT Hub	myasetest-iohub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

When the Edge compute role is set up on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

It can take 20-30 minutes to configure compute because, behind the scenes, virtual machines and a Kubernetes cluster are being created.

After you have successfully configured compute in the Azure portal, a Kubernetes cluster and a default user associated with the IoT namespace (a system namespace controlled by Azure Stack Edge) exist.

Get Kubernetes endpoints

To configure a client to access Kubernetes cluster, you'll need the Kubernetes endpoint. Follow these steps to get Kubernetes API endpoint from the local UI of your Azure Stack Edge Pro device.

1. In the local web UI of your device, go to **Device** page.
2. Under the **Device endpoints**, copy the **Kubernetes API endpoint**. This endpoint is a string in the

following format: [https://compute.<device-name>.<DNS-domain>\[Kubernetes-cluster-IP-address\]](https://compute.<device-name>.<DNS-domain>[Kubernetes-cluster-IP-address]).

The screenshot shows the 'Device' configuration page for a device named 'dl115'. The 'Device endpoints' section is highlighted with a red box. It lists various services with their certificate requirements and endpoints. The 'Kubernetes API service' endpoint is highlighted with a blue box: [https://compute.dl115.teatraining1.com \[10.128.45.200\]](https://compute.dl115.teatraining1.com [10.128.45.200]).

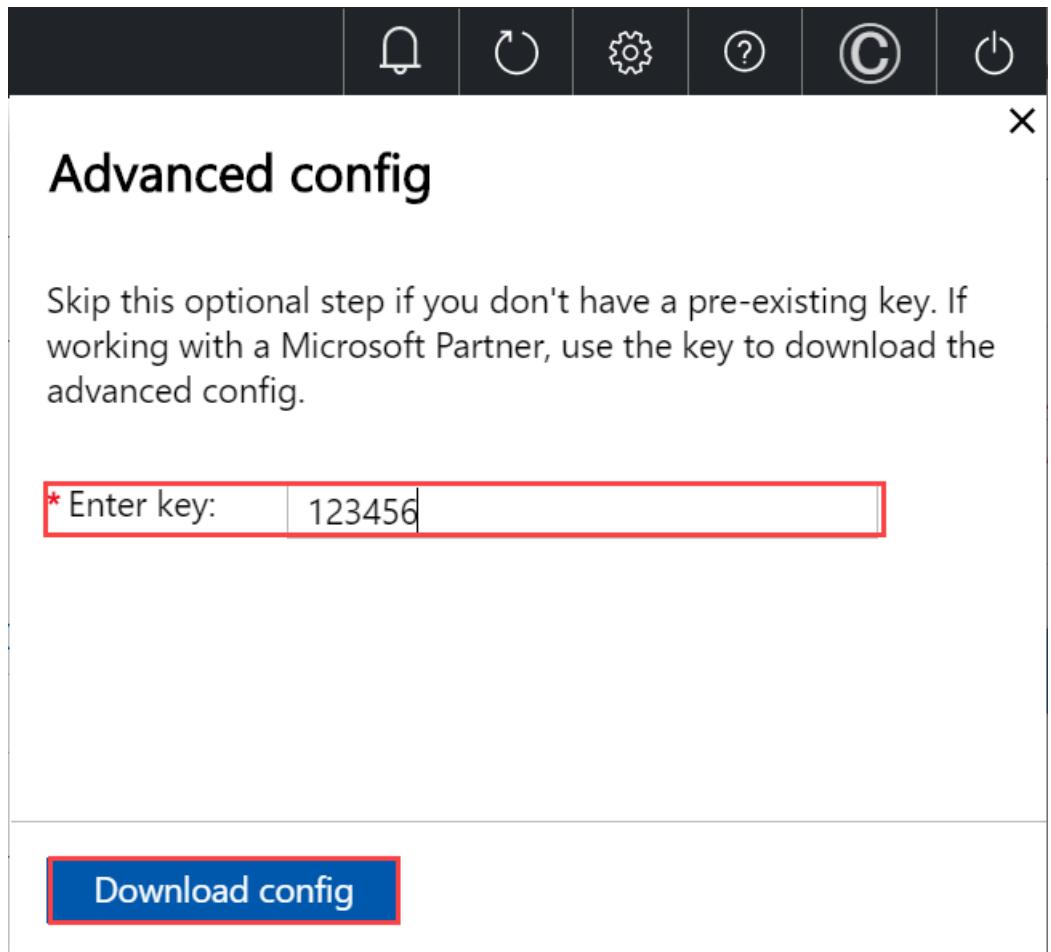
Service	Certificate Required	Endpoint
SMB server	No	\\\dl115.teatraining1.com\Share name]
NFS server	No	\\\[Device IP address]\Share name]
Azure Resource Manager login	Yes	https://login.dl115.teatraining1.com
Azure Resource Manager	Yes	https://management.dl115.teatraining1.com
Blob Storage	Yes	https://[Account name].blob.dl115.teatraining1.com
Kubernetes API service	No	https://compute.dl115.teatraining1.com [10.128.45.200]
Edge IoT hub	Yes	Endpoint not yet created.

3. Save the endpoint string. You'll use this endpoint string later when configuring a client to access the Kubernetes cluster via kubectl.

4. While you are in the local web UI, you can:

- If you've been provided a key from Microsoft (select users may have a key), go to Kubernetes API, select **Advanced config**, and download an advanced configuration file for Kubernetes.

The screenshot shows the 'Device' configuration page for a device named 'myasegpu1'. The 'Device endpoints' section is highlighted with a red box. The 'Kubernetes API' row has a red box around it, and the 'Endpoint' column shows the URL: [https://compute.myasegpu1.wdshcsso.com \[10.128.44.241\]](https://compute.myasegpu1.wdshcsso.com [10.128.44.241]). A blue box highlights the 'Advanced config' link next to the endpoint.



- You can also go to **Kubernetes dashboard** endpoint and download an `aseuser` config file.

The screenshot shows the Azure Stack Edge Device configuration page. The left sidebar lists various configuration options: Overview, Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, and Device (which is selected and highlighted in blue). The main content area shows a 'Device' card for 'myasegpu1'. Under 'Device name', the 'Name' field is set to 'myasegpu1' and the 'DNS domain' field is set to 'wdshcsso.com'. The 'Device endpoints' section contains a table of service endpoints:

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241]
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]

At the bottom, there are buttons for 'Apply', '< Back to Overview', and 'Next: Update server >'.

You can use this config file to sign into the Kubernetes dashboard or debug any issues in your Kubernetes cluster. For more information, see [Access Kubernetes dashboard](#).

Next steps

In this tutorial, you learned how to:

- Configure compute
- Get Kubernetes endpoints

To learn how to administer your Azure Stack Edge Pro device, see:

[Use local web UI to administer an Azure Stack Edge Pro](#)

Configure VPN on your Azure Stack Edge Mini R device via Azure PowerShell

9/21/2022 • 10 minutes to read • [Edit Online](#)

The VPN option provides a second layer of encryption for the data-in-motion over *TLS* from your Azure Stack Edge Mini R or Azure Stack Edge Pro R device to Azure. You can configure VPN on your Azure Stack Edge Mini R device via the Azure portal or via the Azure PowerShell.

This article describes the steps required to configure a Point-to-Site (P2S) VPN on your Azure Stack Edge Mini R device using an Azure PowerShell script to create the configuration in the cloud. The configuration on the Azure Stack Edge device is done via the local UI.

About VPN setup

A P2S VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer or your Azure Stack Edge Mini R device. You start the P2S connection from the client computer or the device. The P2S connection in this case uses IKEv2 VPN, a standards-based IPsec VPN solution.

The typical work flow includes the following steps:

1. Configure prerequisites.
2. Set up necessary resources on Azure.
 - a. Create and configure a virtual network and required subnets.
 - b. Create and configure an Azure VPN gateway (virtual network gateway).
 - c. Set up Azure Firewall and add network and app rules.
 - d. Create Azure Routing Tables and add routes.
 - e. Enable Point-to-site in VPN gateway.
 - a. Add the client address pool.
 - b. Configure tunnel type.
 - c. Configure authentication type.
 - d. Create certificate.
 - e. Upload certificate.
 - f. Download phone book.
3. Set up VPN in the local web UI of the device.
 - a. Provide phone book.
 - b. Provide Service tags (json) file.

The detailed steps are provided in the following sections.

Configure prerequisites

- You should have access to an Azure Stack Edge Mini R device that is installed as per the instructions in [Install your Azure Stack Edge Mini R device](#). This device will be establishing a P2S connection with Azure.
- You should have access to a valid Azure Subscription that is enabled for Azure Stack Edge service in Azure. Use this subscription to create a corresponding resource in Azure to manage your Azure Stack Edge Mini R device.
- You have access to a Windows client that you'll use to access your Azure Stack Edge Mini R device. You'll

use this client to programmatically create the configuration in the cloud.

1. To install the required version of PowerShell on your Windows client, run the following commands:

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser  
Import-Module Az.Accounts
```

2. To connect to your Azure account and subscription, run the following commands:

```
Connect-AzAccount  
Set-AzContext -Subscription "<Your subscription name>"
```

Provide the Azure subscription name you are using with your Azure Stack Edge Mini R device to configure VPN.

3. [Download the script](#) required to create configuration in the cloud. The script will:

- o Create an Azure Virtual network and the following subnets: *GatewaySubnet*, and *AzureFirewallSubnet*.
 - o Create and configure an Azure VPN gateway.
 - o Create and configure an Azure local network gateway.
 - o Create and configure an Azure VPN connection between the Azure VPN gateway and the local network gateway.
 - o Create an Azure Firewall and add network rules, app rules.
 - o Create an Azure Routing table and add routes to it.
4. Create the resource group in the Azure portal under which you want the Azure resources to be created. Go to the list of services in Azure portal, select **Resource group** and then select + Add. Provide the subscription information and the name for your resource group and then select **Create**. If you go to this resource group, it should not have any resources under it at this time.

The screenshot shows the Azure portal interface for the 'mytmarg3' resource group. The 'Overview' tab is selected. The main content area displays a message: 'No resources to display'. Below this, there is a note: 'The resources are currently filtered and not all resources may be displayed, such as hidden resources.' and a link 'Learn more'. The left sidebar contains a navigation menu with several sections: Home > mytmarg3, Overview (selected), Activity log, Access control (IAM), Tags, Events, Settings, Quickstart, Deployments, Policies, Properties, Locks, Export template, Cost Management, Cost analysis, Cost alerts, Budgets, and Advisor recommendations.

5. You will need to have a Base 64 encoded certificate in `.cer` format for your Azure Stack Edge Mini R device. This certificate should be uploaded to your Azure Stack Edge device as `.pfx` with a private key. This certificate also needs to be installed in the trusted root of the store on the client that is trying to establish the P2S connection.

Use the script

First you modify the `parameters-p2s.json` file to input your parameters. Next, you run the script using the modified json file.

Each of these steps is discussed in the following sections.

Download service tags file

You may already have a `ServiceTags.json` file in the folder where you downloaded the script. If not, you can download the service tags file.

Download the service tags from the Azure to your local client and save as a `json` file in the same folder that contains the scripts: <https://www.microsoft.com/download/details.aspx?id=56519>.

This file is uploaded in the local web UI at a later step.

Modify parameters file

The first step would be to modify the `parameters-p2s.json` file and save the changes.

For the Azure resources that you create, you'll provide the following names:

PARAMETER NAME	DESCRIPTION
virtualNetworks_vnet_name	Azure Virtual Network name
azureFirewalls_firewall_name	Azure Firewall name
routeTables_routetable_name	Azure Route table name
publicIPAddresses_VNGW_public_ip_name	Public IP address name for your Virtual network gateway
virtualNetworkGateways_VNGW_name	Azure VPN gateway (virtual network gateway) name
publicIPAddresses_firewall_public_ip_name	Public IP address name for your Azure Firewall
location	This is the region in which you want to create your virtual network. Select the same region as the one associated with your device.
RouteTables_routetable_onprem_name	This is the name of the additional route table to help the firewall route packets back to Azure Stack Edge device. The script creates two additional routes and associates <code>default</code> and <code>GatewaySubnet</code> with this route table.

Provide the following IP addresses and address spaces for the Azure resources that are created including the virtual network and associated subnets (`default`, `firewall`, `GatewaySubnet`).

PARAMETER NAME	DESCRIPTION
VnetIPv4AddressSpace	This is the address space associated with your virtual network. Provide Vnet IP range as private IP range (https://en.wikipedia.org/wiki/Private_network#Private_IPv4_addresses).
DefaultSubnetIPv4AddressSpace	This is the address space associated with the <code>Default</code> subnet for your virtual network.

PARAMETER NAME	DESCRIPTION
FirewallSubnetIPv4AddressSpace	This is the address space associated with the <code>Firewall</code> subnet for your virtual network.
GatewaySubnetIPv4AddressSpace	This is the address space associated with the <code>GatewaySubnet</code> for your virtual network.
GatewaySubnetIPv4bgpPeeringAddress	This is the IP address that is reserved for BGP communication and is based off the address space associated with the <code>GatewaySubnet</code> for your virtual network.
ClientAddressPool	This IP address is used for the address pool in the P2S configuration in Azure portal.
PublicCertData	Public certificate data is used by the VPN Gateway to authenticate P2S clients connecting to it. To get the certificate data, install the root certificate. Make sure the certificate is Base-64 encoded with a .cer extension. Open this certificate and copy the text in the certificate between ==BEGIN CERTIFICATE== and ==END CERTIFICATE== in one continuous line.

Run the script

Follow these steps to use the modified `parameters-p2s.json` and run the script to create Azure resources.

1. Run PowerShell. Switch to the directory where the script is located.
2. Run the script.

```
.\AzDeployVpn.ps1 -Location <Location> -AzureAppRuleFilePath "appRule.json" -AzureIPRangesFilePath "<Service tag json file>" -ResourceGroupName "<Resource group name>" -AzureDeploymentName "<Deployment name>" -NetworkRuleCollectionName "<Name for collection of network rules>" -Priority 115 -AppRuleCollectionName "<Name for collection of app rules>"
```

NOTE

In this release, the script works in East US location only.

You will need to input the following information when you run the script:

PARAMETER	DESCRIPTION
Location	This is the region in which the Azure resources must be created.
AzureAppRuleFilePath	This is the file path for <code>appRule.json</code> .
AzureIPRangesFilePath	This is the Service Tag json file that you downloaded in the earlier step.
ResourceGroupName	This is the name of the resource group under which all the Azure resources are created.
AzureDeploymentName	This is the name for your Azure deployment.

PARAMETER	DESCRIPTION
NetworkRuleCollectionName	This is the name for the collection of all the network rules that are created and add to your Azure Firewall.
Priority	This is the priority assigned to all the network and application rules that are created.
AppRuleCollectionName	This is the name for the collection of all the application rules that are created and added to your Azure Firewall.

A sample output is shown below.

```
PS C:\Offline docs\AzureVpnConfigurationScripts> .\AzDeployVpn.ps1 -Location eastus -AzureAppRuleFilePath "appRule.json" -AzureIPRangesFilePath ".\ServiceTags_Public_20200203.json" -ResourceGroupName "mytmargin3" -AzureDeploymentName "tmap2stestdeploy1" -NetworkRuleCollectionName "testnrc1" -Priority 115 -AppRuleCollectionName "testarc2"
    validating vpn deployment parameters
    Starting vpn deployment
    C:\Offline docs\AzureVpnConfigurationScripts\parameters-p2s.json
    C:\Offline docs\AzureVpnConfigurationScripts\template-p2s.json
    vpn deployment: tmap2stestdeploy1 started and status: Running
    Waiting for vpn deployment completion....
==== CUT ===== CUT =====
Adding route 191.236.0.0/18 for AzureCloud.eastus
Adding route 191.237.0.0/17 for AzureCloud.eastus
Adding route 191.238.0.0/18 for AzureCloud.eastus
Total Routes:294, Existing Routes: 74, New Routes Added: 220
Additional routes getting added
```

IMPORTANT

- The script takes approximately 90 minutes to run. Make sure to sign into your network right before the script starts.
- If for any reason there is a failed session with the script, make sure to delete the resource group to delete all the resources created under it.

After the script is complete, a deployment log is generated in the same folder where the script resides.

Verify the Azure resources

After you've successfully run the script, verify that all the resources were created in Azure. Go to the resource group that you created. You should see the following resources:

Subscription (change)
DataBox_Edge_Test

Subscription ID
<Subscription ID>

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 7 of 7 records. Show hidden types No grouping

Name	Type	Location
firewall5	Firewall	East US
firewallpublicip5	Public IP address	East US
routetable5	Route table	East US
routetableonprem5	Route table	East US
vnet5	Virtual network	East US
vngw5	Virtual network gateway	East US
vngpublicip5	Public IP address	East US

< Previous Page 1 of 1 Next >

Download phone book for VPN profile

In this step, you will download the VPN profile for your device.

1. In the Azure portal, go to the resource group and then select the virtual network gateway that you created in the earlier step.

Subscription (change)
DataBox_Edge_Test

Subscription ID
<Subscription ID>

Tags (change)
Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 7 of 7 records. Show hidden types No grouping

Name	Type	Location
firewall5	Firewall	East US
firewallpublicip5	Public IP address	East US
routetable5	Route table	East US
routetableonprem5	Route table	East US
vnet5	Virtual network	East US
<input checked="" type="checkbox"/> vngw5	Virtual network gateway	East US
vngpublicip5	Public IP address	East US

< Previous Page 1 of 1 Next >

2. Go to **Settings > Point-to-site configuration**. Select **Download VPN client**.

3. Save the zipped profile and extract on your Windows client.

4. Go to *WindowsAmd64* folder and then extract the `.exe` : *VpnClientSetupAmd64.exe*.

5. Create a temporary path. For example:

```
C:\NewTemp\vnet\tmp
```

6. Run PowerShell and go to the directory where the `.exe` is located. To execute the `.exe`, type:

```
.\VpnClientSetupAmd64.exe /Q /C /T:"C:\NewTemp\vnet\tmp"
```

7. The temporary path will have new files. Here is a sample output:

```

PS C:\windows\system32> cd "C:\Users\Ase\Downloads\vngw5\WindowsAmd64"
PS C:\Users\Ase\Downloads\vngw5\WindowsAmd64> .\VpnClientSetupAmd64.exe /Q /C
/T:"C:\NewTemp\vnet\tmp"
PS C:\Users\Ase\Downloads\vngw5\WindowsAmd64> cd "C:\NewTemp\vnet"
PS C:\NewTemp\vnet> ls .\tmp

Directory: C:\NewTemp\vnet\tmp

Mode                LastWriteTime       Length Name
----                -----          -----
-a----   2/6/2020  6:18 PM           947 8c670077-470b-421a-8dd8-8cedb4f2f08a.cer
-a----   2/6/2020  6:18 PM           155 8c670077-470b-421a-8dd8-8cedb4f2f08a.cmp
-a----   2/6/2020  6:18 PM          3564 8c670077-470b-421a-8dd8-8cedb4f2f08a.cms
-a----   2/6/2020  6:18 PM          11535 8c670077-470b-421a-8dd8-8cedb4f2f08a.inf
-a----   2/6/2020  6:18 PM          2285 8c670077-470b-421a-8dd8-8cedb4f2f08a.pbk
-a----   2/6/2020  6:18 PM          5430 azurebox16.ico
-a----   2/6/2020  6:18 PM          4286 azurebox32.ico
-a----   2/6/2020  6:18 PM          138934 azurevpnbanner.bmp
-a----   2/6/2020  6:18 PM          46064 cmroute.dll
-a----   2/6/2020  6:18 PM          196 routes.txt

PS C:\NewTemp\vnet>

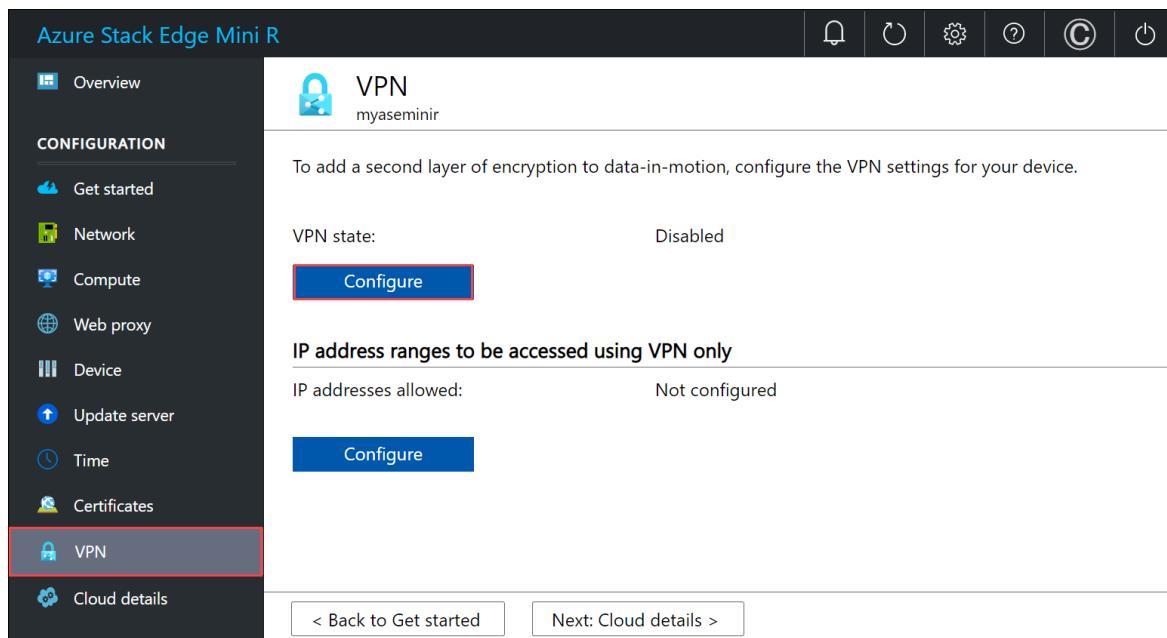
```

- The .pbk file is the phone book for the VPN profile. You will use this in the local UI.

VPN configuration on the device

Follow these steps on the local UI of your Azure Stack Edge device.

- In the local UI, go to **VPN** page. Under VPN state, select **Configure**.



- In the **Configure VPN** blade:

- In the Upload phone book file, point to the .pbk file that you created in the earlier step.
- In the Upload public IP list config file, provide Azure Data Center IP range JSON file as input. You downloaded this file in an earlier step from: <https://www.microsoft.com/download/details.aspx?id=56519>.
- Select **eastus** as the region and select **Apply**.

Configure VPN

* VPN settings

* Upload phone book file

8c670077-470b-421a-8dd8-8cedb4f2f08 ✓

* Upload public IP List config file

ServiceTags_Public_20200203.json ✓

Region

eastus ▾

If the phone book file (.pbk) and the public IP list config file (.json) are already uploaded, uploading those again will override the previous copies.

3. In the IP address ranges to be accessed using VPN only section, enter the Vnet IPv4 range that you had chosen for your Azure Virtual Network.

IP address ranges to be accessed using VPN only

Specify a range of IP addresses to be included for your VPN connection.

IPv4 range

Example: 10.10.10.10/24

Add

172.28.0.0/16

Delete

Apply

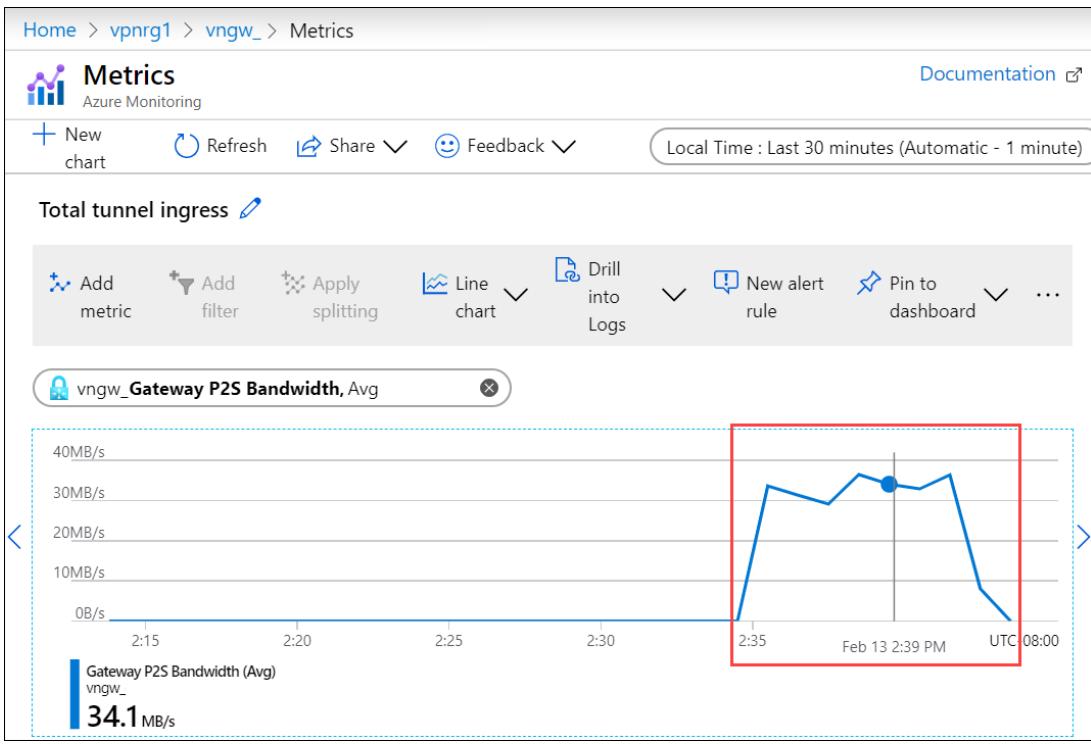
Verify client connection

1. In the Azure portal, go to the VPN gateway.
2. Go to **Settings > Point-to-site configuration**. Under **Allocated IP addresses**, the IP address of your Azure Stack Edge device should show up.

Validate data transfer through VPN

To confirm that VPN is working, copy data to an SMB share. Follow the steps in [Add a share](#) on your Azure Stack Edge device.

1. Copy a file, for example \data\pictures\waterfall.jpg to the SMB share that you mounted on your client system.
2. To validate that the data is going through VPN, while the data is being copied:
 - a. Go to the VPN gateway in the Azure portal.
 - b. Go to **Monitoring > Metrics**.
 - c. In the right-pane, choose the **Scope** as your VPN gateway, **Metric** as Gateway P2S bandwidth, and **Aggregation** as Avg.
 - d. As the data is being copied, you will see an increase in the bandwidth utilization and when the data copy is complete, the bandwidth utilization will drop.



3. Verify that this file shows up in your storage account on the cloud.

Debug issues

To debug any issues, use the following commands:

```
Get-AzResourceGroupDeployment -DeploymentName $deploymentName -ResourceGroupName $ResourceGroupName
```

The sample output is shown below:

```
PS C:\Projects\TZA\VPN\Azure-VpnDeployment> Get-AzResourceGroupDeployment -DeploymentName "tznvpngr14_deployment" -ResourceGroupName "tznvpngr14"
```

```

DeploymentName      : tznvpngr14_deployment
ResourceGroupName   : tznvpngr14
ProvisioningState   : Succeeded
Timestamp          : 1/21/2020 6:23:13 PM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name           Type       Value
    ======  ======  ======
    virtualNetworks_vnet_name     String
tznvpngr14_vnet      :
    azureFirewalls_firewall_name String
tznvpngr14_firewall  :
    routeTables_routetable_name String
tznvpngr14_routetable  :
    publicIPAddresses_VNGW_public_ip_name String
tznvpngr14_vngwpublicip  :
    virtualNetworkGateways_VNGW_name String
tznvpngr14_vngw      :
    publicIPAddresses_firewall_public_ip_name String
tznvpngr14_fwpip     :
    localNetworkGateways_LNGW_name String
tznvpngr14_lngw      :
    connections_vngw_lngw_name String
tznvpngr14_connection  :
    location          String
    vnetIPv4AddressSpace String
    East US
172.24.0.0/16        :
    defaultSubnetIPv4AddressSpace String
172.24.0.0/24        :
    firewallSubnetIPv4AddressSpace String
172.24.1.0/24        :
    gatewaySubnetIPv4AddressSpace String
172.24.2.0/24        :
    gatewaySubnetIPv4bgpPeeringAddress String
172.24.2.254         :
    customerNetworkAddressSpace String
10.0.0.0/18          :
    customerPublicNetworkAddressSpace String
207.68.128.0/24      :
    dbeIOTNetworkAddressSpace String
10.139.218.0/24      :
    azureVPNsharedKey      String
    dbE-Gateway-ipaddress  String
    1234567890
207.68.128.113       :

Outputs             :
    Name           Type       Value
    ======  ======  ======
    virtualNetwork     Object
    {
        "provisioningState": "Succeeded",
        "resourceGuid": "dcf673d3-5c73-4764-b077-77125eda1303",
        "addressSpace": {
            "addressPrefixes": [
                "172.24.0.0/16"
            ]
    ====== CUT ====== CUT ======
```

```
Get-AzResourceGroupDeploymentOperation -ResourceGroupName $ResourceGroupName -DeploymentName
$AzureDeploymentName
```

Next steps

Configure VPN via the local UI on your Azure Stack Edge device.

Configure business continuity and disaster recovery for Azure Stack Edge VPN

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to configure business continuity and disaster recovery (BCDR) on a virtual private network (VPN) configured on an Azure Stack Edge device.

This article applies to both Azure Stack Edge Pro R and Azure Stack Edge Mini R device.

Configure failover to a paired region

Your Azure Stack Edge device uses other Azure services, for example Azure Storage. You can configure BCDR on any specific Azure service that is used by the Azure Stack Edge device. If an Azure service used by Azure Stack Edge fails over to its paired region, the Azure Stack Edge device will now connect to the new IP addresses and the communication will not be doubly encrypted.

The Azure Stack Edge device uses split tunneling and all the data and services that are configured in the home region (the region associated with your Azure Stack Edge device) go over the VPN tunnel. If the Azure services fail over to a paired region which is outside of the home region, then the data will no longer go over VPN and hence is not doubly encrypted.

In this scenario, typically only a handful of Azure services are impacted. To address this issue, the following changes should be made in the Azure Stack Edge VPN configuration:

1. Add the failover Azure service IP range(s) in the inclusive routes for VPN on Azure Stack Edge. The services will then start getting routed through the VPN.

To add the inclusive routes, you need to download the json file that has the service specific routes. Make sure to update this file with the new routes.

2. Add the corresponding Azure service IP range(s) in Azure Route table.
3. Add the routes to the firewall.

NOTE

1. The failover of an Azure VPN gateway and Azure Virtual Network (VNET) is addressed in section [Recover from an Azure region that failed due to disaster](#).
2. IP ranges added in the Azure route table could cross the limit of 400. If this occurs, you will need to follow the guidance in section, [Move from one Azure region to another Azure region](#).

Recover from a failed Azure region

In the event that the entire Azure region fails over due to a catastrophic event such as earthquake, all the Azure services in that region including the Azure Stack Edge service will fail over. Since there are multiple services, the inclusive routes could easily range into a few hundreds. Azure has a limitation of 400 routes.

When the region fails over, the virtual network (Vnet) also fails over to the new region and so does the Virtual network gateway (VPN gateway). To address this change, make the following changes in your Azure Stack Edge

VPN configuration:

1. Move your Vnet to the target region. For more information, see: [Move an Azure virtual network to another region via the Azure portal](#).
2. Deploy a new Azure VPN gateway in the target region where you moved the Vnet. For more information, see [Create a virtual network gateway](#).
3. Update Azure Stack Edge VPN configuration to use the above VPN gateway in the VPN connection and then select the target region to add routes that use the VPN gateway.
4. Update the incoming Azure route table if the client address pool also changes.

Move from an Azure region to another

You can move your Azure Stack Edge device from one location to another location. To use a region closest to where your device is deployed, you will need to configure the device for a new home region. Make the following changes:

1. You can update Azure Stack Edge VPN configuration to use a new region's VPN gateway and select the new region to add routes that use VPN gateway.

Next steps

[Back up your Azure Stack Edge device](#).

Use the local web UI to manage wireless connectivity on your Azure Stack Edge Mini R

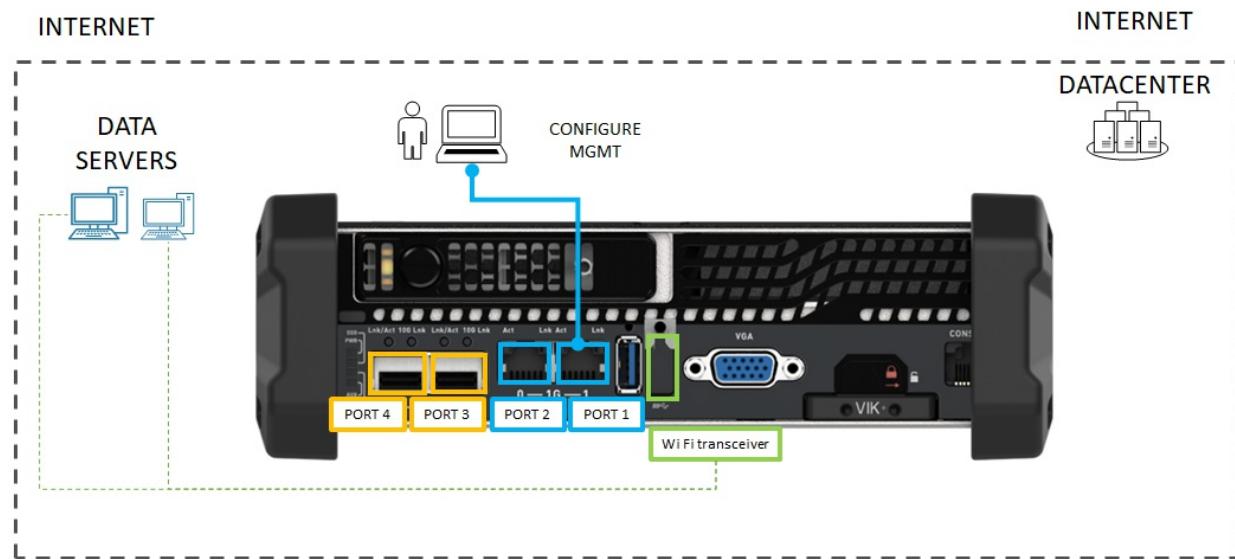
9/21/2022 • 3 minutes to read • [Edit Online](#)

This article describes how to manage wireless network connectivity on your Azure Stack Edge Mini R device. You can use the local web UI on your Azure Stack Edge Mini R device via to add, connect to, and delete Wi-Fi profiles.

About Wi-Fi

Your Azure Stack Edge Mini R device can operate both when wired to the network or via a wireless network. The device has a Wi-Fi port that must be enabled to allow the device to connect to a wireless network.

Your device has five ports, PORT 1 through PORT 4 and a fifth Wi-Fi port. Here is a diagram of the back plane of a Mini R device when connected to a wireless network.



Add, connect to Wi-Fi profile

Do the following steps in the local UI of your device to add and connect to a Wi-Fi profile.

1. Go to the **Get started** page in the local web UI of your device. On the **Network** tile, select **Configure**.

On your physical device, there are five network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3 and PORT 4 are all 10-Gbps network interfaces. The fifth port is the Wi-Fi port.

Azure Stack Edge Mini R

Overview

CONFIGURATION

- Get started
- Network**
- Compute
- Web proxy
- Device
- Update server
- Time
- Certificates
- VPN
- Cloud details

MAINTENANCE

- Power
- Hardware health
- Software update
- Password change
- Device reset

Network

DVM-TMA-00095

Link on the following port(s) is not active: Port WiFi.

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	-	-		3C-37-86-8B-4F-9A

Wifi profiles settings

For the Wifi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
Add Wifi profile	Connect Wifi Profile	Delete Wifi profile	

< Back to Get started Next: Compute >

Select the Wi-Fi port and configure the port settings.

IMPORTANT

We strongly recommend that you configure a static IP address for the Wi-Fi port.

Network settings (Port WiFi)

* IP settings

DHCP Static

* Subnet mask
255.255.252.0 ✓

Gateway
10.128.44.1 ✓

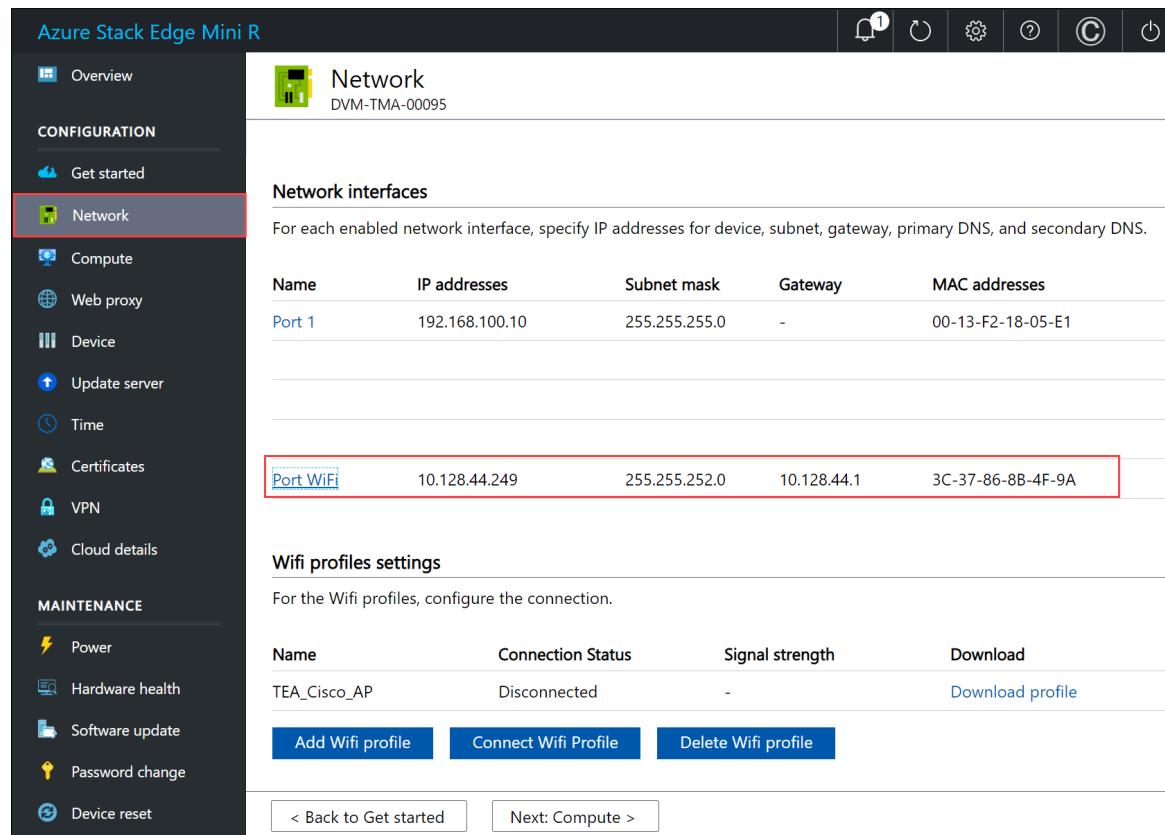
Primary DNS
10.50.50.50 ✓

Secondary DNS
10.50.10.50 ✓

Serial number	IP address	MAC address
VM-TMA-00095	10.128.44.249 ✓	3C-37-86-8B-4F-9A

Apply

The Network page updates after you apply the Wi-Fi port settings.



Azure Stack Edge Mini R

Network DVM-TMA-00095

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Wifi profiles settings

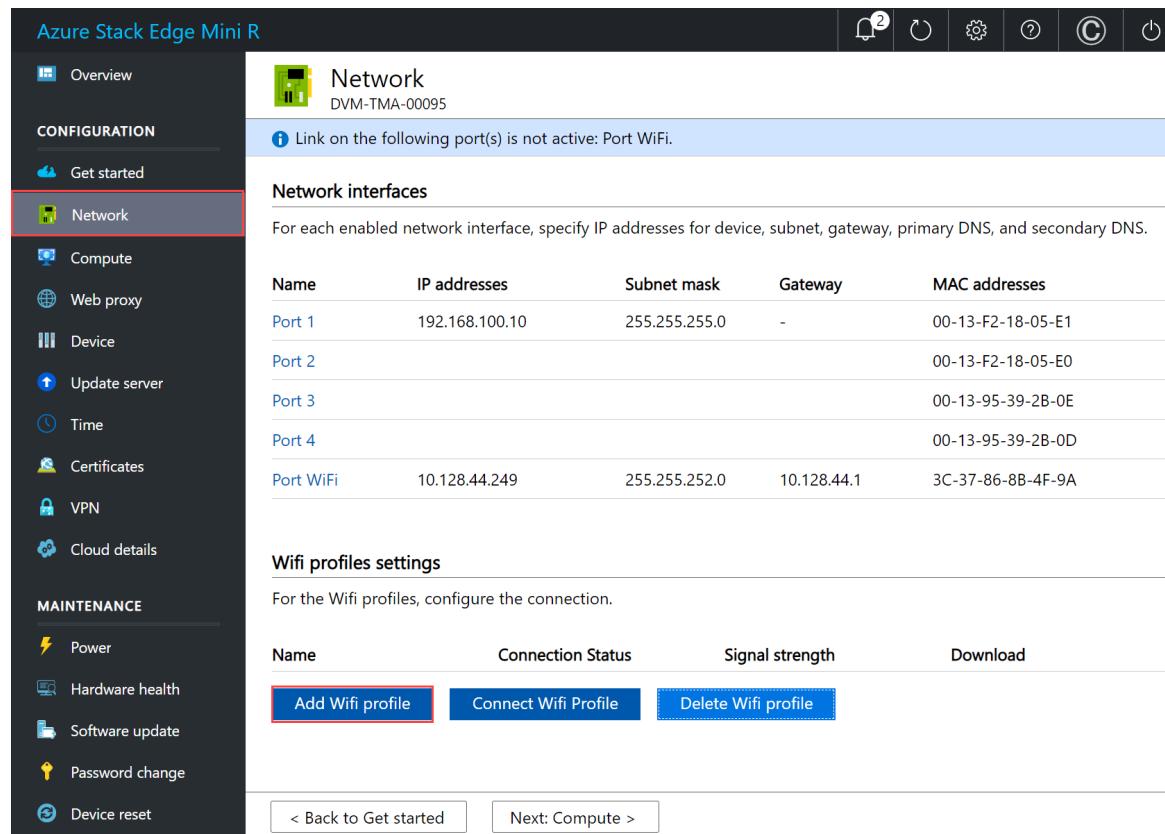
For the WiFi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
TEA_Cisco_AP	Disconnected	-	Download profile

[Add WiFi profile](#) [Connect WiFi Profile](#) [Delete WiFi profile](#)

< Back to Get started [Next: Compute >](#)

2. Select **Add Wi-Fi profile** and upload your Wi-Fi profile.



Azure Stack Edge Mini R

Network DVM-TMA-00095

Link on the following port(s) is not active: Port WiFi.

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Wifi profiles settings

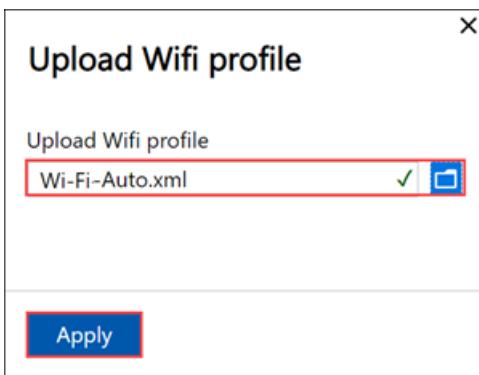
For the WiFi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
Add WiFi profile	Connect WiFi Profile	Delete WiFi profile	

< Back to Get started [Next: Compute >](#)

A wireless network profile contains the SSID (network name), password key, and security information to be able to connect to a wireless network. You can get the Wi-Fi profile for your environment from your network administrator.

For information about preparing your Wi-Fi profiles, see [Use Wi-Fi profiles with Azure Stack Edge Mini R devices](#).



After the profile is added, the list of Wi-Fi profiles updates to reflect the new profile. The profile should show the **Connection status** as **Disconnected**.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Name	Connection Status	Signal strength	Download
Aruba	Disconnected	-	Download profile

3. After the wireless network profile is successfully loaded, connect to this profile. Select **Connect to Wi-Fi profile**.

The screenshot shows the Azure Stack Edge Mini R interface. The left sidebar has sections for Overview, Configuration (Get started, Network, Compute, Web proxy, Device, Update server, Time, Certificates, VPN, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and a bottom section for Back to Get started and Next: Compute.

Network

Network interfaces

For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS.

Name	IP addresses	Subnet mask	Gateway	MAC addresses
Port 1	192.168.100.10	255.255.255.0	-	00-13-F2-18-05-E1
Port 2				00-13-F2-18-05-E0
Port 3				00-13-95-39-2B-0E
Port 4				00-13-95-39-2B-0D
Port WiFi	10.128.44.249	255.255.252.0	10.128.44.1	3C-37-86-8B-4F-9A

Wifi profiles settings

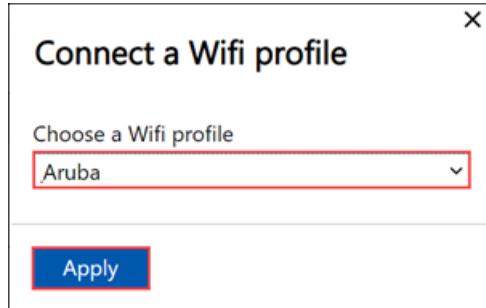
For the WiFi profiles, configure the connection.

Name	Connection Status	Signal strength	Download
Aruba	Disconnected	-	Download profile

[Add Wifi profile](#) [Connect Wifi Profile](#) [Delete Wifi profile](#)

[< Back to Get started](#) [Next: Compute >](#)

4. Select the Wi-Fi profile that you added in the previous step and select **Apply**.



The **Connection status** should update to **Connected**. The signal strength updates to indicate the quality of the signal.

The screenshot shows the Azure Stack Edge Mini R local web interface. The left sidebar has sections for Overview, Configuration (with Network selected), Compute, Web proxy, Device, Update server, Time, Certificates, VPN, and Cloud details. The Maintenance section includes Power, Hardware health, Software update, Password change, and Device reset. The Network section contains tables for Network interfaces and WiFi profiles settings. A note at the bottom of the Network section says: "For each enabled network interface, specify IP addresses for device, subnet, gateway, primary DNS, and secondary DNS." The WiFi profiles table shows one entry for Aruba with a connection status of Connected and signal strength of Moderate. Buttons for Add WiFi profile, Connect WiFi Profile (disabled), and Delete WiFi profile are present. Navigation buttons < Back to Get started and Next: Compute > are at the bottom.

NOTE

To transfer large amounts of data, we recommend that you use a wired connection instead of the wireless network.

Download Wi-Fi profile

You can download a Wi-Fi profile that you are using for the wireless network connectivity.

1. In the local web UI of your device, go to **Configuration > Network**.
2. Under Wi-Fi profile settings, select **Download profile**. This should download the Wi-Fi profile that you are currently using.

Delete Wi-Fi profile

You can delete a Wi-Fi profile that you are using for the wireless network connectivity.

1. In the local web UI of your device, go to **Configuration > Network**.
2. Under Wi-Fi profile settings, select **Delete Wi-Fi profile**.
3. In the **Delete Wi-Fi profile** blade, choose the profile you want to delete. Select **Apply**.

Configure Cisco Wi-Fi profile

Here is some guidance for how to manage and configure a Cisco wireless controller and access point on your device.

DHCP Bridging Mode

To use a Cisco Wireless controller for your device, you must enable dynamic host configuration protocol (DHCP) bridging mode on the wireless LAN controller (WLC).

For more information, see [DHCP Bridging Mode](#).

Bridging configuration example

To enable the DHCP bridging functionality on the controller, you must disable the DHCP proxy feature on the controller. To enable DHCP bridging using the command line:

```
(Cisco Controller) > config dhcp proxy disable  
(Cisco Controller) > show dhcp proxy  
DHCP Proxy Behaviour: disabled
```

If the DHCP server does not exist on the same Layer 2 (L2) network as the client, then the broadcast should be forwarded to the DHCP server at the client gateway using an IP helper. This is a sample of this configuration:

```
Switch#conf t  
Switch(config)#interface vlan <client vlan #>  
Switch(config-if)#ip helper-address <dhcp server IP>
```

The DHCP bridging feature is a global setting, so it affects all DHCP transactions within the controller. You need to add IP helper statements in the wired infrastructure for all necessary virtual local area networks (VLAN)s on the controller.

Enable the passive client for WLAN

To enable the passive client feature for wireless local area network (WLAN) on a Cisco Wireless controller:

- The interface associated to the WLAN must have a VLAN tagging enabled.
- Multicast VLAN must be enabled for the WLAN.
- GARP forwarding must be enabled on the WLC.

For more information, see [Multicast VLAN Information About Multicast Optimization](#).

Troubleshoot

If you encounter issues with IP address allocations on VMs running on an Azure Stack Edge Mini R device, the above configuration settings on your network environment should be validated.

Next steps

- Learn how to [Deploy Azure Stack Edge Mini R device](#).

Use Wi-Fi profiles with Azure Stack Edge Mini R devices

9/21/2022 • 5 minutes to read • [Edit Online](#)

This article describes how to use wireless network (Wi-Fi) profiles with your Azure Stack Edge Mini R devices.

How you prepare the Wi-Fi profile depends on the type of wireless network:

- On a Wi-Fi Protected Access 2 (WPA2) - Personal network, such as a home network or Wi-Fi open hotspot, you may be able to download and use an existing wireless profile with the same password you use with other devices.
- In a high-security enterprise environment, you'll access your device over a WPA2 - Enterprise network. On this type of network, each client computer will have a distinct Wi-Fi profile and will be authenticated via certificates. You'll need to work with your network administrator to determine the required configuration.

We'll discuss profile requirements for both types of network further later.

In either case, it's very important to make sure the profile meets the security requirements of your organization before you test or use the profile with your device.

About Wi-Fi profiles

A Wi-Fi profile contains the SSID (service set identifier, or **network name**), password key, and security information needed to connect your Azure Stack Edge Mini R device to a wireless network.

The following code example shows basic settings for a profile to use with a typical wireless network:

- `ssid` is the network name.
- `name` is the user-friendly name for the Wi-Fi connection. That is the name users will see when they browse the available connections on their device.
- The profile is configured to automatically connect the computer to the wireless network when it's within range of the network (`connectionMode` = `auto`).

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.contoso.com/networking/WLAN/profile/v1">
  <name>ContosoWIFICORP</name>
  <SSIDConfig>
    <SSID>
      <hex>1A234561234B5012</hex>
    </SSID>
    <nonBroadcast>false</nonBroadcast>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <autoSwitch>false</autoSwitch>
```

For more information about Wi-Fi profile settings, see [Enterprise profile](#) in [Add Wi-Fi settings for Windows 10 and newer devices](#), and see [Configure Cisco Wi-Fi profile](#).

To enable wireless connections on an Azure Stack Edge Mini R device, you configure the Wi-Fi port on your

device, and then add the Wi-Fi profile(s) to the device. On an enterprise network, you'll also upload certificates to the device. You can then connect to a wireless network from the local web UI for the device. For more information, see [Manage wireless connectivity on your Azure Stack Edge Mini R](#).

Profile for WPA2 - Personal network

On a Wi-Fi Protected Access 2 (WPA2) - Personal network, such as a home network or Wi-Fi open hotspot, multiple devices may use the same profile and the same password. On your home network, your mobile phone and laptop use the same wireless profile and password to connect to the network.

For example, a Windows 10 client can generate a runtime profile for you. When you sign in to the wireless network, you're prompted for the Wi-Fi password and, once you provide that password, you're connected. No certificate is needed in this environment.

On this type of network, you may be able to export a Wi-Fi profile from your laptop, and then add it to your Azure Stack Edge Mini R device. For instructions, see [Export a Wi-Fi profile](#), below.

IMPORTANT

Before you create a Wi-Fi profile for your Azure Stack Edge Mini R device, contact your network administrator to find out the organization's security requirements for wireless networking. You shouldn't test or use any Wi-Fi profile on your device until you know the wireless network meets requirements.

Profiles for WPA2 - Enterprise network

On a Wireless Protected Access 2 (WPA2) - Enterprise network, you'll need to work with your network administrator to get the needed Wi-Fi profile and certificate to connect your Azure Stack Edge Mini R device to the network.

For highly secure networks, the Azure device can use Protected Extensible Authentication Protocol (PEAP) with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). PEAP with EAP-TLS uses machine authentication: the client and server use certificates to verify their identities to each other.

NOTE

- User authentication using PEAP Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP MSCHAPv2) is not supported on Azure Stack Edge Mini R devices.
- EAP-TLS authentication is required in order to access Azure Stack Edge Mini R functionality. A wireless connection that you set up using Active Directory will not work.

The network administrator will generate a unique Wi-Fi profile and a client certificate for each computer. The network administrator decides whether to use a separate certificate for each device or a shared certificate.

If you work in more than one physical location at the workplace, the network administrator may need to provide more than one site-specific Wi-Fi profile and certificate for your wireless connections.

On an enterprise network, we recommend that you do not change settings in the Wi-Fi profiles that your network administrator provides. The only adjustment you may want to make is to the automatic connection settings. For more information, see [Basic profile](#) in Wi-Fi settings for Windows 10 and newer devices.

In a high-security enterprise environment, you may be able to use an existing wireless network profile as a template:

- You can download the corporate wireless network profile from your work computer. For instructions, see [Export a Wi-Fi profile](#), below.

- If others in your organization are already connecting to their Azure Stack Edge Mini R devices over a wireless network, they can download the Wi-Fi profile from their device. For instructions, see [Download Wi-Fi profile](#).

Export a Wi-Fi profile

To export a profile for the Wi-Fi interface on your computer, do these steps:

1. Make sure the computer you'll use to export the wireless profile can connect to the Wi-Fi network that your device will use.
2. To see the wireless profiles on your computer, on the **Start** menu, open **Command prompt** (cmd.exe), and enter this command:

```
netsh wlan show profiles
```

The output will look something like this:

```
Profiles on interface Wi-Fi:
Group policy profiles (read only)
-----
<None>

User profiles
-----
All User Profile      : ContosoCORP
All User Profile      : ContosoFTINET
All User Profile      : GusIS2809
All User Profile      : GusGuests
All User Profile      : SeaTacGUEST
All User Profile      : Boat
```

3. To export a profile, enter the following command:

```
netsh wlan export profile name=<profileName> folder=<path>\<profileName> key=clear
```

For example, the following command saves the ContosoFTINET profile in XML format to the Downloads folder for the user named `gusp`.

```
C:\Users\gusp>netsh wlan export profile name="ContosoFTINET" folder=c:Downloads key=clear
Interface profile "ContosoFTINET" is saved in file "c:Downloads\ContosoFTINET.xml" successfully.
```

Add certificate, Wi-Fi profile to device

When you have the Wi-Fi profiles and certificates that you need, do these steps to configure your Azure Stack Edge Mini R device for wireless connections:

1. For a WPA2 - Enterprise network, upload the needed certificates to the device following the guidance in [Upload certificates](#).
2. Upload the Wi-Fi profile(s) to the Mini R device and then connect to it by following the guidance in [Add, connect to Wi-Fi profile](#).

Next steps

- Learn how to [Configure network for Azure Stack Edge Mini R](#).

- Learn how to Manage Wi-Fi on your Azure Stack Edge Mini R.

What is local Azure Resource Manager on Azure Stack Edge?

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Azure Resource Manager provides a management layer that enables you to create, update, and delete resources in your Azure subscription. The Azure Stack Edge devices support the same Azure Resource Manager APIs to create, update, and delete VMs in a local subscription. This support lets you manage the device in a manner consistent with the cloud.

This article provides an overview of the local Azure Resource Manager that can be used to connect to the local APIs on your Azure Stack Edge devices.

About local Azure Resource Manager

The local Azure Resource Manager provides a consistent management layer for all the calls to the Azure Stack Edge device via the use of Resource Manager templates. The benefits of local Azure Resource Manager are discussed in the following sections.

Consistent management layer

The local Azure Resource Manager provides a consistent management layer to call the Azure Stack Edge device APIs and perform operations such as create, update, and delete VMs.

1. When you send a request from REST APIs or SDKs, the local Azure Resource Manager on the device receives the request.
2. The local Azure Resource Manager uses the Security Token Service (STS) to authenticate and authorize the request. STS is responsible for creation, validation, renewal, and cancellation of security tokens. STS creates both types of security tokens - the access tokens and the refresh tokens. These tokens are used for continuous communication between the device and the clients accessing the device via the local Azure Resource Manager.
3. The Resource Manager then sends the request to the resource providers that take the requested action.

The resource providers that are pre-registered with the Azure Stack Edge are as follows:

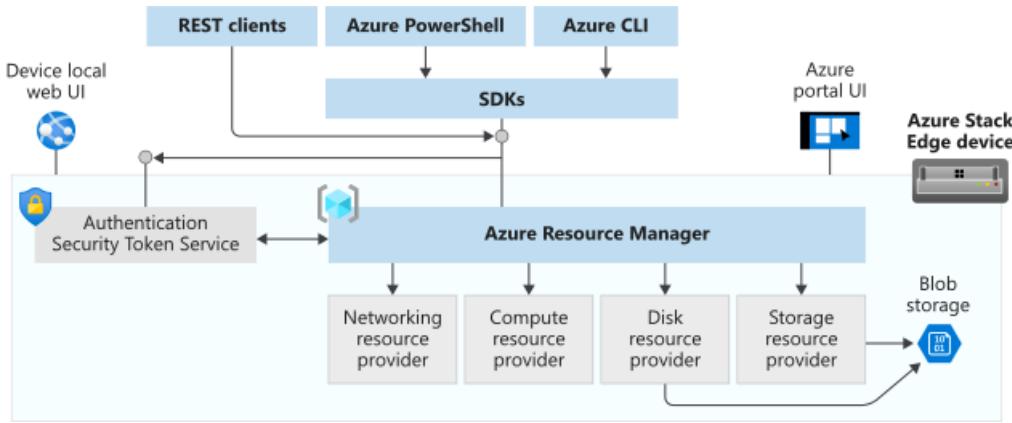
- **Compute:** The `Microsoft.Compute` or the Compute Resource Provider lets you deploy VMs on your Azure Stack Edge. The Compute Resource Provider includes the ability to create VMs and VM extensions.
- **Networking Resource Provider:** The `Microsoft.Network` or the Networking Resource Provider lets you create resources like network interfaces and virtual networks.
- **Storage Resource Provider:** The `Microsoft.Storage` or the Storage Resource Provider delivers Azure-consistent blob storage service and Key Vault account management providing management and auditing of secrets, such as passwords and certificates.
- **Disk Resource Provider:** The `Microsoft.Disks` or the Disk Resource Provider will let you create managed disks that can be used to create VMs.

Resources are manageable items that are available through Azure Stack Edge and the resource providers

are responsible for providing resources. For example, virtual machines, storage accounts, and virtual networks are examples of resources. And the compute resource provider supplies the virtual machine resource.

Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.

The following image shows the mechanism of handling all the API requests and the role the local Azure Resource Manager plays in providing a consistent management layer to handle those requests.



Use of Resource Manager templates

Another key benefit of Azure Resource Manager is that it lets you use Resource Manager templates. These are JavaScript Object Notation (JSON) files in a declarative syntax that can be used to deploy the resources consistently and repeatedly. The declarative syntax lets you state "Here is what I intend to create" without having to write the sequence of programming commands to create it. For example, you can use these declarative syntax templates to deploy virtual machines on your Azure Stack Edge devices. For detailed information, see [Deploy virtual machines on your Azure Stack Edge device via templates](#).

Connect to the local Azure Resource Manager

To create virtual machines or shares or storage accounts on your Azure Stack Edge device, you will need to create the corresponding resources. For example, for virtual machines, you will need resources such as network interface, OS and data disks on VM, from the networking, disk, and storage resource providers.

To request the creation of any resources from the resource providers, you will need to first connect to the local Azure Resource Manager. For detailed steps, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

The first time you connect to Azure Resource Manager, you would also need to reset your password. For detailed steps, see [Reset your Azure Resource Manager password](#).

Azure Resource Manager endpoints

The local Azure Resource Manager and the STS services run on your device and can be reached at specific endpoints. The following table summarizes the various endpoints exposed on your device by these services, the supported protocols, and the ports to access those endpoints.

#	ENDPOINT	SUPPORTED PROTOCOLS	PORT USED	USED FOR
1.	Azure Resource Manager	https	443	To connect to Azure Resource Manager for automation

#	ENDPOINT	SUPPORTED PROTOCOLS	PORT USED	USED FOR
2.	Security token service	https	443	To authenticate via access and refresh tokens

Next steps

[Connect to the local Azure Resource Manager on your Azure Stack Edge Pro GPU device.](#)

Connect to Azure Resource Manager on your Azure Stack Edge device

9/21/2022 • 19 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

Azure Resource Manager provides a management layer that enables you to create, update, and delete resources in your Azure subscription. The Azure Stack Edge device supports the same Azure Resource Manager APIs to create, update, and delete VMs in a local subscription. This support lets you manage the device in a manner consistent with the cloud.

This article describes how to connect to the local APIs on your Azure Stack Edge device via Azure Resource Manager using Azure PowerShell.

Endpoints on Azure Stack Edge device

The following table summarizes the various endpoints exposed on your device, the supported protocols, and the ports to access those endpoints. Throughout the article, you will find references to these endpoints.

#	ENDPOINT	SUPPORTED PROTOCOLS	PORT USED	USED FOR
1.	Azure Resource Manager	https	443	To connect to Azure Resource Manager for automation
2.	Security token service	https	443	To authenticate via access and refresh tokens
3.	Blob*	https	443	To connect to Blob storage via REST

* Connection to blob storage endpoint is not required to connect to Azure Resource Manager.

Connecting to Azure Resource Manager workflow

The process of connecting to local APIs of the device using Azure Resource Manager requires the following steps:

STEP #	YOU'LL DO THIS STEP ON THIS LOCATION.
1.	Configure your Azure Stack Edge device	Local web UI
2.	Create and install certificates	Windows client/local web UI
3.	Review and configure the prerequisites	Windows client
4.	Set up Azure PowerShell on the client	Windows client
5.	Modify host file for endpoint name resolution	Windows client or DNS server

STEP #	YOU'LL DO THIS STEP ON THIS LOCATION.
6.	Check that the endpoint name is resolved	Windows client
7.	Use Azure PowerShell cmdlets to verify connection to Azure Resource Manager	Windows client

The following sections detail each of the above steps in connecting to Azure Resource Manager.

Prerequisites

Before you begin, make sure that the client used for connecting to device via Azure Resource Manager is using TLS 1.2. For more information, go to [Configure TLS 1.2 on Windows client accessing Azure Stack Edge device](#).

Step 1: Configure Azure Stack Edge device

Take the following steps in the local web UI of your Azure Stack Edge device.

1. Complete the network settings for your Azure Stack Edge device.

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.128.24.0	No
Port 3	5.5.0.0	No
Port 4	5.5.0.0	No
Port 5	5.5.0.0	No
Port 6	5.5.0.0	No

Make a note of the device IP address. You will use this IP later.

2. Configure the device name and the DNS domain from the **Device** page. Make a note of the device name and the DNS domain as you will use these later.

To complete this step, you will need to apply the desired device name and DNS domain.

Device name

Assign a friendly name and DNS domain for the device.

* Name	DBE-1CSPHQ2
* DNS domain	wdshcsso.com

Device endpoints

Use these device endpoints to reach the following services. Some services require a certificate. For those services, certificates must be uploaded for the endpoint to be valid.

Service	Certificate Required	Endpoint
SMB server	No	Endpoint not yet created.
NFS server	No	Endpoint not yet created.
Azure Resource Manager login	Yes	https://login.dbe-1csphq2.microsoftdatabox.com
Azure Resource Manager	Yes	https://management.dbe-1csphq2.microsoftdatabox.com
Blob Storage	Yes	https://[Account name].blob.dbe-1csphq2.microsoftdatabox.com
Kubernetes API	No	Endpoint not yet created.
Kubernetes dashboard	Yes	Endpoint not yet created.
Edge IoT hub	Yes	Endpoint not yet created.
Edge container registry	Yes	Endpoint not yet created.

IMPORTANT

The device name, DNS domain will be used to form the endpoints that are exposed. Use the Azure Resource Manager and Blob endpoints from the **Device** page in the local web UI.

Step 2: Create and install certificates

Certificates ensure that your communication is trusted. On your Azure Stack Edge device, self-signed appliance, blob, and Azure Resource Manager certificates are automatically generated. Optionally, you can bring in your own signed blob and Azure Resource Manager certificates as well.

When you bring in a signed certificate of your own, you also need the corresponding signing chain of the certificate. For the signing chain, Azure Resource Manager, and the blob certificates on the device, you will need the corresponding certificates on the client machine also to authenticate and communicate with the device.

To connect to Azure Resource Manager, you will need to create or get signing chain and endpoint certificates, import these certificates on your Windows client, and finally upload these certificates on the device.

Create certificates

For test and development use only, you can use Windows PowerShell to create certificates on your local system. While creating the certificates for the client, follow these guidelines:

1. You first need to create a root certificate for the signing chain. For more information, see See steps to [Create signing chain certificates](#).
2. You can next create the endpoint certificates for Azure Resource Manager and blob (optional). You can get these endpoints from the **Device** page in the local web UI. See the steps to [Create endpoint certificates](#).
3. For all these certificates, make sure that the subject name and subject alternate name conform to the following guidelines:

Type	Subject Name (SN)	Subject Alternative Name (SAN)	Subject Name Example
Azure Resource Manager	management.<Device name>.<Dns Domain>	login.<Device name>.<Dns Domain> management.<Device name>.<Dns Domain>	management.mydevice1.microsoftdatabox.com
Blob storage*	*.blob.<Device name>.<Dns Domain>	*.blob.<Device name>.<Dns Domain>	*.blob.mydevice1.microsoftdatabox.com
Multi-SAN single certificate for both endpoints	<Device name>.<dnsdomain>	login.<Device name>.<Dns Domain> management.<Device name>.<Dns Domain> *.blob.<Device name>.<Dns Domain>	mydevice1.microsoftdatabox.com

* Blob storage is not required to connect to Azure Resource Manager. It is listed here in case you are creating local storage accounts on your device.

For more information on certificates, go to how to [Upload certificates on your device and import certificates on the clients accessing your device](#).

Upload certificates on the device

The certificates that you created in the previous step will be in the Personal store on your client. These certificates need to be exported on your client into appropriate format files that can then be uploaded to your device.

1. The root certificate must be exported as a DER format file with .cer file extension. For detailed steps, see [Export certificates as a .cer format file](#).
2. The endpoint certificates must be exported as .pfx files with private keys. For detailed steps, see [Export certificates as .pfx file with private keys](#).
3. The root and endpoint certificates are then uploaded on the device using the +Add certificate option on the Certificates page in the local web UI. To upload the certificates, follow the steps in [Upload certificates](#).

Import certificates on the client running Azure PowerShell

The Windows client where you will invoke the Azure Resource Manager APIs needs to establish trust with the device. To this end, the certificates that you created in the previous step must be imported on your Windows client into the appropriate certificate store.

1. The root certificate that you exported as the DER format with .cer extension should now be imported in the Trusted Root Certificate Authorities on your client system. For detailed steps, see [Import certificates into the Trusted Root Certificate Authorities store](#).
2. The endpoint certificates that you exported as the .pfx must be exported as .cer. This .cer is then imported in the Personal certificate store on your system. For detailed steps, see [Import certificates into personal store](#).

Step 3: Install PowerShell on the client

- Az
- AzureRM

Your Windows client must meet the following prerequisites:

1. Run PowerShell Version 5.0. You must have PowerShell version 5.0. To check the version of PowerShell on your system, run the following cmdlet:

```
$PSVersionTable.PSVersion
```

Compare the **Major** version and ensure that it is 5.0 or later.

If you have an outdated version, see [Upgrading existing Windows PowerShell](#).

If you don't have PowerShell 5.0, follow [Installing Windows PowerShell](#).

An example output is shown below.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\windows\system32> $PSVersionTable.PSVersion
Major  Minor  Build  Revision
-----  -----  -----  -----
5       1       19041  906
```

2. You can access the PowerShell Gallery.

Run PowerShell as administrator. Verify that PowerShellGet version is older than 2.2.3. Additionally, verify if the `PSGallery` is registered as a repository.

```
Install-Module PowerShellGet -MinimumVersion 2.2.3
Import-Module -Name PackageManagement -ErrorAction Stop
Get-PSRepository -Name "PSGallery"
```

An example output is shown below.

```
PS C:\windows\system32> Install-Module PowerShellGet -MinimumVersion 2.2.3
PS C:\windows\system32> Import-Module -Name PackageManagement -ErrorAction Stop
PS C:\windows\system32> Get-PSRepository -Name "PSGallery"
Name            InstallationPolicy   SourceLocation
----            -----           -----
PSGallery        Trusted           https://www.powershellgallery.com/api/v2
```

If your repository is not trusted or you need more information, see [Validate the PowerShell Gallery accessibility](#).

Step 4: Set up Azure PowerShell on the client

- [Az](#)
- [AzureRM](#)

You will install Azure PowerShell modules on your client that will work with your device.

1. Run PowerShell as an administrator. You need access to PowerShell gallery.
2. First verify that there are no existing versions of `AzureRM` and `Az` modules on your client. To check, run the following commands:

```
# Check existing versions of AzureRM modules
Get-InstalledModule -Name AzureRM -AllVersions

# Check existing versions of Az modules
Get-InstalledModule -Name Az -AllVersions
```

If there are existing versions, use the `Uninstall-Module` cmdlet to uninstall. For more information, see

- [Uninstall AzureRM modules](#).

- [Uninstall Az modules.](#)
3. To install the required Azure PowerShell modules from the PowerShell Gallery, run the following command:

- If your client is using PowerShell Core version 7.0 and later:

```
# Install the Az.BootStrapper module. Select Yes when prompted to install NuGet.  
Install-Module -Name Az.BootStrapper  
  
# Install and import the API Version Profile into the current PowerShell session.  
Use-AzProfile -Profile 2020-09-01-hybrid -Force  
  
# Confirm the installation of PowerShell  
Get-Module -Name "Az*" -ListAvailable
```

- If your client is using PowerShell 5.1 and later:

```
#Install the Az module version 1.10.0  
  
Install-Module -Name Az -RequiredVersion 1.10.0
```

4. Make sure that you have Az module version 1.10.0 running at the end of the installation.

If you used PowerShell core 7.0 and later, the example output below indicates that the Az version 1.10.0 modules were installed successfully.

```
PS C:\windows\system32> Install-Module -Name Az.BootStrapper  
PS C:\windows\system32> Use-AzProfile -Profile 2020-09-01-hybrid -Force  
Loading Profile 2020-09-01-hybrid  
PS C:\windows\system32> Get-Module -Name "Az*" -ListAvailable
```

If you used PowerShell 5.1 and later, the example output below indicates that that the Az version 1.10.0 modules were installed successfully.

```
PS C:\WINDOWS\system32> Get-InstalledModule -Name Az -AllVersions  
Version          Name           Repository      Description  
-----          ----           -----          -----  
1.10.0          Az             PSGallery      Mic...  
  
PS C:\WINDOWS\system32>
```

Step 5: Modify host file for endpoint name resolution

You will now add the device IP address to:

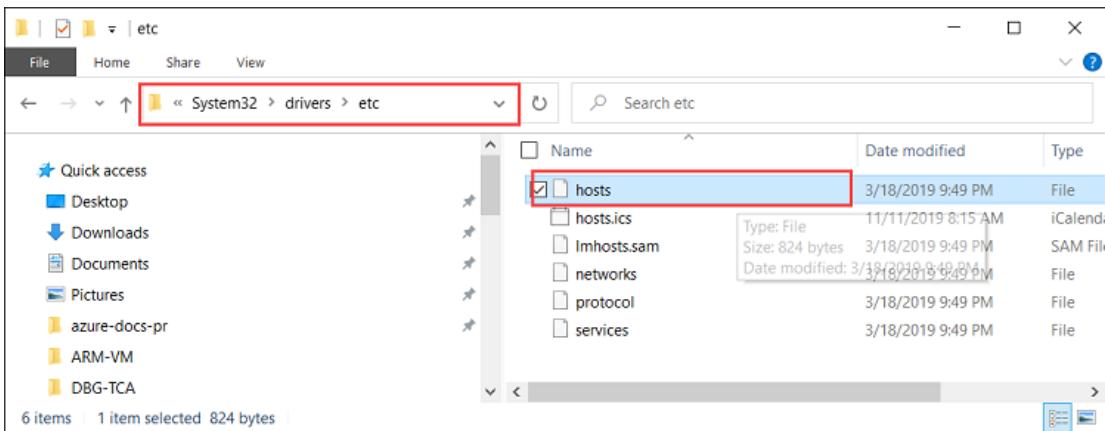
- The host file on the client, OR,
- The DNS server configuration

IMPORTANT

We recommend that you modify the the DNS server configuration for endpoint name resolution.

On your Windows client that you are using to connect to the device, take the following steps:

1. Start **Notepad** as an administrator, and then open the **hosts** file located at C:\Windows\System32\Drivers\etc.



2. Add the following entries to your **hosts** file replacing with appropriate values for your device:

```
<Device IP> login.<appliance name>.<DNS domain>
<Device IP> management.<appliance name>.<DNS domain>
<Device IP> <storage name>.blob.<appliance name>.<DNS domain>
```

IMPORTANT

The entry in the hosts file should match exactly that provided to connect to Azure Resource Manager at a later step. Make sure that the DNS Domain entry here is all in the lowercase. To get the values for the `<appliance name>` and `<DNS domain>`, go to the Device page in the local UI of your device.

You saved the device IP from the local web UI in an earlier step.

The `login.<appliance name>.<DNS domain>` entry is the endpoint for Security Token Service (STS). STS is responsible for creation, validation, renewal, and cancellation of security tokens. The security token service is used to create the access token and refresh token that are used for continuous communication between the device and the client.

The endpoint for blob storage is optional when connecting to Azure Resource Manager. This endpoint is needed when transferring data to Azure via storage accounts.

3. For reference, use the following image. Save the **hosts** file.

A screenshot of a Windows Notepad window titled 'hosts - Notepad'. The window contains a sample HOSTS file. The last two lines, which define the management and login endpoints, are highlighted with a red box. The full content of the file is as follows:

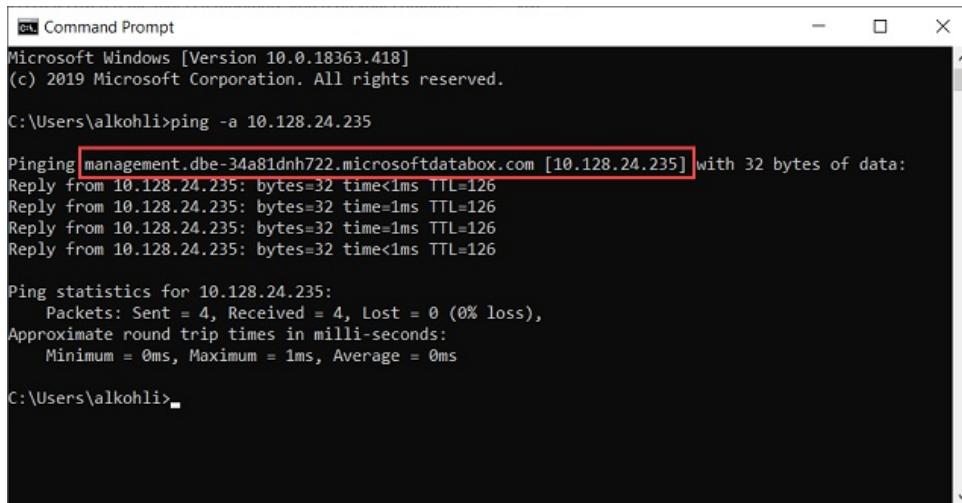
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost
10.128.27.72      management.mydevice1.microsoftdatabox.com
10.128.27.72      login.mydevice1.microsoftdatabox.com
```

Step 6: Verify endpoint name resolution on the client

Check if the endpoint name is resolved on the client that you are using to connect to the device.

1. You can use the `ping.exe` command-line utility to check that the endpoint name is resolved. Given an IP address, the `ping` command will return the TCP/IP host name of the computer you're tracing.

Add the `-a` switch to the command line as shown in the example below. If the host name is returnable, it will also return this potentially valuable information in the reply.



```
Windows PowerShell [Version 10.0.18363.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\alkohli>ping -a 10.128.24.235

Pinging management.dbe-34a81dh722.microsoftdatabox.com [10.128.24.235] with 32 bytes of data:
Reply from 10.128.24.235: bytes=32 time<1ms TTL=126
Reply from 10.128.24.235: bytes=32 time=1ms TTL=126
Reply from 10.128.24.235: bytes=32 time=1ms TTL=126
Reply from 10.128.24.235: bytes=32 time<1ms TTL=126

Ping statistics for 10.128.24.235:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\alkohli>
```

Step 7: Set Azure Resource Manager environment

- [Az](#)
- [AzureRM](#)

Set the Azure Resource Manager environment and verify that your device to client communication via Azure Resource Manager is working fine. Take the following steps for this verification:

1. Use the `Add-AzEnvironment` cmdlet to further ensure that the communication via Azure Resource Manager is working properly and the API calls are going through the port dedicated for Azure Resource Manager - 443.

The `Add-AzEnvironment` cmdlet adds endpoints and metadata to enable Azure Resource Manager cmdlets to connect with a new instance of Azure Resource Manager.

IMPORTANT

The Azure Resource Manager endpoint URL that you provide in the following cmdlet is case-sensitive. Make sure the endpoint URL is all in lowercase and matches what you provided in the hosts file. If the case doesn't match, then you will see an error.

```
Add-AzEnvironment -Name <Environment Name> -ARMEndpoint "https://management.<appliance name>.<DNSDomain>/"
```

A sample output is shown below:

```
PS C:\WINDOWS\system32> Add-AzEnvironment -Name AzASE -ARMEndpoint
"https://management.myasegpu.wdshcsso.com/"

Name  Resource Manager Url          ActiveDirectory Authority
----  -----
AzASE https://management.myasegpu.wdshcsso.com/ https://login.myasegpu.wdshcsso.c...
```

2. Set the environment as Azure Stack Edge and the port to be used for Azure Resource Manager calls as 443. You define the environment in two ways:

- Set the environment. Type the following command:

```
Set-AzEnvironment -Name <Environment Name>
```

Here is an example output.

```
PS C:\WINDOWS\system32> Set-AzEnvironment -Name AzASE

Name  Resource Manager Url          ActiveDirectory Authority
----  -----
AzASE https://management.myasegpu.wdshcsso.com/ https://login.myasegpu.wdshcsso.c...
```

For more information, go to [Set-AzEnvironment](#).

- Define the environment inline for every cmdlet that you execute. This ensures that all the API calls are going through the correct environment. By default, the calls would go through the Azure public but you want these to go through the environment that you set for Azure Stack Edge device.
- See more information on how to [Switch Az environments](#).

3. Call local device APIs to authenticate the connections to Azure Resource Manager.

- These credentials are for a local machine account and are solely used for API access.
- You can connect via `login-AzAccount` or via `Connect-AzAccount` command.
 - To sign in, type the following command.

```
$pass = ConvertTo-SecureString "<Your password>" -AsPlainText -Force;
$cred = New-Object System.Management.Automation.PSCredential("EdgeArmUser", $pass)
Connect-AzAccount -EnvironmentName AzASE -TenantId c0257de7-538f-415c-993a-1b87a031879d
-credential $cred
```

Use the tenant ID c0257de7-538f-415c-993a-1b87a031879d as in this instance it is hard coded. Use the following username and password.

- **Username** - *EdgeArmUser*
- **Password** - Set the password for Azure Resource Manager and use this password to sign in.

Here is an example output for the `Connect-AzAccount`:

```
PS C:\windows\system32> $pass = ConvertTo-SecureString "<Your password>" -AsPlainText -
Force;
PS C:\windows\system32> $cred = New-Object
System.Management.Automation.PSCredential("EdgeArmUser", $pass)
PS C:\windows\system32> Connect-AzAccount -EnvironmentName AzASE -TenantId c0257de7-
538f-415c-993a-1b87a031879d -credential $cred

Account      SubscriptionName   TenantId        Environment
-----      -----
EdgeArmUser@localhost  Default  Provider  Subscription c0257de7-538f-415c-993a-
1b87a031879d  AzASE

PS C:\windows\system32>
```

An alternative way to log in is to use the `login-AzAccount` cmdlet.

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

Here is an example output.

```
PS C:\WINDOWS\system32> login-AzAccount -EnvironmentName AzASE -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

Account	SubscriptionName	TenantId
EdgeArmUser@localhost	Default Provider Subscription	c0257de7-538f-415c-993a-1b87a...

```
PS C:\WINDOWS\system32>
```

4. To verify that the connection to the device is working, use the `Get-AzResource` command. This command should return all the resources that exist locally on the device.

Here is an example output.

```
PS C:\WINDOWS\system32> Get-AzResource

Name          : aseimagestorageaccount
ResourceGroupName : ase-image-resourcegroup
 ResourceType    : Microsoft.Storage/storageaccounts
 Location       : dbelocal
 ResourceId     : /subscriptions/.../resourceGroups/ase-image-
                  resourcegroup/providers/Microsoft.Storage/storageac-
                  counts/aseimagestorageaccount
 Tags          :

Name          : myaselinuxvmimage1
ResourceGroupName : ASERG
 ResourceType    : Microsoft.Compute/images
 Location       : dbelocal
 ResourceId     :
 /subscriptions/.../resourceGroups/ASERG/providers/Microsoft.Compute/images/myaselinuxvmimage1
 Tags          :

Name          : ASEVNET
ResourceGroupName : ASERG
 ResourceType    : Microsoft.Network/virtualNetworks
 Location       : dbelocal
 ResourceId     :
 /subscriptions/.../resourceGroups/ASERG/providers/Microsoft.Network/virtualNetworks/ASEVNET
 Tags          :

PS C:\WINDOWS\system32>
```

If you run into issues with your Azure Resource Manager connections, see [Troubleshoot Azure Resource Manager issues](#) for guidance.

IMPORTANT

The connection to Azure Resource Manager expires every 1.5 hours or if your Azure Stack Edge device restarts. If this happens, any cmdlets that you execute, will return error messages to the effect that you are not connected to Azure anymore. You will need to sign in again.

Switch environments

You may need to switch between two environments.

- [Az](#)
- [AzureRM](#)

Run `Disconnect-AzAccount` command to switch to a different `AzEnvironment`. If you use `Set-AzEnvironment` and `Login-AzAccount` without using `Disconnect-AzAccount`, the environment is not actually switched.

The following examples show how to switch between two environments, `AzASE1` and `AzASE2`.

First, list all the existing environments on your client.

```
PS C:\WINDOWS\system32> Get-AzEnvironment
Name      Resource Manager Url      ActiveDirectory Authority
----      -----
AzureChinaCloud https://management.chinacloudapi.cn/          https://login.chinacloudapi.cn/
AzureCloud     https://management.azure.com/                 https://login.microsoftonline.com/
AzureGermanCloud https://management.microsoftazure.de/       https://login.microsoftonline.de/
AzDBE1        https://management.HVTG1T2-Test.microsoftdatabox.com https://login.hvtg1t2-
test.microsoftdatabox.com/adfs/
AzureUSGovernment https://management.usgovcloudapi.net/      https://login.microsoftonline.us/
AzDBE2        https://management.CVV4PX2-Test.microsoftdatabox.com https://login.csv4px2-
test.microsoftdatabox.com/adfs/
```

Next, get which environment you are currently connected to via your Azure Resource Manager.

```
PS C:\WINDOWS\system32> Get-AzContext | fl *
Name          : Default Provider Subscription (...) - EdgeArmUser@localhost
Account       : EdgeArmUser@localhost
Environment   : AzDBE2
Subscription  : ...
Tenant        : c0257de7-538f-415c-993a-1b87a031879d
TokenCache    : Microsoft.Azure.Commands.Common.Authentication.ProtectedFileTokenCache
VersionProfile :
ExtendedProperties : {}
```

You should now disconnect from the current environment before you switch to the other environment.

```
PS C:\WINDOWS\system32> Disconnect-AzAccount
Id          : EdgeArmUser@localhost
Type        : User
Tenants     : {c0257de7-538f-415c-993a-1b87a031879d}
AccessToken  :
Credential  :
TenantMap   : {}
CertificateThumbprint :
ExtendedProperties : {[Subscriptions, ...], [Tenants, c0257de7-538f-415c-993a-1b87a031879d]}
```

Log into the other environment. The sample output is shown below.

```
PS C:\WINDOWS\system32> Login-AzAccount -Environment "AzDBE1" -TenantId $ArmTenantId
Account      SubscriptionName  TenantId      Environment
-----      -----
EdgeArmUser@localhost  Default Provider Subscription c0257de7-538f-415c-993a-1b87a031879d  AzDBE1
```

Run this cmdlet to confirm which environment you are connected to.

```
PS C:\WINDOWS\system32> Get-AzContext |fl *
```

```
Name          : Default Provider Subscription (...) - EdgeArmUser@localhost
Account       : EdgeArmUser@localhost
Environment   : AzDBE1
Subscription  : ...
Tenant        : c0257de7-538f-415c-993a-1b87a031879d
TokenCache    : Microsoft.Azure.Commands.Common.Authentication.ProtectedFileTokenCache
VersionProfile : 
ExtendedProperties : {}
```

You have now switched to the intended environment.

Set Azure Resource Manager password on Azure Stack Edge Pro GPU device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to set your Azure Resource Manager password. You need to set this password when you are [connecting to the device local APIs via the Azure Resource Manager](#).

Reset password via the Azure portal

1. In the Azure portal, go to the Azure Stack Edge resource you created to manage your device.
2. Go to **Properties**. In the right pane, from the command bar, select **Reset Edge ARM password**.

The screenshot shows the 'VMGADevice5 | Properties' blade in the Azure portal. On the left, there's a sidebar with 'Properties' highlighted. The main area displays device details: Status (Online), Friendly name (D8E-3V78B03), Capacity (5.37 TB), Time zone (Pacific Standard Time), Model (Azure Stack Edge Pro - 1 GPU), Device serial number (3V78B03), Current software version (Azure Stack Edge 2103 (2.2.1529.26267)), and Last software update (-). At the top right, there's a 'Reset Edge ARM password' button, which is also highlighted with a red box.

3. In the **Reset EdgeARM user password** blade, provide a password to connect to your device local APIs via the Azure Resource Manager. Confirm the password and select **Reset**.

The screenshot shows the 'Reset EdgeARMUser password' blade. It has a header 'myasegpudev'. Below it, a message says 'Set the password for EdgeARMUser. These credentials are used for API access.' There are two input fields: 'New password' and 'Confirm password', both showing masked text. At the bottom is a 'Reset' button, which is highlighted with a red box.

Next steps

[Connect to Azure Resource Manager](#)

Configure TLS 1.2 on Windows clients accessing Azure Stack Edge Pro device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

If you are using a Windows client to access your Azure Stack Edge Pro device, you are required to configure TLS 1.2 on your client. This article provides resources and guidelines to configure TLS 1.2 on your Windows client.

The guidelines provided here are based on testing performed on a client running Windows Server 2016.

Configure TLS 1.2 for current PowerShell session

Do the following steps to configure TLS 1.2 on your client.

1. Run PowerShell as administrator.
2. To set TLS 1.2 for the current PowerShell session, type:

```
$TLS12Protocol = [System.Net.SecurityProtocolType] 'Ssl3 , Tls12'  
[System.Net.ServicePointManager]::SecurityProtocol = $TLS12Protocol
```

Configure TLS 1.2 on client

If you want to set system-wide TLS 1.2 for your environment, follow the guidelines in these documents:

- [General- how to enable TLS 1.2](#)
- [How to enable TLS 1.2 on clients](#)
- [How to enable TLS 1.2 on the site servers and remote site systems](#)
- [Protocols in TLS/SSL \(Schannel SSP\)](#)
- [Cipher Suites: Specifically Configuring TLS Cipher Suite Order](#) Make sure that you list your current cipher suites and prepend any missing from the following list:
 - `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
 - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
 - `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`
 - `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`

You can also add these cipher suites by directly editing the registry settings.

```
New-ItemProperty -Path "$Hk1mSoftwarePath\Policies\Microsoft\Cryptography\Configuration\SSL\00010002"  
-Name "Functions" -PropertyType String -Value ("TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,  
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,  
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384")
```

- [How to set elliptical curves](#)

Make sure that you list your current elliptical curves and prepend any missing from the following list:

- o P-256
- o P-384

You can also add these elliptical curves by directly editing the registry settings.

```
New-ItemProperty -Path "$Hk1mSoftwarePath\ Policies\Microsoft\Cryptography\Configuration\SSL\00010002"  
-Name "EccCurves" -PropertyType MultiString -Value @("NistP256", "NistP384")
```

- o Set min RSA key exchange size to 2048.

Next steps

[Connect to Azure Resource Manager](#)

Troubleshoot Azure Resource Manager issues on an Azure Stack Edge device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot issues with Azure Resource Manager that may interfere with management of resources on your Azure Stack Edge device. Azure Resource Manager provides a management layer that enables you to create, update, and delete resources in your Azure account.

Azure Resource Manager configuration errors

The following errors may indicate an issue with your Azure Resource Manager configuration.

ISSUE / ERRORS	RESOLUTION
General issues	<ul style="list-style-type: none">Verify that the device is configured properly.Verify that the client is configured properly.
Add-AzureRmEnvironment: An error occurred while sending the request. At line:1 char:1 + Add-AzureRmEnvironment -Name Az3 -ARMEndpoint "https://management.dbe ...	Your device isn't reachable or isn't configured properly. Verify that the device and the client are configured correctly. For guidance, see the General issues row in this table.
Service returned error. Check InnerException for more details: The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.	There was an error in the creation and installation of the certificate on your device. For more information, see Create and install certificates .
Operation returned an invalid status code 'ServiceUnavailable' Response status code does not indicate success: 503 (Service Unavailable).	<p>This error could be the result of any of these conditions:</p> <ul style="list-style-type: none">• ArmStsPool is in stopped state.• Either Azure Resource Manager is down or the website for the Security Token Service is down.• The Azure Resource Manager cluster resource is down. <p>Restarting the device may fix the issue. To debug further, collect a Support package.</p>
AADSTS50126: Invalid username or password. Trace ID: 29317da9-52fc-4ba0-9778-446ae5625e5a Correlation ID: 1b9752c4-8cbf-4304-a714-8a16527410f4 Timestamp: 2019-11-15 09:21:57Z: The remote server returned an error: (400) Bad Request. At line:1 char:1	This error could be the result of any of these conditions: <ul style="list-style-type: none">• For an invalid username and password, make sure that you have reset the Azure Storage Manager password from the Azure portal, and then use the correct password.• For an invalid tenant ID, make sure the tenant ID is set to <code>c0257de7-538f-415c-993a-1b87a031879d</code>

ISSUE / ERRORS	RESOLUTION
<p>connect-AzureRmAccount: AADSTS90056: The resource is disabled or does not exist. Check your app's code to ensure that you have specified the exact resource URL for the resource you are trying to access.</p> <p>Trace ID: e19bdbca-5dc8-4a74-85c3-ac6abdfda115 Correlation ID: 75c8ef5a-830e-48b5-b039-595a96488ff9 Timestamp: 2019-11-18 07:00:51Z: The remote server returned an error: (400) Bad</p>	<p>The Azure Resource Manager endpoints used in the <code>Add-AzureRmEnvironment</code> command are incorrect. To find the Azure Resource Manager endpoints, check Device endpoints on the Device page of your device's local web UI. For PowerShell instructions, see Set Azure Resource Manager environment.</p>
<p>Unable to get endpoints from the cloud. Ensure you have network connection. Error detail: <code>HTTPSConnectionPool(host='management dbg-of4k6suvvm.microsoftdatabox.com', port=30005): Max retries exceeded with url: /metadata/endpoints?api-version=2015-01-01 (Caused by SSLError(SSLError("bad handshake: Error([('SSL routines', 'tls_process_server_certificate', 'certificate verify failed')],"))))</code></p>	<p>This error appears mostly in a Mac or Linux environment. The error occurs because a PEM format certificate wasn't added to the Python certificate store.</p>

Troubleshoot general issues with Azure Resource Manager

For general issues with Azure Resource Manager, make sure that your device and the client are configured properly. For end-to-end procedures, see [Connect to Azure Resource Manager on your Azure Stack Edge Pro GPU device](#).

Verify the device is configured properly

- From the local UI, verify that the device network is configured correctly.
- [Verify that certificates are updated for all the endpoints](#).
- Get the Azure Resource Manager management and login endpoint from the **Device** page in local UI.
- Verify that the device is activated and registered in Azure.

Verify the client is configured properly

- [Validate that the correct PowerShell version is installed](#).
- [Validate that the correct PowerShell modules are installed](#).
- Validate that Azure Resource Manager and login endpoints are reachable. You can try to ping the endpoints. For example:

```
ping management.28bmdw2-bb9.microsoftdatabox.com ping login.28bmdw2-bb9.microsoftdatabox.com
```

If they aren't reachable, [add DNS / host file entries](#).

- [Validate that client certificates are installed](#).
- If you're using PowerShell, enable the debug preference to see detailed messages by running this PowerShell command:

```
$debugPreference = "Continue"
```

Next steps

- [Troubleshoot device activation issues](#).
- [Troubleshoot device issues](#).

What are certificates on Azure Stack Edge Pro GPU?

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the types of certificates that can be installed on your Azure Stack Edge Pro GPU device. The article also includes the details for each certificate type.

About certificates

A certificate provides a link between a **public key** and an entity (such as domain name) that has been **signed** (verified) by a trusted third party (such as a **certificate authority**). A certificate provides a convenient way of distributing trusted public encryption keys. Certificates thereby ensure that your communication is trusted and that you're sending encrypted information to the right server.

Deploying certificates on device

On your Azure Stack Edge device, you can use the self-signed certificates or bring your own certificates.

- **Device-generated certificates:** When your device is initially configured, self-signed certificates are automatically generated. If needed, you can regenerate these certificates via the local web UI. Once the certificates are regenerated, download and import the certificates on the clients used to access your device.
- **Bring your own certificates:** Optionally, you can bring your own certificates. There are guidelines that you need to follow if you plan to bring your own certificates.
 - Start by understanding the types of the certificates that can be used with your Azure Stack Edge device in this article.
 - Next, review the [Certificate requirements for each type of certificate](#).
 - You can then [Create your certificates via Azure PowerShell](#) or [Create your certificates via Readiness Checker tool](#).
 - Finally, [Convert the certificates to appropriate format](#) so that they are ready to upload on to your device.
 - [Upload your certificates](#) on the device.
 - [Import the certificates on the clients](#) accessing the device.

Types of certificates

The various types of certificates that you can bring for your device are as follows:

- Signing certificates
 - Root CA
 - Intermediate
- Node certificates
- Endpoint certificates
 - Azure Resource Manager certificates
 - Blob storage certificates
- Local UI certificates

- IoT device certificates
- Kubernetes certificates
 - Edge Container Registry certificate
 - Kubernetes dashboard certificate
- Wi-Fi certificates
- VPN certificates
- Encryption certificates
 - Support session certificates

Each of these certificates are described in detail in the following sections.

Signing chain certificates

These are the certificates for the authority that signs the certificates or the signing certificate authority.

Types

These certificates could be root certificates or the intermediate certificates. The root certificates are always self-signed (or signed by itself). The intermediate certificates are not self-signed and are signed by the signing authority.

Caveats

- The root certificates should be signing chain certificates.
- The root certificates can be uploaded on your device in the following format:
 - DER – These are available as a `.cer` file extension.
 - Base-64 encoded – These are available as `.cer` file extension.
 - P7b – This format is used only for signing chain certificates that includes the root and intermediate certificates.
- Signing chain certificates are always uploaded before you upload any other certificates.

Node certificates

All the nodes in your device are constantly communicating with each other and therefore need to have a trust relationship. Node certificates provide a way to establish that trust. Node certificates also come into play when you are connecting to the device node using a remote PowerShell session over https.

Caveats

- The node certificate should be provided in `.pfx` format with a private key that can be exported.
- You can create and upload 1 wildcard node certificate or 4 individual node certificates.
- A node certificate must be changed if the DNS domain changes but the device name does not change. If you are bringing your own node certificate, then you can't change the device serial number, you can only change the domain name.
- Use the following table to guide you when creating a node certificate.

TYPE	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAME (SAN)	SUBJECT NAME EXAMPLE
Node	<NodeSerialNo>. <DnsDomain>	*.<DnsDomain> <NodeSerialNo>. <DnsDomain>	mydevice1.microsoftdatabox.com

Endpoint certificates

For any endpoints that the device exposes, a certificate is required for trusted communication. The endpoint certificates include those required when accessing the Azure Resource Manager and the blob storage via the REST APIs.

When you bring in a signed certificate of your own, you also need the corresponding signing chain of the certificate. For the signing chain, Azure Resource Manager, and the blob certificates on the device, you will need the corresponding certificates on the client machine also to authenticate and communicate with the device.

Caveats

- The endpoint certificates need to be in `.pfx` format with a private key. Signing chain should be DER format (`.cer` file extension).
- When you bring your own endpoint certificates, these can be as individual certificates or multidomain certificates.
- If you are bringing in signing chain, the signing chain certificate must be uploaded before you upload an endpoint certificate.
- These certificates must be changed if the device name or the DNS domain names change.
- A wildcard endpoint certificate can be used.
- The properties of the endpoint certificates are similar to those of a typical SSL certificate.
- Use the following table when creating an endpoint certificate:

TYPE	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAME (SAN)	SUBJECT NAME EXAMPLE
Azure Resource Manager	<code>management.<Device name>.<Dns Domain></code>	<code>login.<Device name>.<Dns Domain></code> <code>management.<Device name>.<Dns Domain></code>	<code>management.mydevice1.microsoftdatabox.com</code>
Blob storage	<code>*.blob.<Device name>.<Dns Domain></code>	<code>*.blob.<Device name>.<Dns Domain></code>	<code>*.blob.mydevice1.microsoftdatabox.com</code>
Multi-SAN single certificate for both endpoints	<code><Device name>.<dnsdomain></code>	<code><Device name>.<dnsdomain></code> <code>login.<Device name>.<Dns Domain></code> <code>management.<Device name>.<Dns Domain></code> <code>*.blob.<Device name>.<Dns Domain></code>	<code>mydevice1.microsoftdatabox.com</code>

Local UI certificates

You can access the local web UI of your device via a browser. To ensure that this communication is secure, you can upload your own certificate.

Caveats

- The local UI certificate is also uploaded in a `.pfx` format with a private key that can be exported.
- After you upload the local UI certificate, you will need to restart the browser and clear the cache. Refer to the specific instructions for your browser.

TYPE	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAME (SAN)	SUBJECT NAME EXAMPLE
------	-------------------	--------------------------------	----------------------

TYPE	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAME (SAN)	SUBJECT NAME EXAMPLE
Local UI	<Device name>. <DnsDomain>	<Device name>. <DnsDomain>	mydevice1.microsoftdatabox.com

IoT Edge device certificates

Your device is also an IoT device with the compute enabled by an IoT Edge device connected to it. For any secure communication between this IoT Edge device and the downstream devices that may connect to it, you can also upload IoT Edge certificates.

The device has self-signed certificates that can be used if you want to use only the compute scenario with the device. If the device is however connected to downstream devices, then you'll need to bring your own certificates.

There are three IoT Edge certificates that you need to install to enable this trust relation:

- **Root certificate authority or the owner certificate authority**
- **Device certificate authority**
- **Device key certificate**

Caveats

- The IoT Edge certificates are uploaded in `.pem` format.

For more information on IoT Edge certificates, see [Azure IoT Edge certificate details](#) and [Create IoT Edge production certificates](#).

Kubernetes certificates

The following Kubernetes certificates may be used with your Azure Stack Edge device.

- **Edge container registry certificate:** If your device has an Edge container registry, then you'll need an Edge Container Registry certificate for secure communication with the client that is accessing the registry on the device.
- **Dashboard endpoint certificate:** You'll need a dashboard endpoint certificate to access the Kubernetes dashboard on your device.

Caveats

- The Edge Container Registry certificate should:
 - Be a PEM format certificate.
 - Contain either Subject Alternative Name (SAN) or CName (CN) of type: `*.<endpoint suffix>` or `ecr.<endpoint suffix>`. For example: `*.dbe-1d6phq2.microsoftdatabox.com` OR `ecr.dbe-1d6phq2.microsoftdatabox.com`
- The dashboard certificate should:
 - Be a PEM format certificate.
 - Contain either Subject Alternative Name (SAN) or CName (CN) of type: `*.<endpoint-suffix>` or `kubernetes-dashboard.<endpoint-suffix>`. For example: `*.dbe-1d6phq2.microsoftdatabox.com` OR `kubernetes-dashboard.dbe-1d6phq2.microsoftdatabox.com`.

VPN certificates

If VPN (Point-to-site) is configured on your device, you can bring your own VPN certificate to ensure the communication is trusted. The root certificate is installed on the Azure VPN Gateway and the client certificates are installed on each client computer that connects to a virtual network using Point-to-Site.

Caveats

- The VPN certificate must be uploaded as a `.pfx` format with a private key.
- The VPN certificate is not dependant on the device name, device serial number, or device configuration. It only requires the external FQDN.
- Make sure that the client OID is set.

For more information, see [Generate and export certificates for Point-to-Site using PowerShell](#).

Wi-Fi certificates

If your device is configured to operate on a WPA2-Enterprise wireless network, then you will also need a Wi-Fi certificate for any communication that occurs over the wireless network.

Caveats

- The Wi-Fi certificate must be uploaded as a `.pfx` format with a private key.
- Make sure that the client OID is set.

Support session certificates

If your device is experiencing any issues, then to troubleshoot those issues, a remote PowerShell Support session may be opened on the device. To enable a secure, encrypted communication over this Support session, you can upload a certificate.

Caveats

- Make sure that the corresponding `.pfx` certificate with private key is installed on the client machine using the decryption tool.
- Verify that the **Key Usage** field for the certificate is not **Certificate Signing**. To verify this, right-click the certificate, choose **Open** and in the **Details** tab, find **Key Usage**.
- The Support session certificate must be provided as DER format with a `.cer` extension.

Next steps

[Review certificate requirements](#).

Certificate requirements

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes the certificate requirements that must be met before certificates can be installed on your Azure Stack Edge Pro device. The requirements are related to PFX certificates, issuing authority, certificate subject name and subject alternative name, and supported certificate algorithms.

Certificate issuing authority

Certificate issuing requirements are as follows:

- Certificates must be issued from either an internal certificate authority or a public certificate authority.
- The use of self-signed certificates is not supported.
- The certificate's *Issued to*:field must not be the same as its *Issued by*:field except for Root CA certificates.

Certificate algorithms

Only the Rivest–Shamir–Adleman (RSA) certificates are supported with your device. Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are not supported.

Certificates that contain an RSA public key are referred to as RSA certificates. Certificates that contain an Elliptic Curve Cryptographic (ECC) public key are referred to as ECDSA (Elliptic Curve Digital Signature Algorithm) certificates.

Certificate algorithm requirements are as follows:

- Certificates must use the RSA key algorithm.
- Only RSA certificates with Microsoft RSA/Schannel Cryptographic Provider are supported.
- The certificate signature algorithm cannot be SHA1.
- Minimum key size is 4096.

Certificate subject name and subject alternative name

Certificates must meet the following subject name and subject alternative name requirements:

- You can either use a single certificate covering all namespaces in the certificate's Subject Alternative Name (SAN) fields. Alternatively, you can use individual certificates for each of the namespaces. Both approaches require using wild cards for endpoints where required, such as binary large object (Blob).
- Ensure that the subject names (common name in the subject name) is part of subject alternative names in the subject alternative name extension.
- You can use a single wildcard certificate covering all name spaces in the certificate's SAN fields.
- Use the following table when creating an endpoint certificate:

TYPE	SUBJECT NAME (SN)	SUBJECT ALTERNATIVE NAME (SAN)	SUBJECT NAME EXAMPLE
------	-------------------	--------------------------------	----------------------

Type	Subject Name (SN)	Subject Alternative Name (SAN)	Subject Name Example
Azure Resource Manager	management.<Device name>.<Dns Domain>	login.<Device name>.<Dns Domain> management.<Device name>.<Dns Domain>	management.mydevice1.microsoftdatabox.com
Blob storage	*.blob.<Device name>.<Dns Domain>	*.blob.<Device name>.<Dns Domain>	*.blob.mydevice1.microsoftdatabox.com
Local UI	<Device name>.<DnsDomain>	<Device name>.<DnsDomain>	mydevice1.microsoftdatabox.com
Multi-SAN single certificate for both endpoints	<Device name>.<dnsdomain>	<Device name>.<dnsdomain> login.<Device name>.<Dns Domain> management.<Device name>.<Dns Domain> *.blob.<Device name>.<Dns Domain>	mydevice1.microsoftdatabox.com
Node	<NodeSerialNo>.<DnsDomain>	*.<DnsDomain> <NodeSerialNo>.<DnsDomain>	mydevice1.microsoftdatabox.com
VPN	AzureStackEdgeVPNCertificate*<DnsDomain> * AzureStackEdgeVPNCertificate is hardcoded.	*.<DnsDomain> <AzureStackVPN>.<DnsDomain>	edgevpncertificate.microsoftdatabox.com

PFX certificate

The PFX certificates installed on your Azure Stack Edge Pro device should meet the following requirements:

- When you get your certificates from the SSL authority, make sure that you get the full signing chain for the certificates.
- When you export a PFX certificate, make sure that you have selected the **Include all certificates in the chain, if possible** option.
- Use a PFX certificate for endpoint, local UI, node, VPN, and Wi-Fi as both the public and private keys are required for Azure Stack Edge Pro. The private key must have the local machine key attribute set.
- The certificate's PFX Encryption should be 3DES. This is the default encryption used when exporting from a Windows 10 client or Windows Server 2016 certificate store. For more information related to 3DES, see [Triple DES](#).
- The certificate PFX files must have valid *Digital Signature* and *KeyEncipherment* values in the *Key Usage* field.
- The certificate PFX files must have the values *Server Authentication (1.3.6.1.5.5.7.3.1)* and *Client Authentication (1.3.6.1.5.5.7.3.2)* in the *Enhanced Key Usage* field.
- The passwords to all certificate PFX files must be the same at the time of deployment if you are using the Azure Stack Readiness Checker Tool. For more information, see [Create certificates for your Azure Stack Edge Pro using Azure Stack Hub Readiness Checker tool](#).
- The password to the certificate PFX must be a complex password. Make a note of this password because it is used as a deployment parameter.

- Use only RSA certificates with the Microsoft RSA/Schannel Cryptographic provider.

For more information, see [Export PFX certificates with private key](#).

Next steps

- Create certificates for your device
 - Via [Azure PowerShell cmdlets](#)
 - Via [Azure Stack Hub Readiness Checker tool](#).

Use certificates with Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the procedure to create your own certificates using the Azure PowerShell cmdlets. The article includes the guidelines that you need to follow if you plan to bring your own certificates on Azure Stack Edge device.

Certificates ensure that the communication between your device and clients accessing it is trusted and that you're sending encrypted information to the right server. When your Azure Stack Edge device is initially configured, self-signed certificates are automatically generated. Optionally, you can bring your own certificates.

You can use one of the following methods to create your own certificates for the device:

- Use the Azure PowerShell cmdlets.
- Use the Azure Stack Hub Readiness Checker tool to create certificate signing requests (CSRs) that would help your certificate authority issue you certificates.

This article only covers how to create your own certificates using the Azure PowerShell cmdlets.

Prerequisites

Before you bring your own certificates, make sure that:

- You are familiar with the [Types of the certificates that can be used with your Azure Stack Edge device](#).
- You have reviewed the [Certificate requirements for each type of certificate](#).

Create certificates

The following section describes the procedure to create signing chain and endpoint certificates.

Certificate workflow

You will have a defined way to create the certificates for the devices operating in your environment. You can use the certificates provided to you by your IT administrator.

For development or test purposes only, you can also use Windows PowerShell to create certificates on your local system. While creating the certificates for the client, follow these guidelines:

1. You can create any of the following types of certificates:
 - Create a single certificate valid for use with a single fully qualified domain name (FQDN). For example, *mydomain.com*.
 - Create a wildcard certificate to secure the main domain name and multiple sub domains as well. For example, **.mydomain.com*.
 - Create a subject alternative name (SAN) certificate that will cover multiple domain names in a single certificate.
2. If you are bringing your own certificate, you will need a root certificate for the signing chain. See steps to [Create signing chain certificates](#).

3. You can next create the endpoint certificates for the local UI of the appliance, blob, and Azure Resource Manager. You can create 3 separate certificates for the appliance, blob, and Azure Resource Manager, or you can create one certificate for all the 3 endpoints. For detailed steps, see [Create signing and endpoint certificates](#).

4. Whether you are creating 3 separate certificates or one certificate, specify the subject names (SN) and subject alternative names (SAN) as per the guidance provided for each certificate type.

Create signing chain certificate

Create these certificates via Windows PowerShell running in administrator mode. **The certificates created this way should be used for development or test purposes only.**

The signing chain certificate needs to be created only once. The other end point certificates will refer to this certificate for signing.

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=RootCert" -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\LocalMachine\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

Create signed endpoint certificates

Create these certificates via Windows PowerShell running in administrator mode.

In these examples, endpoints certificates are created for a device with: - Device name: **DBE-HWDC1T2** - DNS domain: **microsoftdatabox.com**

Replace with the name and DNS domain for your device to create certificates for your device.

Blob endpoint certificate

Create a certificate for the Blob endpoint in your personal store.

```
$AppName = "DBE-HWDC1T2"  
$domain = "microsoftdatabox.com"  
  
New-SelfSignedCertificate -Type Custom -DnsName "*.$AppName.$domain" -Subject  
"CN=*.blob.$AppName.$domain" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -  
CertStoreLocation "Cert:\LocalMachine\My" -Signer $cert -KeySpec KeyExchange -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Azure Resource Manager endpoint certificate

Create a certificate for the Azure Resource Manager endpoints in your personal store.

```
$AppName = "DBE-HWDC1T2"  
$domain = "microsoftdatabox.com"  
  
New-SelfSignedCertificate -Type Custom -DnsName "management.$AppName.$domain", "login.$AppName.$domain" -  
Subject "CN=management.$AppName.$domain" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -  
CertStoreLocation "Cert:\LocalMachine\My" -Signer $cert -KeySpec KeyExchange -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Device local web UI certificate

Create a certificate for the local web UI of the device in your personal store.

```
$AppName = "DBE-HWDC1T2"
$domain = "microsoftdatabox.com"

New-SelfSignedCertificate -Type Custom -DnsName "$AppName.$domain" -Subject "CN=$AppName.$domain" -
KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation
"Cert:\LocalMachine\My" -Signer $cert -KeySpec KeyExchange -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Single multi-SAN certificate for all endpoints

Create a single certificate for all the endpoints in your personal store.

```
$AppName = "DBE-HWDC1T2"
$domain = "microsoftdatabox.com"
$DeviceSerial = "HWDC1T2"

New-SelfSignedCertificate -Type Custom -DnsName
"$AppName.$domain","$DeviceSerial.$domain","management.$AppName.$domain","login.$AppName.$domain","*.blob.$A
ppName.$domain" -Subject "CN=$AppName.$domain" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength
2048 -CertStoreLocation "Cert:\LocalMachine\My" -Signer $cert -KeySpec KeyExchange -TextExtension
@("2.5.29.37={text}1.3.6.1.5.5.7.3.1")
```

Once the certificates are created, the next step is to upload the certificates on your Azure Stack Edge Pro GPU device.

Next steps

[Upload certificates on your device.](#)

Create certificates for your Azure Stack Edge Pro GPU using Azure Stack Hub Readiness Checker tool

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to create certificates for your Azure Stack Edge Pro using the Azure Stack Hub Readiness Checker tool.

Using Azure Stack Hub Readiness Checker tool

Use the Azure Stack Hub Readiness Checker tool to create Certificate Signing Requests (CSRs) for an Azure Stack Edge Pro device deployment. You can create these requests after you place an order for the Azure Stack Edge Pro device and wait for the device to arrive.

NOTE

Use this tool only for test or development purposes and not for production devices.

You can use the Azure Stack Hub Readiness Checker tool (`AzsReadinessChecker`) to request the following certificates:

- Azure Resource Manager certificate
- Local UI certificate
- Node certificate
- Blob certificate
- VPN certificate

Prerequisites

To create CSRs for Azure Stack Edge Pro device deployment, make sure that:

- You've a client running Windows 10 or Windows Server 2016 or later.
- You've downloaded the Microsoft Azure Stack Hub Readiness Checker tool [from the PowerShell Gallery](#) on this system.
- You have the following information for the certificates:
 - Device name
 - Node serial number
 - External fully qualified domain name (FQDN)

Generate certificate signing requests

Use these steps to prepare the Azure Stack Edge Pro device certificates:

1. Run PowerShell as administrator (5.1 or later).
2. Install the Azure Stack Hub Readiness Checker tool. At the PowerShell prompt, type:

```
Install-Module -Name Microsoft.AzureStack.ReadinessChecker
```

To get the installed version, type:

```
Get-InstalledModule -Name Microsoft.AzureStack.ReadinessChecker | ft Name, Version
```

3. Create a directory for all the certificates if you don't already have one. Type:

```
New-Item "C:\certrequest" -ItemType Directory
```

4. To create a certificate request, provide the following information. If you are generating a VPN certificate, some of these inputs do not apply.

INPUT	DESCRIPTION
OutputRequestPath	The file path on your local client where you want the certificate requests to be created.
DeviceName	The name of your device in the Device page in the local web UI of your device. This field isn't required for a VPN certificate.
NodeSerialNumber	The Node serial number of the device node shown on the Overview page in the local web UI of your device. This field isn't required for a VPN certificate.
ExternalFQDN	The DNS domain value in the Device page in the local web UI of your device.
RequestType	The request type can be for MultipleCSR - different certificates for the various endpoints, or SingleCSR - a single certificate for all the endpoints. This field isn't required for a VPN certificate.

For all the certificates except the VPN certificate, type:

```
$edgeCSRparams = @{
    CertificateType = 'AzureStackEdgeDEVICE'
    DeviceName = 'myTEA1'
    NodeSerialNumber = 'VM1500-00025'
    externalFQDN = 'azurestackedge.contoso.com'
    requestType = 'MultipleCSR'
    OutputRequestPath = "C:\certrequest"
}
New-AzsCertificateSigningRequest @edgeCSRparams
```

If you are creating a VPN certificate, type:

```
$edgeCSRparams = @{
    CertificateType = 'AzureStackEdgeVPN'
    externalFQDN = 'azurestackedge.contoso.com'
    OutputRequestPath = "C:\certrequest"
}
New-AzsCertificateSigningRequest @edgeCSRparams
```

5. You will find the certificate request files in the directory you specified in the OutputRequestPath parameter above. When using the `MultipleCSR` parameter, you'll see the following four files with the `.req` extension:

FILE NAMES	TYPE OF CERTIFICATE REQUEST
Starting with your <code>DeviceName</code>	Local web UI certificate request
Starting with your <code>NodeSerialNumber</code>	Node certificate request
Starting with <code>login</code>	Azure Resource Manager Endpoint certificate request
Starting with <code>wildcard</code>	Blob storage certificate request. It contains a wildcard because it covers all the storage accounts that you may create on the device.
Starting with <code>AzureStackEdgeVPNCertificate</code>	VPN client certificate request.

You'll also see an INF folder. This contains a management.<edge-devicename> information file in clear text explaining the certificate details.

6. Submit these files to your certificate authority (either internal or public). Be sure that your CA generates certificates, using your generated request, that meet the Azure Stack Edge Pro certificate requirements for [node certificates](#), [endpoint certificates](#), and [local UI certificates](#).

Prepare certificates for deployment

The certificate files that you get from your certificate authority (CA) must be imported and exported with properties that match the certificate requirements of the Azure Stack Edge Pro device. Complete the following steps on the same system where you generated the certificate signing requests.

- To import the certificates, follow the steps in [Import certificates on the clients accessing your Azure Stack Edge Pro device](#).
- To export the certificates, follow the steps in [Export certificates from the client accessing the Azure Stack Edge Pro device](#).

Validate certificates

First, you'll generate a proper folder structure and place the certificates in the corresponding folders. Only then you'll validate the certificates using the tool.

- Run PowerShell as administrator.
- To generate the appropriate folder structure, at the prompt type:

```
New-AzsCertificateFolder -CertificateType AzureStackEdgeDevice -OutputPath  
"$ENV:USERPROFILE\Documents\AzureStackCSR"
```

- Convert the PFX password into a secure string. Type:

```
$pfxPassword = Read-Host -Prompt "Enter PFX Password" -AsSecureString
```

- Next, validate the certificates. Type:

```
Invoke-AzsCertificateValidation -CertificateType AzureStackEdgeDevice -DeviceName myteal -  
NodeSerialNumber VM1500-00025 -externalFQDN azurestackedge.contoso.com -CertificatePath  
$ENV:USERPROFILE\Documents\AzureStackCSR\AzureStackEdge -pfxPassword $pfxPassword
```

Next steps

[Upload certificates on your device.](#)

Prepare certificates to upload on your Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to convert the certificates into appropriate format for upload on your Azure Stack Edge device. This procedure is typically required when you bring your own certificates.

To know more about how to create these certificates, see [Create certificates using Azure PowerShell](#).

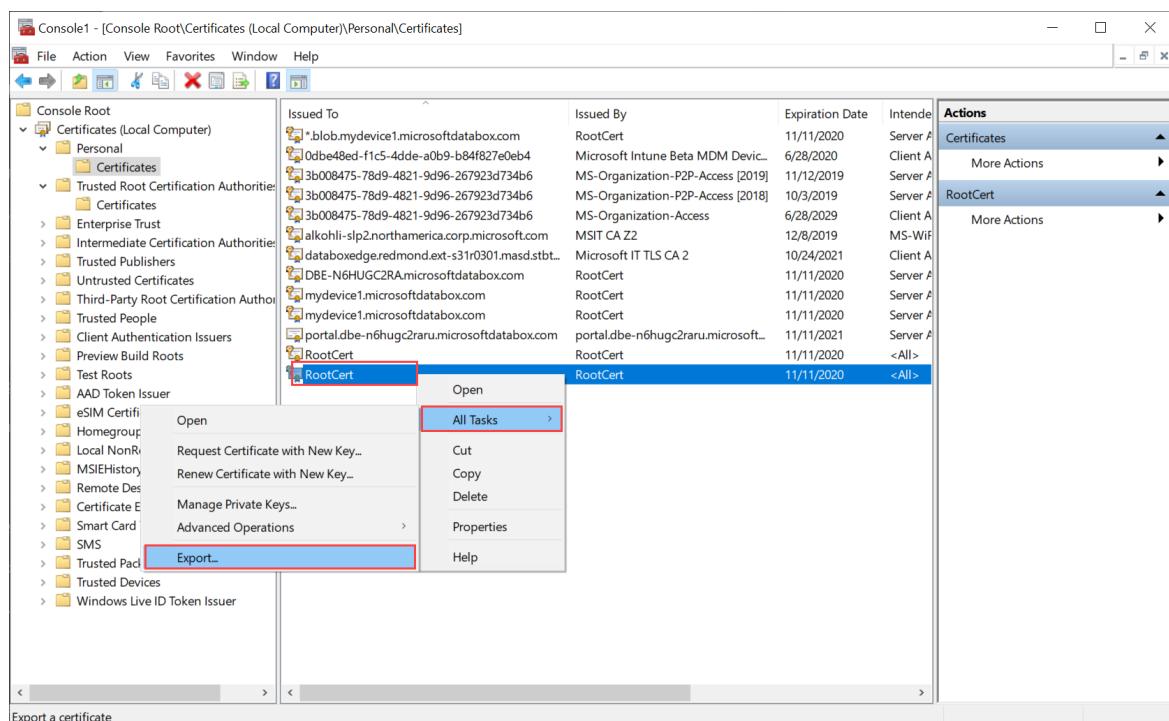
Prepare certificates

If you bring your own certificates, then the certificates that you created for your device by default reside in the **Personal store** on your client. These certificates need to be exported on your client into appropriate format files that can then be uploaded to your device.

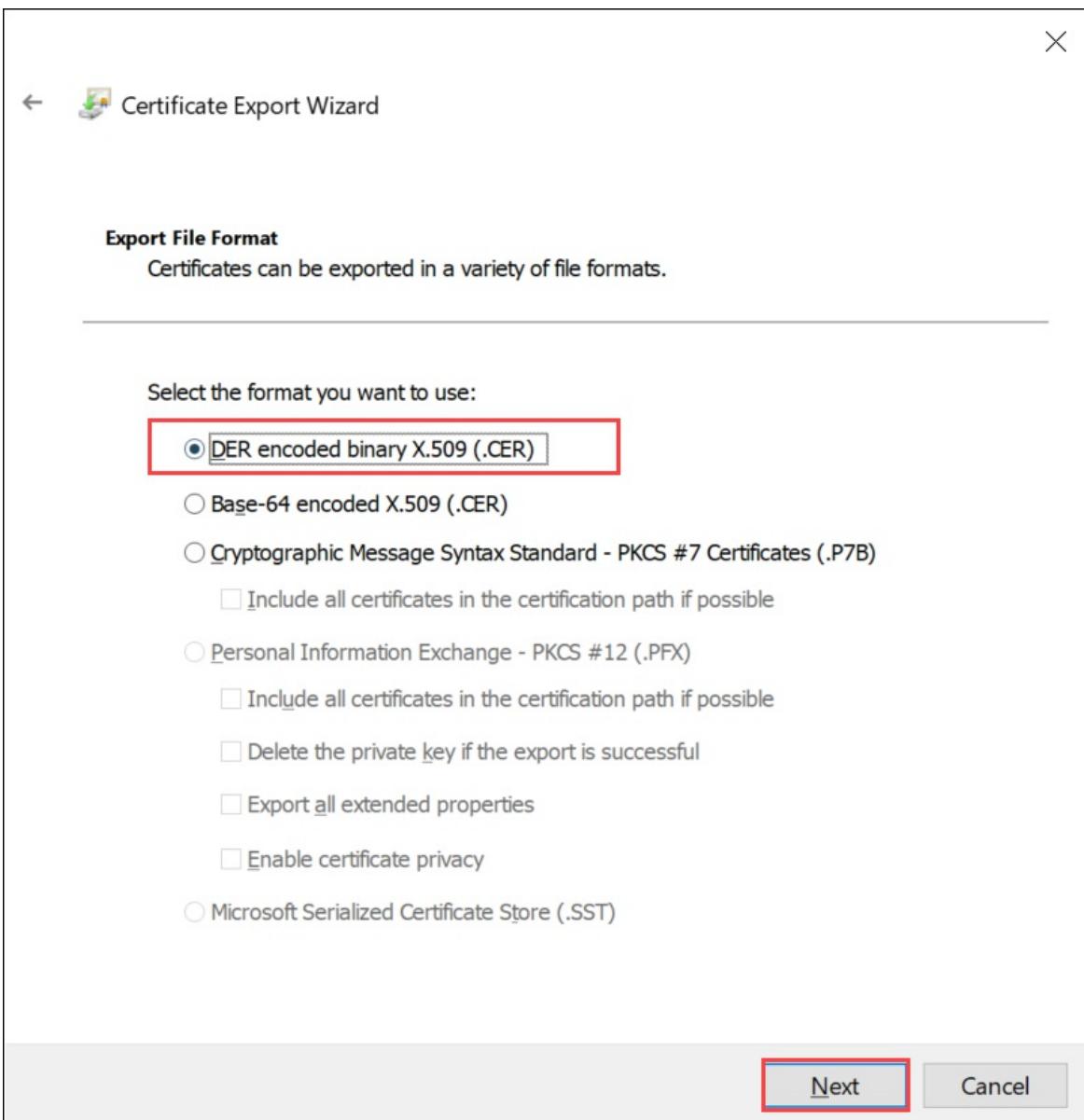
- **Prepare root certificates:** The root certificate must be exported as DER format with `.cer` extension. For detailed steps, see [Export certificates as DER format](#).
- **Prepare endpoint certificates:** The endpoint certificates must be exported as `.pfx` files with private keys. For detailed steps, see [Export certificates as .pfx file with private keys](#).

Export certificates as DER format

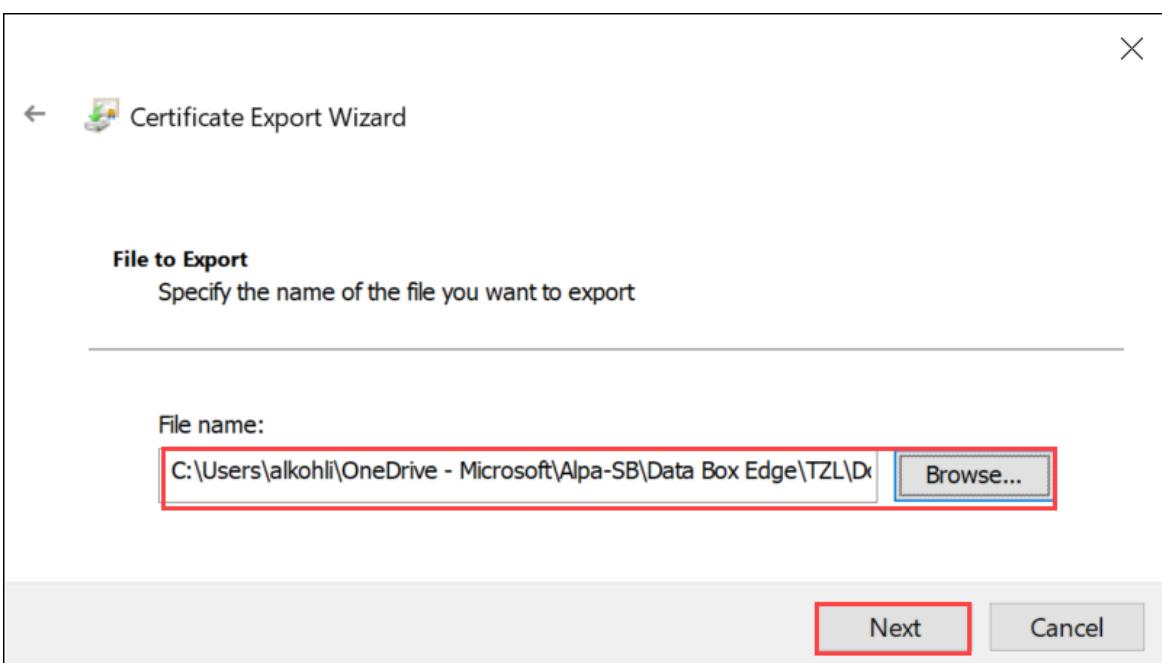
1. Run `certlm.msc` to launch the local machine certificate store.
2. In the Personal certificate store, select the root certificate. Right-click and select **All Tasks > Export...**



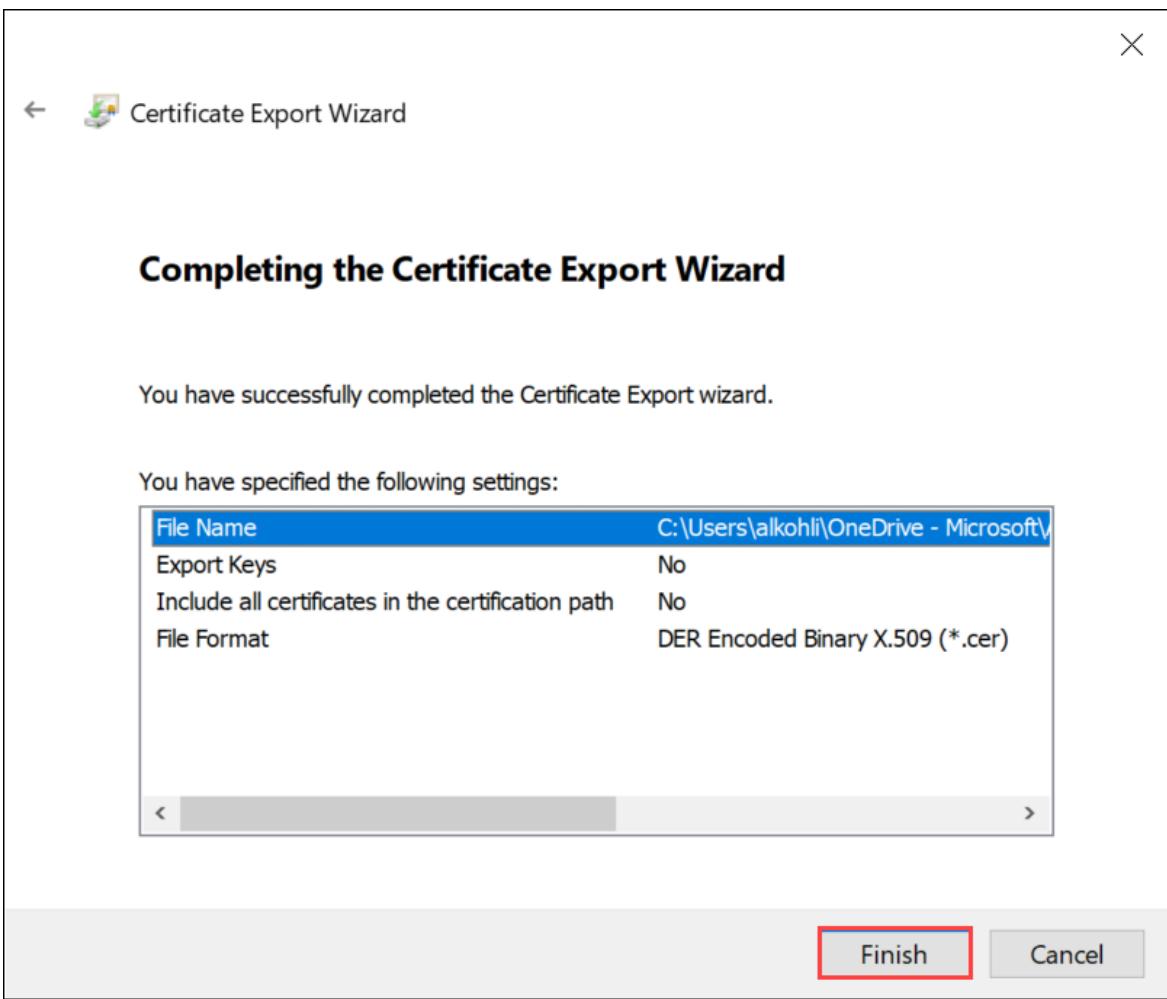
3. The certificate wizard opens. Select the format **DER encoded binary X.509 (.cer)**. Select **Next**.



4. Browse and select the location where you want to export the .cer format file.



5. Select Finish.



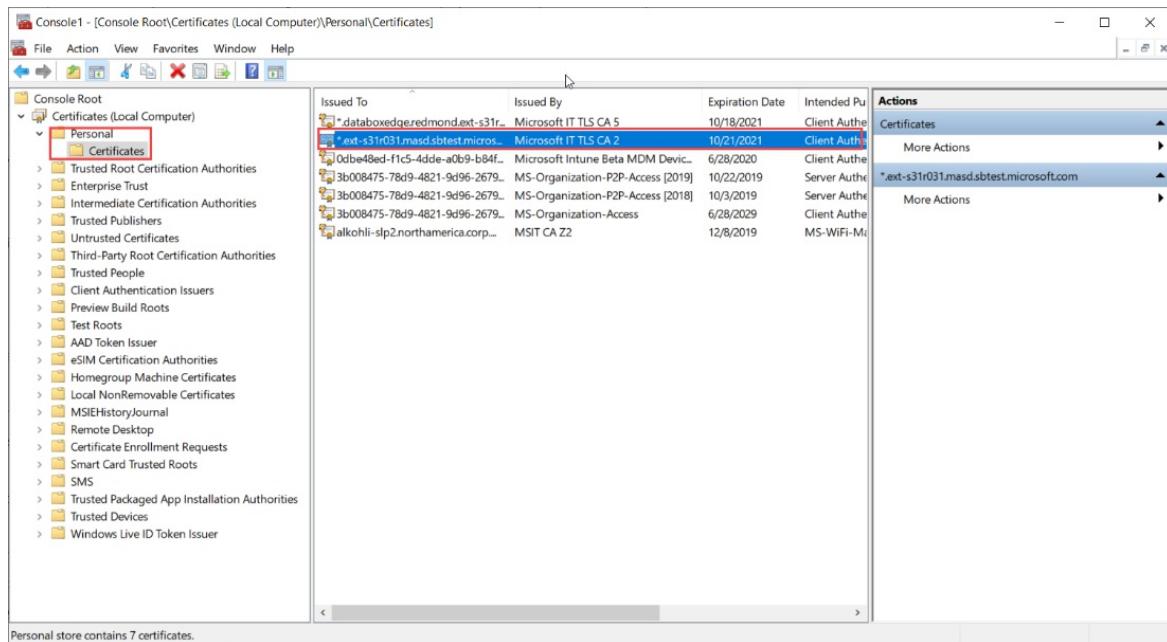
Export certificates as .pfx format with private key

Take the following steps to export an SSL certificate with private key on a Windows machine.

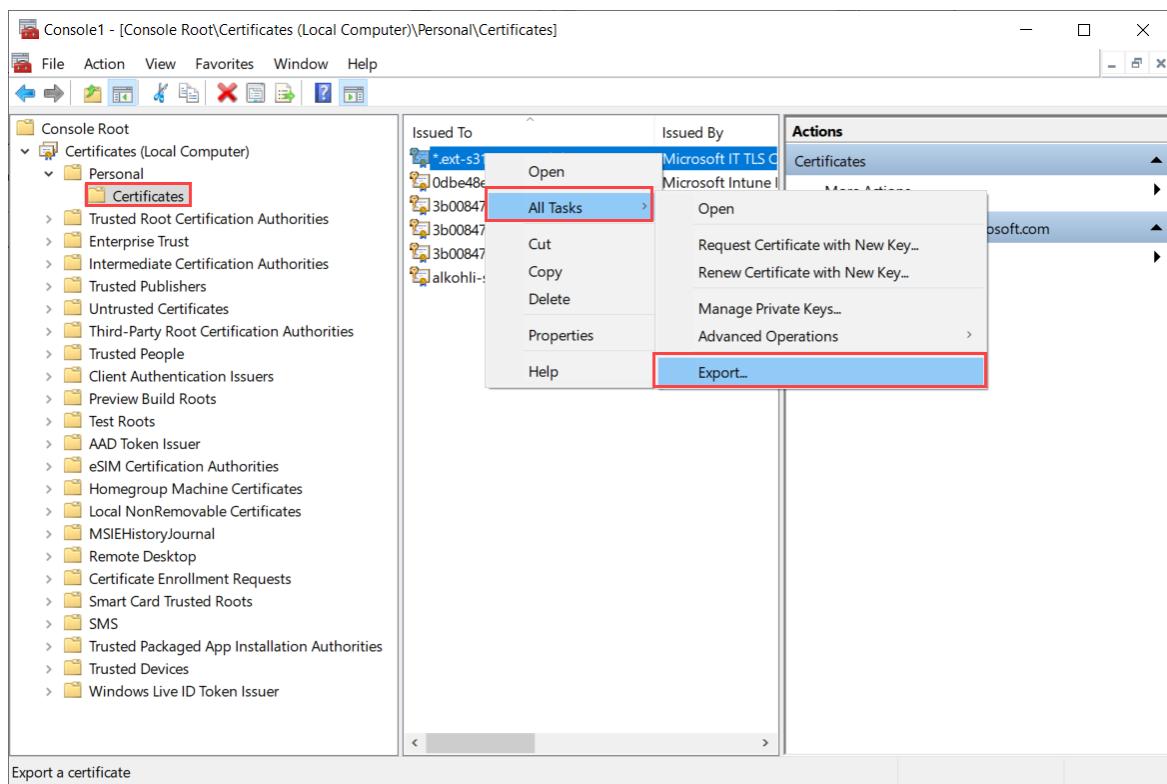
IMPORTANT

Perform these steps on the same machine that you used to create the certificate.

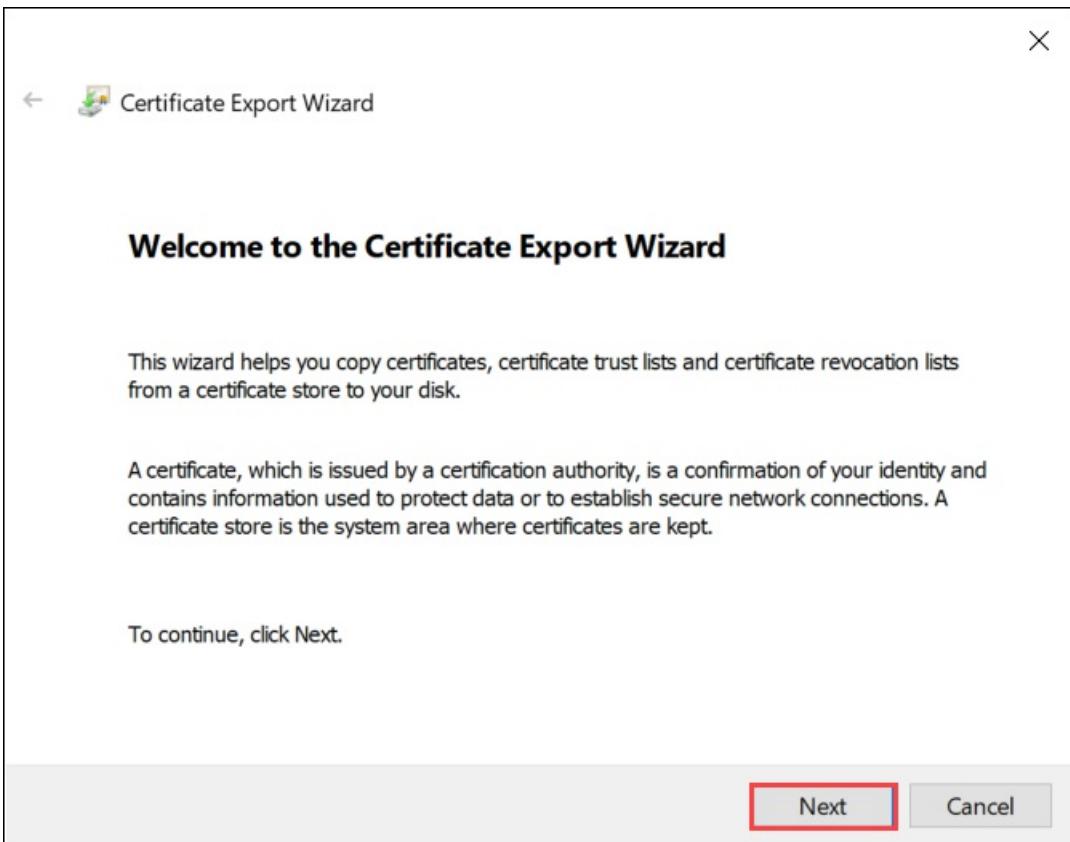
1. Run `certlm.msc` to launch the local machine certificate store.
2. Double-click on the **Personal** folder, and then on **Certificates**.



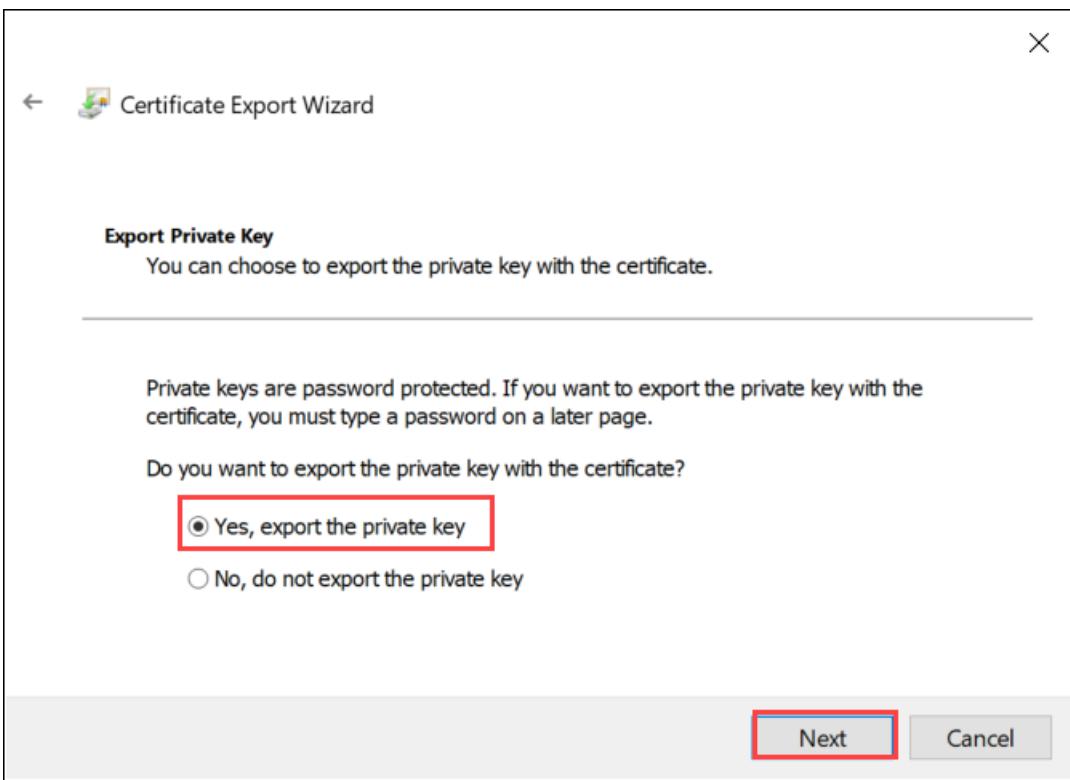
3. Right-click on the certificate you would like to back up and choose All tasks > Export....



4. Follow the Certificate Export Wizard to back up your certificate to a .pfx file.



5. Choose Yes, export the private key.

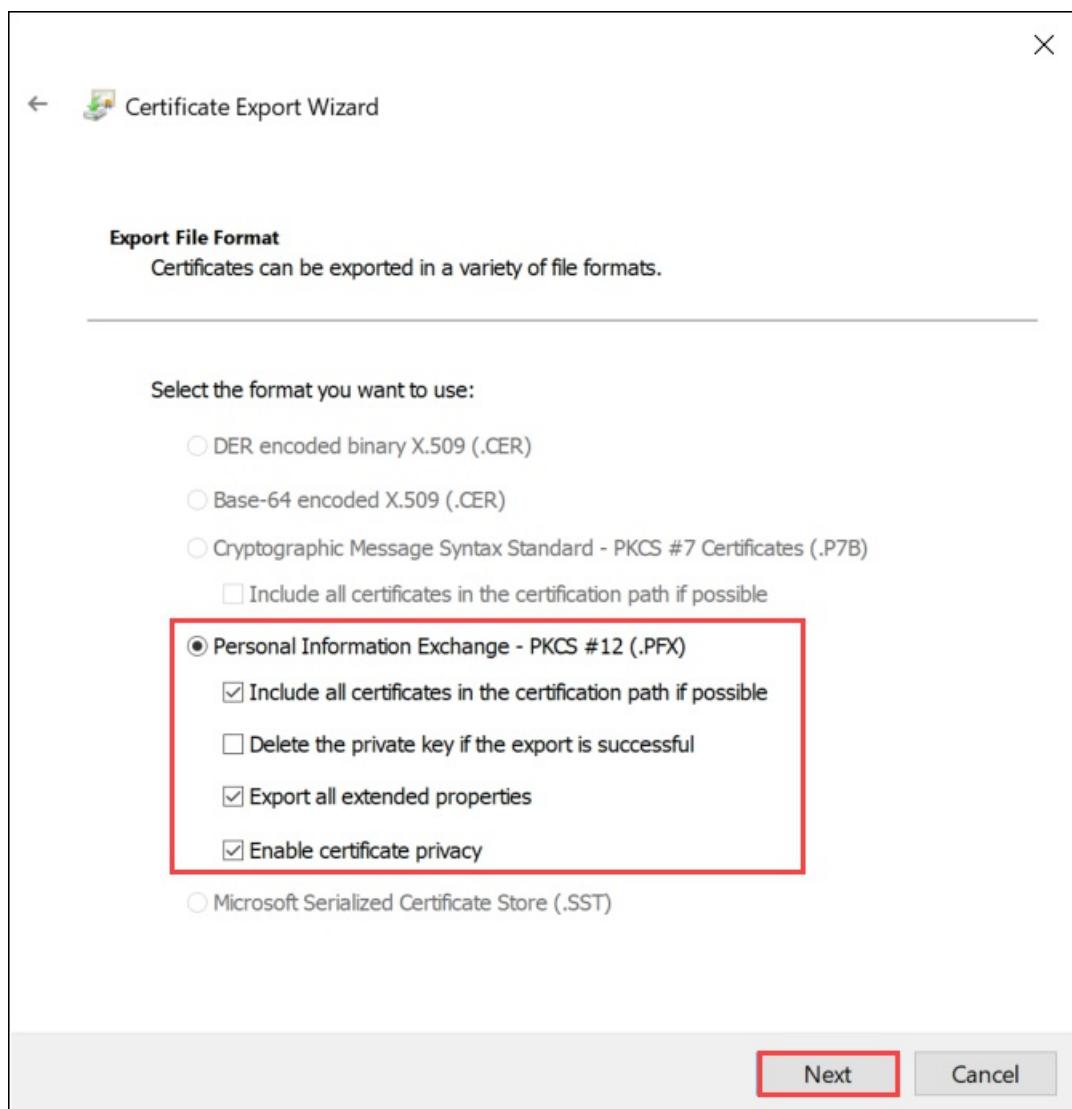


6. Choose **Include all certificates in certificate path if possible, Export all extended properties and Enable certificate privacy**.

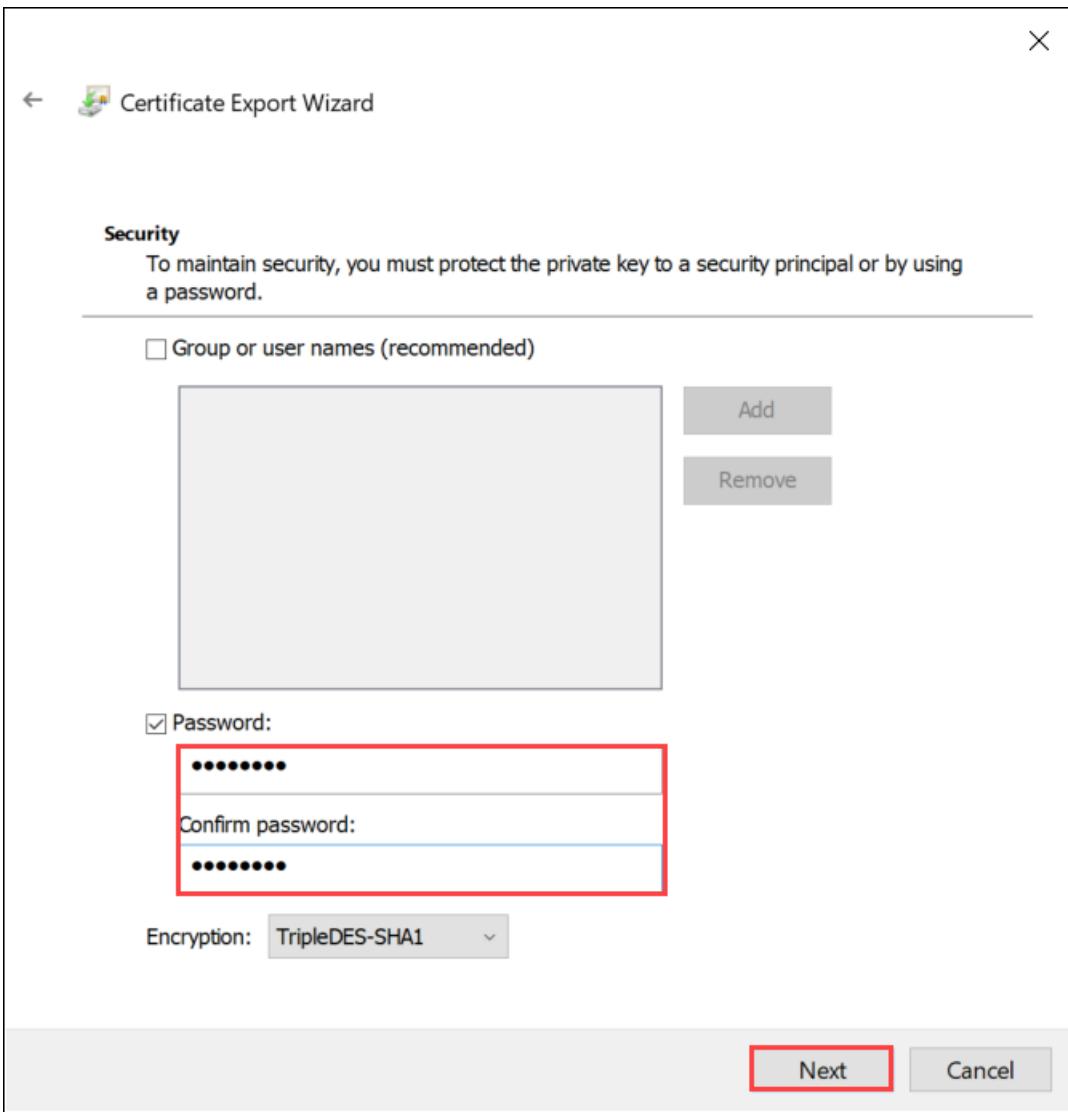
When you include all certificates in your export, you don't need to add the signing chain separately before adding that certificate when you configure certificates using the local web UI. For more information, see [Bring your own certificates](#).

IMPORTANT

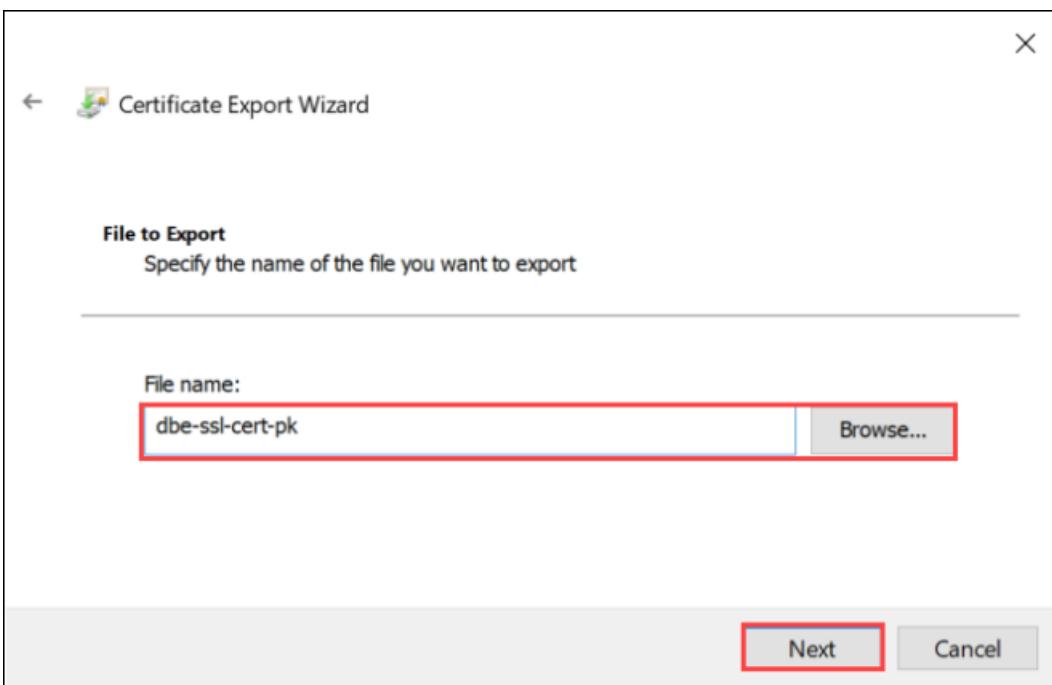
DO NOT select the Delete Private Key option if export is successful.



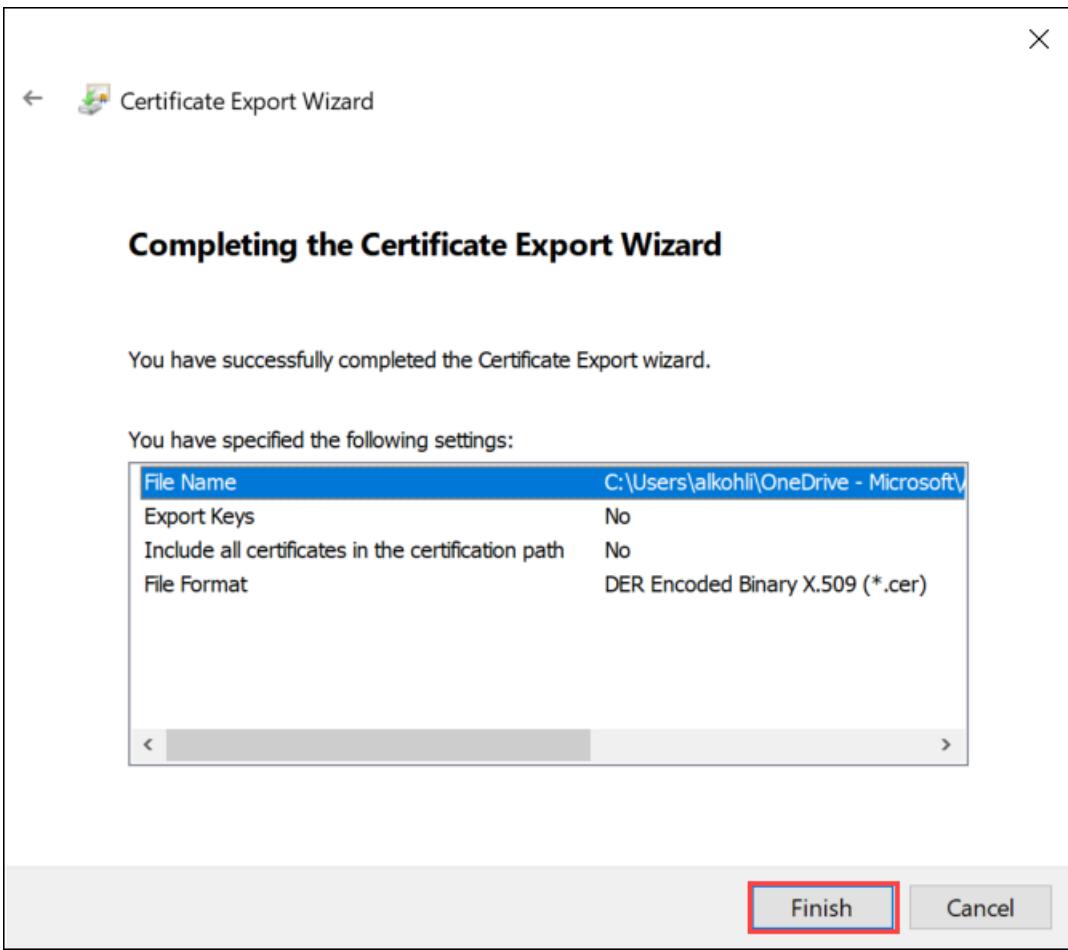
7. Enter a password you will remember. Confirm the password. The password protects the private key.



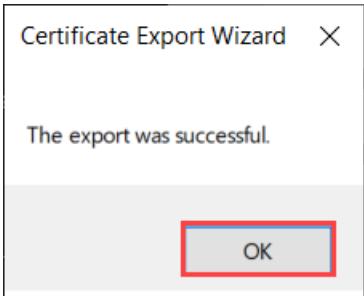
8. Choose to save the file in a set location.



9. Select Finish.



10. You receive a message that the export was successful. Select OK.



The .pfx file backup is now saved in the selected location, and is ready to be moved or stored for safekeeping.

Next steps

Learn how to [Upload certificates on your device](#).

Upload, import, export, and delete certificates on Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

To ensure secure and trusted communication between your Azure Stack Edge device and the clients connecting to it, you can use self-signed certificates or bring your own certificates. This article describes how to manage these certificates, including how to upload, import, and export these certificates. You can also view certificate expiration dates and delete your old signing certificates.

To know more about how to create these certificates, see [Create certificates using Azure PowerShell](#).

Upload certificates on your device

If you bring your own certificates, then the certificates that you created for your device by default reside in the **Personal store** on your client. These certificates need to be exported on your client into appropriate format files that can then be uploaded to your device.

Prerequisites

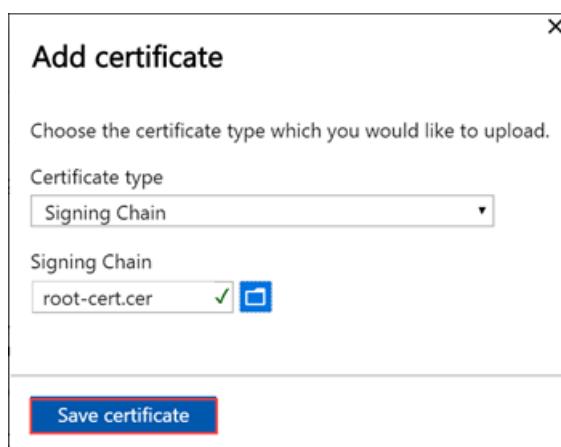
Before you upload your root certificates and endpoint certificates on to the device, make sure the certificates are exported in appropriate format.

- The root certificate must be exported as DER format with `.cer` extension. For detailed steps, see [Export certificates as DER format](#).
- The endpoint certificates must be exported as `.pfx` files with private keys. For detailed steps, see [Export certificates as .pfx file with private keys](#).

Upload certificates

To upload the root and endpoint certificates on the device, use the **+ Add certificate** option on the **Certificates** page in the local web UI. Follow these steps:

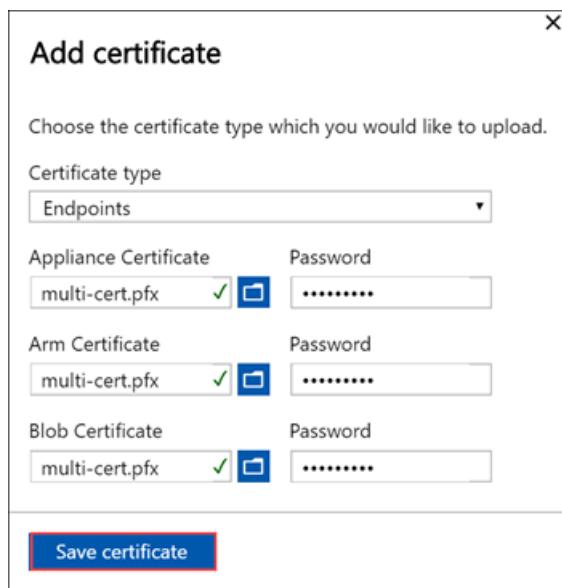
1. Upload the root certificates first. In the local web UI, go to **Certificates**.
2. Select **+ Add certificate**.



3. Save the certificate.

Upload endpoint certificate

1. Next upload the endpoint certificates.



Choose the certificate files in `.pfx` format and enter the password you supplied when you exported the certificate. The Azure Resource Manager certificate may take a few minutes to apply.

If the signing chain is not updated first, and you try to upload the endpoint certificates, then you will get an error.



Go back and upload the signing chain certificate and then upload and apply the endpoint certificates.

IMPORTANT

If the device name or the DNS domain are changed, new certificates must be created. The client certificates and the device certificates should then be updated with the new device name and DNS domain.

Upload Kubernetes certificates

The Kubernetes certificates can be for Edge Container Registry or for Kubernetes dashboard. In each case, a certificate and a key file must be uploaded. Follow these steps to create and upload Kubernetes certificates:

1. You'll use `openssl` to create the Kubernetes dashboard certificate or Edge Container Registry. Make sure to install `openssl` on the system you would use to create the certificates. On a Windows system, you can use Chocolatey to install `openssl`. After you've installed Chocolatey, open PowerShell and type:

```
choco install openssl
```

2. Use `openssl` to create these certificates. A `cert.pem` certificate file and `key.pem` key file are created.

- For Edge Container Registry, use the following command:

```
openssl req -newkey rsa:4096 -nodes -sha256 -keyout key.pem -x509 -days 365 -out cert.pem -subj "/CN=<ecr.endpoint-suffix>"
```

Here is an example output:

```
PS C:\WINDOWS\system32> openssl req -newkey rsa:4096 -nodes -sha256 -keyout key.pem -x509 -days 365 -out cert.pem -subj "/CN=ecr.dbe-1d6phq2.microsoftdatabase.com"
Generating a RSA private key
.....+++++....+++++
writing new private key to 'key.pem'
-----
PS C:\WINDOWS\system32>
```

- For Kubernetes dashboard certificate, use the following command:

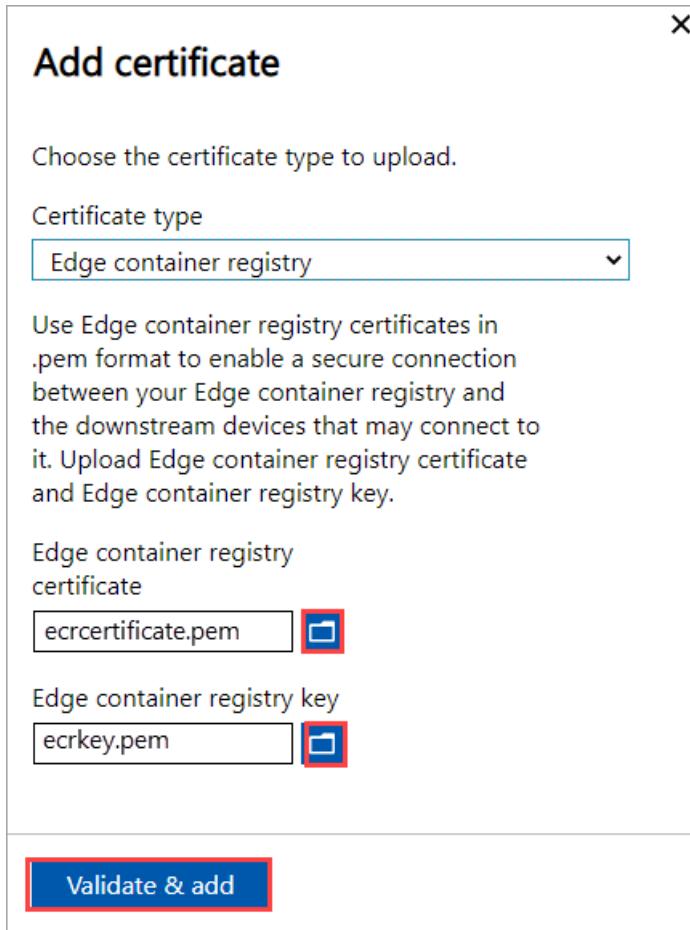
```
openssl req -newkey rsa:4096 -nodes -sha256 -keyout key.pem -x509 -days 365 -out cert.pem -subj "/CN=<<kubernetes-dashboard.endpoint-suffix> OR <endpoint-suffix>>"
```

Here is an example output:

```
PS C:\WINDOWS\system32> openssl req -newkey rsa:4096 -nodes -sha256 -keyout key.pem -x509 -days 365 -out cert.pem -subj "/CN=kubernetes-dashboard.dbe-1d8phq2.microsoftdatabase.com"
Generating a RSA private key
.....+++++....+++++
writing new private key to 'key.pem'
-----
PS C:\WINDOWS\system32>
```

3. Upload the Kubernetes certificate and the corresponding key file that you generated earlier.

- For Edge Container Registry



- For Kubernetes dashboard

Add certificate

Choose the certificate type to upload.

Certificate type

Kubernetes dashboard

Use Kubernetes dashboard certificates in .pem format to enable a secure connection to kubernetes dashboard. Upload Kubernetes dashboard certificate and Kubernetes dashboard key.

Kubernetes dashboard certificate

k8dashbdcert.pem 

Kubernetes dashboard key

k8dashbdkey.pem 

Validate & add

Import certificates on the client accessing the device

You can use the device-generated certificates or bring your own certificates. When using device-generated certificates, you must download the certificates on your client before you can import those into the appropriate certificate store. See [Download certificates to your client accessing the device](#).

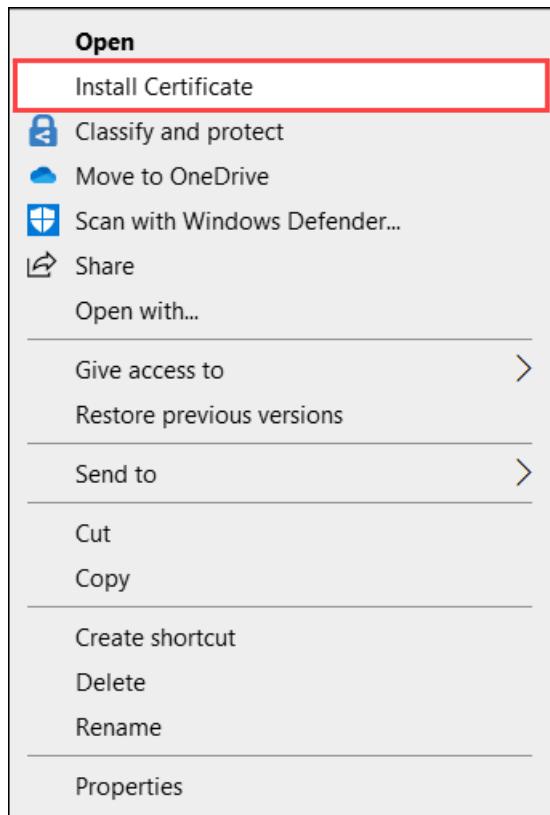
In both the cases, the certificates that you created and uploaded to your device must be imported on your Windows client (accessing the device) into the appropriate certificate store.

- The root certificate that you exported as the DER should now be imported in the **Trusted Root Certificate Authorities** on your client system. For detailed steps, see [Import certificates into the Trusted Root Certificate Authorities store](#).
- The endpoint certificates that you exported as the `.pfx` must be exported as DER with `.cer` extension. This `.cer` is then imported in the **Personal certificate store** on your system. For detailed steps, see [Import certificates into the Personal certificate store](#).

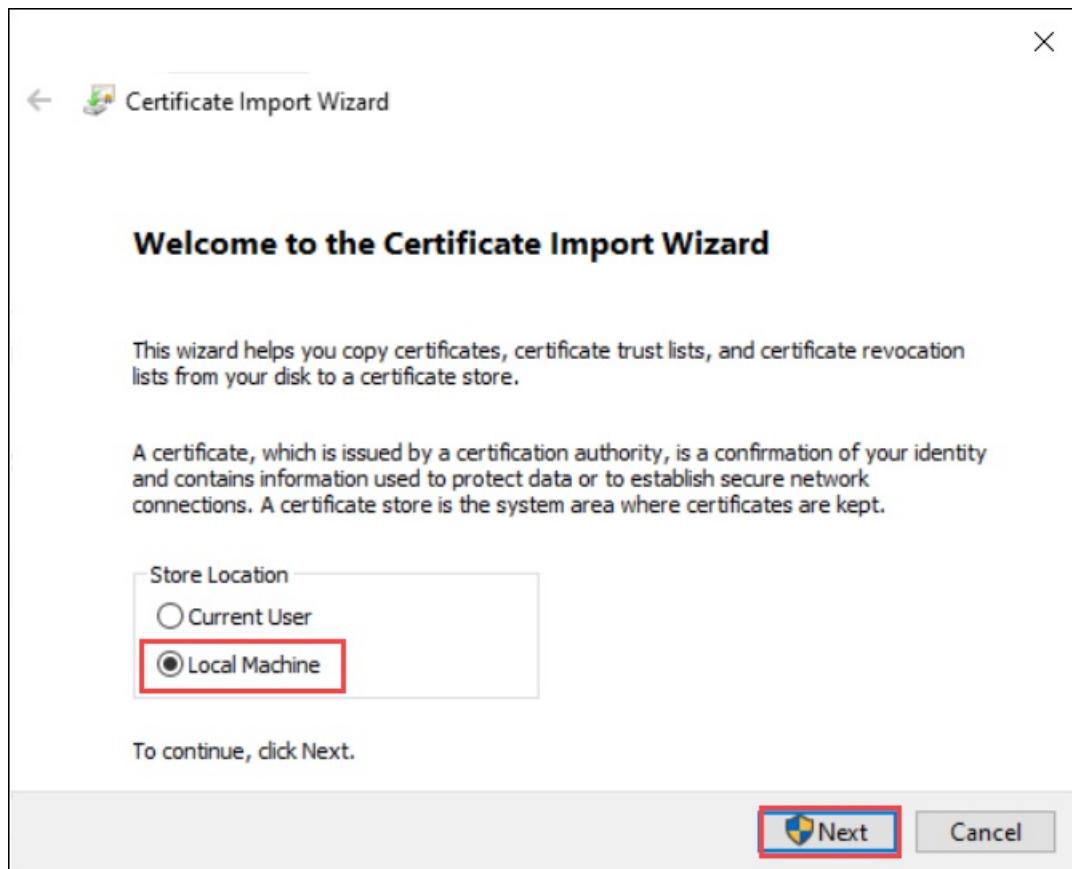
Import certificates as DER format

To import certificates on a Windows client, take the following steps:

1. Right-click the file and select **Install certificate**. This action starts the Certificate Import Wizard.

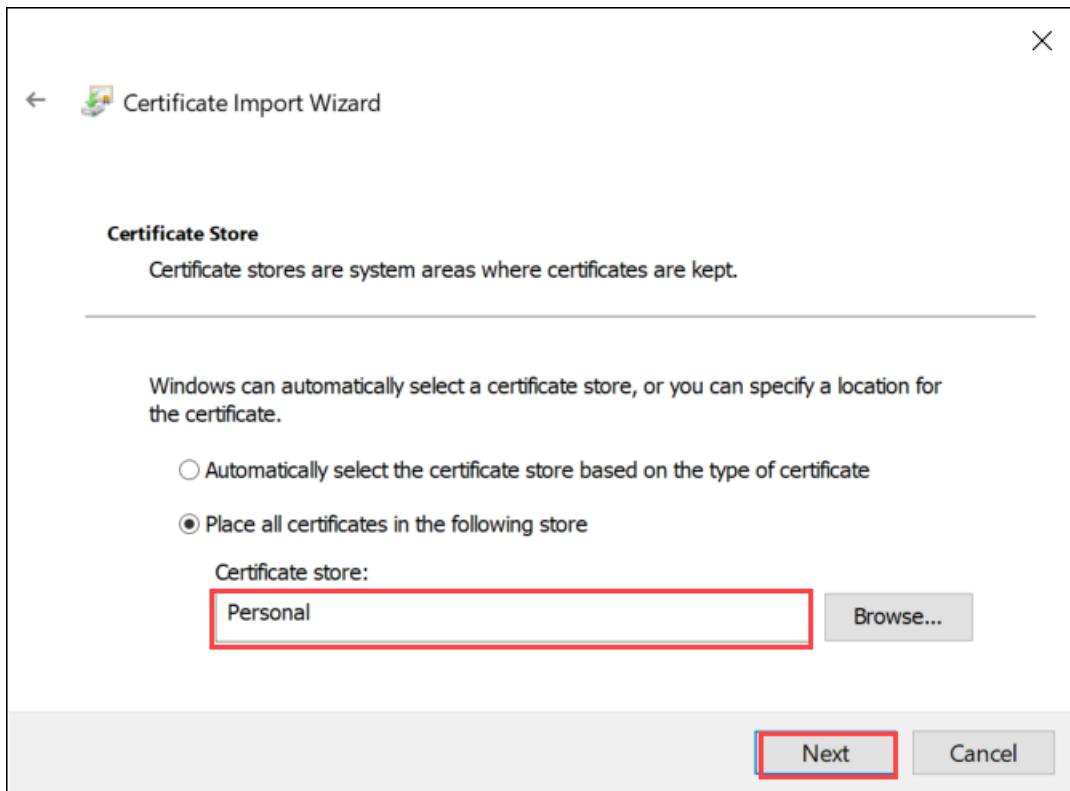


2. For **Store location**, select **Local Machine**, and then select **Next**.

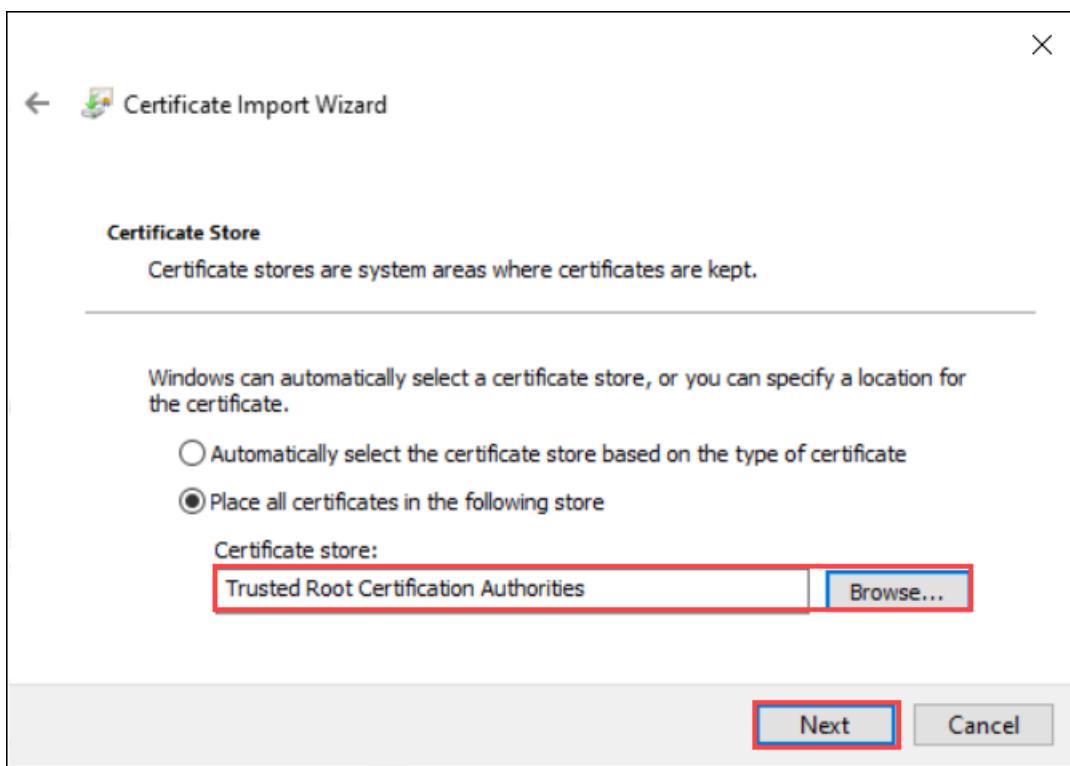


3. Select **Place all certificates in the following store**, and then select **Browse**.

- To import into personal store, navigate to the Personal store of your remote host, and then select **Next**.



- To import into trusted store, navigate to the Trusted Root Certificate Authority, and then select Next.



- Select Finish. A message to the effect that the import was successful appears.

View certificate expiry

If you bring in your own certificates, the certificates will expire typically in 1 year or 6 months. To view the expiration date on your certificate, go to the **Certificates** page in the local web UI of your device. If you select a specific certificate, you can view the expiration date on your certificate.

Delete signing chain certificate

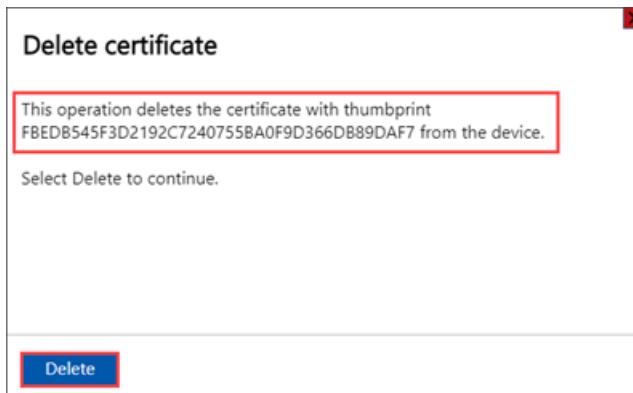
You can delete an old, expired signing chain certificate from your device. When you do, any dependent certificates in the signing chain will no longer be valid. Only signing chain certificates can be deleted.

To delete a signing chain certificate from your Azure Stack Edge device, take the following steps:

1. In the local web UI of your device, go to **CONFIGURATION > Certificates**.
2. Select the signing chain certificate you want to delete. Then select **Delete**.

Name	Status	Expiration date	Thumbprint	Download	Delete
Signing Chain	Valid	1/12/2023	FBEDB545F3D2192C7240755BA0F9D366DB89DAF7	-	Delete
Signing Chain	Valid	1/28/2023	BA84243ECCFE578CD2D475031C8F9C2AF7944267	-	Delete
Node (WIN-ICH4FTEGN45)	Valid	1/10/2024	819C926CEA0AF64CB41C3211DEB3C915B82F1B27	Download	-
Azure Resource Manager	Valid	1/10/2024	3966EE538D0890C6373A4613FAA1B94D02E77F3EA	Download	-
Blob storage	Valid	1/28/2023	9A74B97699BCD66B217D184E01A890F8BDC95FBB	-	-
Local web UI	Valid	1/10/2024	6AC507B629AE8297213610BE179963F1F25AA501	Download	-

3. On the **Delete certificate** pane, verify the certificate's thumbprint, and then select **Delete**. Certificate deletion can't be reversed.



After certificate deletion is complete, all dependent certificates in the signing chain are no longer valid.

4. To see the status updates, refresh the display. The signing chain certificate will no longer be displayed, and dependent certificates will have **Not valid** status.

Next steps

Learn how to [Troubleshoot certificate issues](#)

Troubleshooting certificate errors

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The article provides troubleshooting common certificate errors when installing certificates to your Azure Stack Edge Pro device.

Common certificate errors

The following table shows common certificate errors and detailed information about these errors and possible solutions:

NOTE

Occurrences of "{0}, {1}, ... , {n}" indicate positional parameters. The positional parameters will take values depending on the certificates that you are using.

ERROR CODE	DESCRIPTION
CertificateManagement_UntrustedCertificate	Certificate with subject name {0} has certificate chain broken. Upload the signing chain certificate before uploading this certificate.
CertificateManagement_DeviceNotRegistered	Your device is not activated. You can upload a support certificate only after activation.
CertificateManagement_ExpiredCertificate	Certificate with type {0} has expired or expires soon. Check the certificate expiration and if needed, bring in a new certificate.
CertificateManagement_FormatMismatch	Certificate format is not supported. Check the certificate format and if needed, bring in a new certificate. Expected {0}, found {1}.
CertificateManagement_GenericError	Could not perform the certificate management operation. Retry this operation in few minutes. If the problem persists, contact Microsoft Support.
CertificateManagement_HttpsBindingFailure	Certificate with subject name {0} failed to create a secure https channel. Check the certificate you have uploaded and if needed bring in a new certificate. This error occurs with the device node certificate.
CertificateManagement_IncorrectKeyCertSignKeyUsage	Certificate with subject name {0} should not have key usage Certificate Signing. Check the key usage of the certificate and if needed, bring in a new certificate. This error occurs with the signing chain certificate.

Error Code	Description
CertificateManagement_IncorrectKeyNumber	Certificate with subject name {0} has an incorrect key number {1}. Check the key number of the certificate and if needed, bring in a new certificate.
CertificateManagement_InvalidP7b	Uploaded certificate file is not valid. Check the certificate format and if needed, bring in a new certificate.
CertificateManagement_KeyAlgorithmNotRSA	This certificate does not use the RSA key algorithm. Only the RSA certificates are supported.
CertificateManagement_KeySizeNotSufficient	Certificate with subject name {0} has insufficient key size {1}. Minimum key size is 4096.
CertificateManagement_MissingClientOid	Certificate with subject name {0} does not have client authentication OID. Check your certificate properties and if needed, bring in a new certificate.
CertificateManagement_MissingDigitalSignatureKeyUsage	Certificate with subject name {0} does not have Digital Signature in Key Usage. Check your certificate properties and if needed, bring in a new certificate.
CertificateManagement_MissingKeyCertSignKeyUsage	Certificate with subject name {0} does not have Certificate Signing in Key Usage. Check your certificate properties and if needed, bring in a new certificate.
CertificateManagement_MissingKeyEnciphermentKeyUsage	Certificate with subject name {0} does not have Key Encipherment in Key Usage. Check your certificate properties and if needed, bring in a new certificate.
CertificateManagement_MissingServerOid	Certificate with subject name {0} does not have server authentication OID. Check your certificate properties and if needed, bring in a new certificate.
CertificateManagement_NameMismatch	Certificate type mismatch. Expected scope: {0}, found {1}. Upload appropriate certificate.
CertificateManagement_NoPrivateKeyPresent	Certificate with subject name {0} has no private key present. Upload a .pfx certificate with private key.
CertificateManagement_NoRSACryptoPrivateKey	The private key for certificate with subject name {0} is not accessible. Make sure that you are using a supported certificate. Only the Microsoft RSA/Schannel Cryptographic Provider is supported.
CertificateManagement_NotSelfSignedCertificate	Certificate with subject name {0} is not self signed. Root certificates should be self signed
CertificateManagement_NotSupportedOnVirtualAppliance	This operation is not supported on the virtual device. This error indicates that signing will only occur with Data Box Gateway running in Tactical Cloud Appliance. This error occurs while managing the device through Windows PowerShell.
CertificateManagement_SelfSignedCertificate	Certificate with subject name {0} is self signed. Upload a certificate which is properly signed.

ERROR CODE	DESCRIPTION
CertificateManagement_SignatureAlgorithmSha1	Certificate with subject name {0} has unsupported signature algorithm. SHA1-RSA is not supported.
CertificateManagement_SubjectNamesInvalid	Certificate with subject name {0} does not have the correct subject name or subject alternative names for {1} certificate. Check the certificate you have uploaded and if needed bring in a new certificate. You should also check your DNS name to match the SANS names.
CertificateManagement_UnreadableCertificate	Certificate with type {0} could not be read. This error occurs when the certificate is unreadable or corrupted. Bring in a new certificate.
CertificateSubjectNotFound	Certificate with subject name {0} could not be found. Bring in a new certificate.
CertificateRotationGenericFailure	One or more certificates rotation failed. Retry in few minutes. If the problem persists, contact Microsoft Support.
CertificateImportFailure	Certificate with thumbprint {0} was not imported on node {1}. If the problem persists, contact Microsoft Support.
CertificateApplyFailure	Certificate with thumbprint {0} was not applied on node {1}. If the problem persists, contact Microsoft Support.
NodeNotReachable	Could not validate certificate on {0}. Check the system hardware and software health.

Next steps

- Review [Certificate requirements](#).
- [Troubleshoot using device logs, diagnostic tests](#).

Virtual machines on your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article provides a brief overview of virtual machines (VMs) running on your Azure Stack Edge devices, supported VM sizes, and summarizes the various ways of creating VM images, deploying, and then managing VMs.

About VMs

Azure Stack Edge solution provides purpose-built hardware-as-a-service devices from Microsoft that can be used to deploy edge computing workloads and get quick actionable insights at the edge where the data is generated.

Depending on your environment and the type of applications you're running, you can deploy one of the following edge computing workloads on these devices:

- **Containerized** - Use IoT Edge or Kubernetes to run your containerized applications.
- **Non-containerized** - Deploy both Windows and Linux virtual machines on your devices to run non-containerized applications.

You deploy a VM on your device when you need more control over the computing environment. You can use VMs on your device in several ways ranging from development and test to running applications on the edge.

Before you create a VM

Before you begin, review the following considerations about your VM:

- The size of the VM you'll use.
- The maximum number of VMs that can be created on your device.
- The operating system that the VM runs.
- The configuration of the VM after it starts.

VM size

You need to be aware of VM sizes if you're planning to deploy VMs. There are multiple sizes available for the VMs that you can use to run apps and workloads on your device. The size that you choose then determines factors such as processing power, memory, and storage capacity. For more information, see [Supported VM sizes](#).

To figure out the size and the number of VMs that you can deploy on your device, factor in the usable compute on your device and other workloads that you're running. If running Kubernetes, consider the compute requirements for the Kubernetes master and worker VMs as well.

KUBERNETES VM TYPE	CPU AND MEMORY REQUIREMENT
Master VM	4 cores, 4-GB RAM
Worker VM	12 cores, 32-GB RAM

For the usable compute and memory on your device, see the [Compute and memory specifications](#) for your device model.

For a GPU virtual machine, you must use a [VM size from the NCsT4-v3-series](#).

VM limits

You can run a maximum of 24 VMs on your device. This is another factor to consider when deploying your workload.

Operating system disks and images

On your device, you can use Generation 1 or Generation 2 VMs with a fixed virtual hard disk (VHD) format. VHDs are used to store the machine operating system (OS) and data. VHDs are also used for the images you use to install an OS.

The images that you use to create VM images can be generalized or specialized. When creating images for your VMs, you must prepare the images. See the various ways to prepare and use VM images on your device:

- [Prepare Windows generalized image from a VHD](#)
- [Prepare generalized image from an ISO](#)
- [Create custom VM images starting from an Azure VM](#)
- [Use specialized image](#)

Extensions

The following extensions are available for the VMs on your device.

EXTENSION	DESCRIPTION	LEARN MORE
Custom script extensions	Use custom script extensions to configure workloads.	Deploy Custom Script Extension on VMs running on your device
GPU extensions	Use GPU extensions to install GPU drivers.	Create GPU VMs and Install GPU extensions
Reset VM password extensions	Reset a VM password using PowerShell.	Install the VM password reset extension

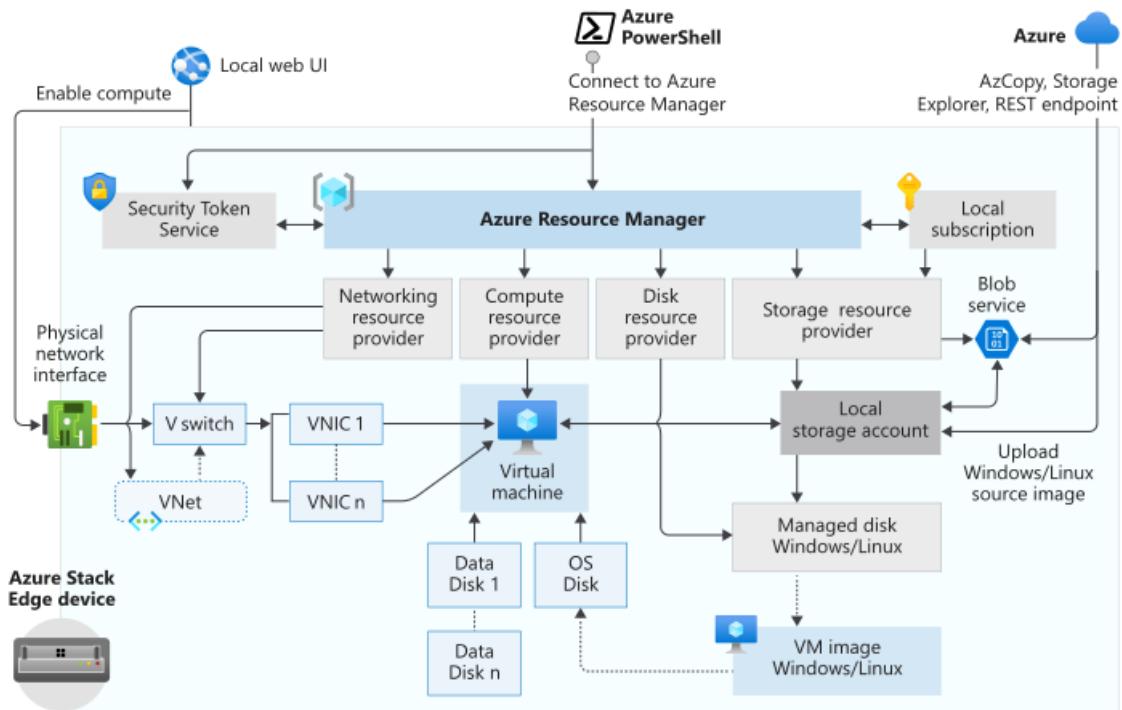
Create a VM

To deploy a VM, you first need to create all the resources that are needed to create a VM. Regardless of the method employed to create a VM, you'll follow these steps:

1. Connect to the local Azure Resource Manager of your device.
2. Identify the built-in subscription on the device.
3. Bring your VM image.
 - a. Create a resource group in the built-in subscription. The resource group will contain the VM and all the related resources.
 - b. Create a local storage account on the device to store the VHD that will be used to create a VM image.
 - c. Upload a Windows/Linux source image into the storage account to create a managed disk.
 - d. Use the managed disk to create a VM image.
4. Enable compute on a device port to create a virtual switch.
 - a. This creates a virtual network using the virtual switch attached to the port on which you enabled compute.
5. Create a VM using the previously created VM image, virtual network, and virtual network interface(s) to communicate within the virtual network and assign a public IP address to remotely access the VM. Optionally

include data disks to provide more storage for your VM.

The deployment workflow is displayed in the following diagram:



There are several ways to deploy a VM on your device. Your choice depends on your environment. The following table summarizes the various ways to deploy a VM on your device:

METHOD	ARTICLE
Azure portal	Deploy a VM on your device via the Azure portal.
Templates	Deploy a VM on your device via templates
PowerShell	Deploy a VM on your device via Azure PowerShell cmdlets Deploy a VM on your device via Azure PowerShell script
CLI/Python	Deploy a VM on your device via Azure CLI/Python
GPU	Deploy a VM on your device using GPUs

Manage your VM

You can manage the VMs on your device via the Azure portal, via the PowerShell interface of the device, or directly through the APIs. Some typical management tasks are:

- Get information about a VM.
- Connect to a VM, start, stop, delete VMs.
- Manage disks, VM sizes, network interfaces, virtual switches
- Back up VM disks.

Get information about your VM

To get more information about your VM via the Azure portal, follow these steps:

- Go to Azure Stack Edge resource for your device and then go to **Virtual machines > Overview**.
- In the **Overview** page, go to **Virtual machines** and select the virtual machine that you're interested in. You

can then view the details of the VM.

Connect to your VM

Depending on the OS that your VM runs, you can connect to the VM as follows:

- [Connect to a Windows VM on your device.](#)
- [Connect to a Linux VM on your device.](#)

Start, stop, delete VMs

You can [turn on the VM, suspend or shut down the VM](#). Finally, you can [delete the VMs](#) after you're done using them.

Manage network interfaces, virtual switches

You can [add, modify, detach network interfaces](#) for your VMs. You can also [create new virtual switches](#) on your device to deploy VMs.

Manage data disks, VM size

You can add a [data disk to an existing VM](#), [attach an existing disk](#), [detach a data disk](#), and finally [resize the VM](#) itself via the Azure portal.

Back up VMs

You can back up the VM disks and in the event of a device failure, restore the data from the backups. For more information, see [Back up VM disks](#).

Next steps

- Learn about [VM sizes and types for Azure Stack Edge Pro GPU](#).

VM sizes and types for Azure Stack Edge Pro

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes the supported sizes for the virtual machines running on your Azure Stack Edge Pro devices. Use this article before you deploy virtual machines on your Azure Stack Edge Pro devices.

Supported VM sizes

The VM size determines the amount of compute resources (like CPU, GPU, and memory) that are made available to the VM. You should create virtual machines by using a VM size appropriate for the workload. Even though all machines will be running on the same hardware, machine sizes have different limits for disk access. This can help you manage overall disk access across your VMs. If a workload increases, you can also resize an existing virtual machine.

The following VMs are supported for creation on your Azure Stack Edge device.

Dv2-series

SIZE	VCPU	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICs
Standard_D1_v2	1	3.5	50	1000	3000	500	4	2
Standard_D2_v2	2	7	100	1000	6000	500	8	4
Standard_D3_v2	4	14	200	1000	12000	500	16	4
Standard_D4_v2	8	28	400	1000	24000	500	32	8
Standard_D5_v2	16	56	800	1000	48000	500	64	8
Standard_D11_v2	2	14	100	1000	6000	500	8	2
Standard_D12_v2	4	28	200	1000	12000	500	16	4

SIZE	VCPU	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICs
Standard_D13_v2	8	56	400	1000	24000	500	32	8

DSv2-series

SIZE	VCPU	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICs
Standard_DS1_v2	1	3.5	7	2000	4000	2300	4	2
Standard_DS2_v2	2	7	14	2000	8000	2300	8	2
Standard_DS3_v2	4	14	28	2000	16000	2300	16	4
Standard_DS4_v2	8	28	56	2000	32000	2300	32	8
Standard_DS5_v2	16	56	112	2000	64000	2300	64	8
Standard_DS11_v2	2	14	28	2000	8000	2300	8	2
Standard_DS12_v2	4	28	56	2000	16000	2300	16	4
Standard_DS13_v2	8	56	112	2000	32000	2300	32	8

For more information, see [Dv2 and DSv2-series](#).

N-series GPU optimized

These sizes are supported for GPU VMs on your device and are optimized for compute-intensive GPU-accelerated applications, for example, inferencing workloads. The GPU VM that you deploy should match the GPU type on your Azure Stack Edge device.

For Nvidia's Tesla T4 GPU.

SIZE	VCPU	MEMORY (GIB)	TEMP STORAGE (GIB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	GPU	GPU MEMORY (GIB)	MAX NICS
Standard_NC4as_T4_v3	4	28	176	2000	48000	2300	1	16	4
Standard_NC8as_T4_v3	8	56	352	2000	48000	2300	1	16	8
Standard_NC16as_T4_v3	16	110	352	2000	48000	2300	1	16	8

For more information, see [NCasT4_v3-series](#).

For Nvidia's A2 Tensor Core GPU

SIZE	VCPU	MEMORY (GIB)	TEMP STORAGE (GIB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	GPU	GPU MEMORY (GIB)	MAX NICS
Standard_NC4as_A2	4	28	176	2000	48000	2300	1	16	4
Standard_NC8as_A2	8	56	352	2000	48000	2300	1	16	8
Standard_NC16as_A2	16	110	352	2000	48000	2300	1	16	8

F-series

These series are optimized for computational workloads and run on Intel Xeon processors.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (GIB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICS
Standard_F1	1	2	16	1000	3000	500	4	2

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (GIB)	MAX OS DISK THROUG HPUT (IOPS)	MAX TEM P STORAGE THROUG HPUT (IOPS)	MAX DATA DISK THROUG HPUT (IOPS)	MAX DATA DISKS	MAX NICS
Standard_F2	2	4	32	1000	6000	500	8	4
Standard_F4	4	8	64	1000	12000	500	16	4
Standard_F8	8	16	128	1000	24000	500	32	8
Standard_F12	12	24	256	1000	48000	500	64	8
Standard_F16	16	32	256	1000	48000	500	64	8
Standard_F1s	1	2	4	2000	4000	2300	4	2
Standard_F2s	2	4	8	2000	8000	2300	8	4
Standard_F4s	4	8	16	2000	16000	2300	16	4
Standard_F8s	8	16	32	2000	32000	2300	32	8
Standard_F16s	16	32	64	2000	64000	2300	64	8

For more information, see [Fsv2-series](#).

High-performance network VMs

The high-performance network (HPN) virtual machines are tailored for workloads that require fast and uninterrupted performance using high speed network interfaces. Due to the nature of logical core pairing, the supported VM sizes have vCPU count in multiples of 2.

HPN DSv2-series

SIZE	VCPU	MEMORY (GIB)	TEMP STORAGE (GIB)	MAX OS DISK THROUG HPUT (IOPS)	MAX TEM P STORAGE THROUG HPUT (IOPS)	MAX DATA DISK THROUG HPUT (IOPS)	MAX DATA DISKS	MAX NICS
Standard_DS2_v2_HPN	2	7	14	2000	8000	2300	8	2

SIZE	VCPU	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICs
Standard_DS3_v2_HPN	4	14	28	2000	16000	2300	16	4
Standard_DS4_v2_HPN	8	28	56	2000	32000	2300	32	8

HPN F-series

SIZE	VCPU	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX OS DISK THROUGHPUT (IOPS)	MAX TEMP STORAGE THROUGHPUT (IOPS)	MAX DATA DISK THROUGHPUT (IOPS)	MAX DATA DISKS	MAX NICs
Standard_F2s_HPN	2	4	8	2000	8000	2300	8	4
Standard_F4s_HPN	4	8	16	2000	16000	2300	16	4
Standard_F8s_HPN	8	16	32	2000	32000	2300	32	8
Standard_F16s_HPN	16	32	64	2000	64000	2300	64	8
Standard_F12_HPN	12	64	64	1000	48000	500	64	8

Unsupported VM operations and cmdlets

Scale sets, availability sets, and snapshots aren't supported.

Next steps

[Deploy VMs on your Azure Stack Edge Pro GPU device via the Azure portal](#)

Resource provider API profile versions for Azure Stack Edge

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

You can find the resource provider and version numbers for each API profile used by Azure Stack Edge in this article. The tables in this article list the versions supported for each resource provider and the API versions of the profiles. Each resource provider contains a set of resource types and specific version numbers.

The API profile uses three naming conventions:

- **latest**
- **yyyy-mm-dd-hybrid**
- **yyyy-mm-dd-profile**

Overview of the 2019-03-01-hybrid profile

RESOURCE PROVIDER	API VERSION
Microsoft.Compute	2017-12-01
Microsoft.Network	2017-10-01 VPN Gateway will be 2017-10-01
Microsoft.Storage (Data Plane)	2019-07-07
Microsoft.Storage (Control Plane)	2019-06-01
Microsoft.Resources (Azure Resource Manager itself)	2020-06-01
Microsoft.Authorization (policy operations)	2016-09-01

For a list of the versions for each resource type for the providers in the API profile, see [Details for the 2019-03-01-hybrid profile](#).

Details for the 2019-03-01-hybrid profile

Microsoft.Compute

The Azure Compute APIs give you programmatic access to virtual machines and their supporting resources. For more information, see [Azure Compute](#).

RESOURCE TYPE	API VERSION
Locations	2017-12-01
Locations/vmSizes	2017-12-01

RESOURCE TYPE	API VERSION
Virtual Machines	2017-12-01
Virtual Machines/extensions	2017-12-01

Microsoft.Network

The operations call result is a representation of the available Network cloud operations list. For more information, see [Operation REST API](#).

RESOURCE TYPES	API VERSIONS
Network Interfaces	2017-10-01
Virtual Networks	2017-10-01

Microsoft.Resources

Azure Resource Manager lets you deploy and manage the infrastructure for your Azure solutions. You organize related resources in resource groups and deploy your resources with JSON templates. For an introduction to deploying and managing resources with Resource Manager, see the [Azure Resource Manager overview](#).

RESOURCE TYPES	API VERSIONS
Deployments	2020-06-01
Deployments/operations	2020-06-01
Links	2020-06-01
Locations	2020-06-01
Operations	2020-06-01
Providers	2020-06-01
ResourceGroups	2020-06-01
Resources	2020-06-01
Subscriptions	2018-09-01
Subscriptions/locations	2018-09-01
Subscriptions/operationresults	2020-06-01
Subscriptions/providers	2020-06-01
Subscriptions/ResourceGroups	2020-06-01
Subscriptions/resourceGroups/resources	2020-06-01
Subscriptions/resources	2020-06-01

RESOURCE TYPES	API VERSIONS
Subscriptions/tagNames	2020-06-01
Subscriptions/tagNames/tagValues	2020-06-01
Tenants	2018-09-01

Microsoft.Storage

The Storage Resource Provider (SRP) lets you manage your storage account and keys programmatically. For more information, see the [Azure Storage Resource Provider REST API reference](#).

RESOURCE TYPES	API VERSIONS
CheckNameAvailability	2019-06-01
Locations	2019-06-01
Locations/quotas	2019-06-01
Operations	2019-06-01
StorageAccounts	2019-06-01
Usages	2019-06-01

Next steps

- [Manage an Azure Stack Edge Pro GPU device via Windows PowerShell](#)

GPU virtual machines for Azure Stack Edge Pro GPU devices

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

GPU-accelerated workloads on an Azure Stack Edge Pro GPU device require a GPU virtual machine. This article provides an overview of GPU VMs, including supported OSs, GPU drivers, and VM sizes. Deployment options for GPU VMs used with Kubernetes clusters also are discussed.

About GPU VMs

Your Azure Stack Edge devices may be equipped with 1 or 2 of Nvidia's Tesla T4 or Tensor Core A2 GPU. To deploy GPU-accelerated VM workloads on these devices, use GPU-optimized VM sizes. The GPU VM chosen should match with the make of the GPU on your Azure Stack Edge device. For more information, see [Supported N series GPU optimized VMs](#).

To take advantage of the GPU capabilities of Azure N-series VMs, Nvidia GPU drivers must be installed. The Nvidia GPU driver extension installs appropriate Nvidia CUDA or GRID drivers. You can [install the GPU extensions using templates or via the Azure portal](#).

You can [install and manage the extension using the Azure Resource Manager templates](#) after VM deployment. In the Azure portal, you can install the GPU extension during or after you deploy a VM; for instructions, see [Deploy GPU VMs on your Azure Stack Edge device](#).

If your device will have a Kubernetes cluster configured, be sure to review [deployment considerations for Kubernetes clusters](#) before you deploy GPU VMs.

Supported OS and GPU drivers

The Nvidia GPU driver extensions for Windows and Linux support the following OS versions.

Supported OS for GPU extension for Windows

This extension supports the following operating systems (OSs). Other versions may work but have not been tested in-house on GPU VMs running on Azure Stack Edge devices.

DISTRIBUTION	VERSION
Windows Server 2019	Core
Windows Server 2016	Core

Supported OS for GPU extension for Linux

This extension supports the following OS distros, depending on the driver support for specific OS version. Other versions may work but have not been tested in-house on GPU VMs running on Azure Stack Edge devices.

DISTRIBUTION	VERSION
Ubuntu	18.04 LTS

DISTRIBUTION	VERSION
Red Hat Enterprise Linux	7.4

GPU VM deployment

You can deploy a GPU VM via the Azure portal or using Azure Resource Manager templates. The GPU extension is installed after VM creation.

- **Portal:** In the Azure portal, you can quickly [install the GPU extension when you create a VM](#) or [after VM deployment](#).
- **Templates:** Using Azure Resource Manager templates, [you create a VM](#) and then [install the GPU extension](#).

GPU VMs and Kubernetes

Before you deploy GPU VMs on your device, review the following considerations if Kubernetes is configured on the device.

For 1-GPU device:

- **Create a GPU VM followed by Kubernetes configuration on your device:** In this scenario, the GPU VM creation and Kubernetes configuration will both be successful. Kubernetes will not have access to the GPU in this case.
- **Configure Kubernetes on your device followed by creation of a GPU VM:** In this scenario, the Kubernetes will claim the GPU on your device and the VM creation will fail as there are no GPU resources available.

For 2-GPU device

- **Create a GPU VM followed by Kubernetes configuration on your device:** In this scenario, the GPU VM that you create will claim one GPU on your device and Kubernetes configuration will also be successful and claim the remaining one GPU.
- **Create two GPU VMs followed by Kubernetes configuration on your device:** In this scenario, the two GPU VMs will claim the two GPUs on the device and the Kubernetes is configured successfully with no GPUs.
- **Configure Kubernetes on your device followed by creation of a GPU VM:** In this scenario, the Kubernetes will claim both the GPUs on your device and the VM creation will fail as no GPU resources are available.

Next steps

- Learn how to [Deploy GPU VMs](#).
- Learn how to [Install GPU extension](#) on the GPU VMs running on your device.

Create custom VM images for your Azure Stack Edge Pro GPU device

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

To deploy VMs on your Azure Stack Edge Pro GPU device, you need to be able to create custom VM images that you can use to create VMs in Azure. This article describes the steps to create custom VM images in Azure for Windows and Linux VMs and download or copy those images to an Azure Storage account.

There's a required workflow for preparing a custom VM image. For the image source, you need to use a fixed VHD from any size that Azure supports. For VM size options, see [Supported VM sizes](#).

Prerequisites

Complete the following prerequisite before you create your VM image:

- [Download AzCopy](#). AzCopy gives you a fast way to copy an OS disk to an Azure Storage account.

Create a custom VM image

The steps for preparing a custom VM image vary for a Windows or Linux VM.

- [Windows](#)
- [Linux](#)

Do the following steps to create a Windows VM image:

1. Create a Windows virtual machine in Azure. For portal instructions, see [Create a Windows virtual machine in the Azure portal](#). For PowerShell instructions, see [Tutorial: Create and manage Windows VMs with Azure PowerShell](#).

The virtual machine can be a Generation 1 or Generation 2 VM. The OS disk that you use to create your VM image must be a fixed-size VHD of any size that Azure supports. For VM size options, see [Supported VM sizes](#).

You can use any Windows Gen1 or Gen2 VM with a fixed-size VHD in Azure Marketplace. For a list of Azure Marketplace images that could work, see [Commonly used Azure Marketplace images for Azure Stack Edge](#).

2. Generalize the virtual machine. To generalize the VM, connect to the virtual machine, open a command prompt, and run the following `sysprep` command:

```
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown /mode:vm
```

IMPORTANT

After the command is complete, the VM will shut down. **Do not restart the VM.** Restarting the VM will corrupt the disk you just prepared.

Download OS disk to storage account

To use your custom VM image to deploy VMs on your device, you must download the OS disk to an Azure Storage account. We recommend that you use the same storage account that you used for your device.

To download the OS disk for the VM to an Azure storage account, do the following steps:

1. [Stop the VM in the portal](#). You need to do this to deallocate the OS disk even if your Windows VM was shut down after you ran `sysprep` to generalize it.
2. [Generate a download URL for the OS disk](#), and make a note of the URL. By default, the URL expires after 3600 seconds (1 hour). You can increase that time if needed.
3. Download the VHD to your Azure Storage account using one of these methods:
 - Method 1: For a faster transfer, use AzCopy to copy the VHD to your Azure Storage account. For instructions, see [Use AzCopy to copy VM image to storage account](#), below.
 - Method 2: For a simple, one-click method, you can select **Download the VHD file** when you generate a download URL (in step 3b) to download the disk from the portal. **When you use this method, the disk copy can take quite a long time, and you'll need to upload the VHD to your Azure storage account to be able to create VMs using the portal.**

You can now use this VHD to create and deploy VMs on your Azure Stack Edge Pro GPU device.

Copy VHD to storage account using AzCopy

The following procedures describe how to use AzCopy to copy a custom VM image to an Azure Storage account so you can use the image to deploy VMs on your Azure Stack Edge Pro GPU device. We recommend that you store your custom VM images in any existing storage account that you're using which is in the same region/subscription as Azure Stack Edge.

Create target URI for a container

AzCopy requires a *target URI* that tells where to copy the new image to in your storage account. Before you run AzCopy, you'll generate a shared-access signature (SAS) URL for the blob container you want to copy the file to. To create the target URI, you'll add the filename to the SAS URL.

To create the target URI for your prepared VHD, do the following steps:

1. Generate a SAS URL for a container in an Azure Storage account, do the following steps:
 - a. In the Azure portal, open the storage account, and select **Containers**. Select and then right-click the blob container you want to use, and select **Generate SAS**.

The screenshot shows the 'Containers' section of the Azure Storage account 'mystorageaccountvdalc'. A context menu is open over the 'virtualr' container, with the 'Generate SAS' option highlighted. The left sidebar shows 'Containers' selected under 'Data storage'.

Name	Last modified	Public access level	Lease state
\$logs	5/21/2021, 8:59:08 AM	Private	Available
virtualr	5/21/2021, 9:01:19 AM	Private	Available

- b. On the Generate SAS screen, select **Read** and **Write** in Permissions.

The 'Generate SAS' dialog box is open. The 'Permissions' section is highlighted with a red box, showing '2 selected' and checkboxes for 'Read' and 'Write', both of which are checked. Other options like 'Add', 'Create', 'Delete', and 'List' are available but not selected.

Generate SAS

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. [Learn more](#)

Signing method

Account key User delegation key

Signing key [\(i\)](#)

Key 1

Permissions * [\(i\)](#)

2 selected

Read
 Add
 Create
 Write
 Delete
 List

11:53:32 AM (US & Canada)
7:53:32 PM (UTC-08:00) Pacific Time (US & Canada)

Allowed IP addresses [\(i\)](#)
for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols [\(i\)](#)
 HTTPS only HTTPS and HTTP

Generate SAS token and URL

- c. Select **Generate SAS token and URL**, and then select **Copy** to copy the Blob SAS URL.

Generate SAS

X

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. [Learn more](#)

Signing method

Account key User delegation key

Signing key [i](#)

Key 1 [▼](#)

Permissions * [i](#)

2 selected [▼](#)

Start and expiry date/time [i](#)

Start

05/21/2021 [▼](#) 11:53:32 AM

(UTC-08:00) Pacific Time (US & Canada) [▼](#)

Expiry

05/21/2021 [▼](#) 7:53:32 PM

(UTC-08:00) Pacific Time (US & Canada) [▼](#)

Allowed IP addresses [i](#)

for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols [i](#)

HTTPS only HTTPS and HTTP

Generate SAS token and URL

Blob SAS token [i](#)

sp=rw&st=2021-05-21T18:53:32Z&se=2021-05-22T02:53:32Z&spr=https&sv=2020-02... [Copy](#)

Blob SAS URL

<https://mystorageaccountvdalc.blob.core.windows.net/virtualmachines?sp=rw&st=2021-05-21T18:53:32Z&se=2021-05-22T02:53:32Z&spr=https&sv=2020-02-10&sr=c&sig=PV3Q3zpaQ%2FOLidbQJDKIW9nK%2BJ7PkzYv2Eczxko5k%2Bg%3D> [Copy to clipboard](#)

2. To create the target URI for the `azcopy` command, add the desired filename to the SAS URL.

The Blob SAS URL has the following format.

https://mystorageaccount.blob.core.windows.net/virtualmachines?sp=rw&st=2021-05-21T16:52:24Z&se=2021-05-22T00:52:24Z&spr=https&sv=2020-02-10&sr=c&sig=PV3Q3zpaQ%2FOLidbQJDKIW9nK%2BJ7PkzYv2Eczxko5k%2Bg%3D

Insert the filename, in the format `/<filename>.vhdx` before the question mark that begins the query string.
The filename extension must be VHD.

Insert filename here
format: /<filename>.vhdx

Blob container path

Query string begins

For example, the following Blob SAS URL will copy the `osdisk.vhd` file to the `virtualmachines` blob container in `mystorageaccount`.

`https://mystorageaccount.blob.core.windows.net/virtualmachines/osdisk.vhd?sp=rw&st=2021-05-21T16:52:24Z&se=2021-05-22T00:52:24Z&spr=https&sv=2020-02-10&sr=c&sig=PV3Q3zpaQ%2FOLidbQJDKIW9nK%2BJ7PkzYv2Eczxko5k%2Bg%3D`

Copy VHD to blob container

To copy your VHD to a blob container using AzCopy, do the following steps:

1. Download AZCopy if you haven't done that already.
2. In PowerShell, navigate to the directory where you stored azcopy.exe, and run the following command:

```
.\azcopy copy <source URI> <target URI> --recursive
```

where:

- <source URI> is the download URL that you generated earlier.
- <target URI> tells which blob container to copy the new image to in your Azure Storage account. For instructions, see [Use AzCopy to copy VM image to storage account](#).

For example, the following URI will copy a file named **windowsosdisk.vhd** to the **virtual machines** blob container in the **mystorageaccount** storage account:

```
.\azcopy copy "https://md-h1rvdq3wtdp.z24.blob.storage.azure.net/gxs3kpbghkr/abcd?sv=2018-03-28&sr=b&si=f86003fc-a231-43b0-baf2-61dd51e3a05a&sig=o5Rj%2BNZSook%2FVNMcuCcwEwsr0i7sy%2F7gIDzak6Jh1Kg%3D" "https://mystorageaccount.blob.core.windows.net/virtualmachines/osdisk.vhd?sp=rw&st=2021-05-21T16:52:24Z&se=2021-05-22T00:52:24Z&spr=https&sv=2020-02-10&sr=c&sig=PV3Q3zpaQ%2FOLidbQJDK1W9nK%2BJ7PkzYv2Eczxko5k%2Bg%3D" --recursive
```

Sample output

For the example AzCopy command above, the following output indicates a successful copy was completed.

```
PS C:\azcopy\azcopy_windows_amd64_10.10.0> .\azcopy copy "https://md-h1rvdq3wtdp.z24.blob.storage.azure.net/gxs3kpbghkr/abcd?sv=2018-03-28&sr=b&si=f86003fc-a231-43b0-baf2-61dd51e3a05a&sig=o5Rj%2BNZSook%2FVNMcuCcwEwsr0i7sy%2F7gIDzak6Jh1Kg%3D" "https://mystorageaccount.blob.core.windows.net/virtualmachines/osdisk.vhd?sp=rw&st=2021-05-21T16:52:24Z&se=2021-05-22T00:52:24Z&spr=https&sv=2020-02-10&sr=c&sig=PV3Q3zpaQ%2FOLidbQJDK1W9nK%2BJ7PkzYv2Eczxko5k%2Bg%3D" --recursive
INFO: Scanning...
INFO: Failed to create one or more destination container(s). Your transfers may still succeed if the container already exists.
INFO: Any empty folders will not be processed, because source and/or destination doesn't have full folder support

Job 783f2177-8317-3e4b-7d2f-697a8f1ab63c has started
Log file is located at: C:\Users\aseuser\.azcopy\783f2177-8317-3e4b-7d2f-697a8f1ab63c.log

INFO: Destination could not accommodate the tier P10. Going ahead with the default tier. In case of service to service transfer, consider setting the flag --s2s-preserve-access-tier=false.
100.0 %, 0 Done, 0 Failed, 1 Pending, 0 Skipped, 1 Total,

Job 783f2177-8317-3e4b-7d2f-697a8f1ab63c summary
Elapsed Time (Minutes): 1.4671
Number of File Transfers: 1
Number of Folder Property Transfers: 0
Total Number of Transfers: 1
Number of Transfers Completed: 1
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 136367309312
Final Job Status: Completed

PS C:\azcopy\azcopy_windows_amd64_10.10.0>
```

Next steps

- [Deploy VMs on your device using the Azure portal](#)
- [Deploy VMs on your device via PowerShell](#)

Prepare generalized image from Windows VHD to deploy VMs on Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

To deploy VMs on your Azure Stack Edge Pro GPU device, you need to be able to create custom VM images that you can use to create VMs. This article describes how to prepare a generalized image from a Windows VHD or VHDX, which you can use to deploy virtual machines on Windows Stack Edge Pro GPU devices.

To prepare a generalized VM image using an ISO, see [Prepare a generalized image from an ISO to deploy VMs on Azure Stack Edge Pro GPU](#).

About VM images

A Windows VHD or VHDX can be used to create a *specialized* image or a *generalized* image. The following table summarizes key differences between the *specialized* and the *generalized* images.

IMAGE TYPE	GENERALIZED	SPECIALIZED
Target	Deployed on any system.	Targeted to a specific system.
Setup after boot	Setup required at first boot of the VM.	No setup needed. Platform turns on the VM.
Configuration	Hostname, admin-user, and other VM-specific settings required.	Preconfigured.
Used when	Creating multiple new VMs from the same image.	Migrating a specific machine or restoring a VM from previous backup.

Workflow

The high-level workflow to prepare a Windows VHD to use as a generalized image, starting from the VHD or VHDX of an existing virtual machine, has the following steps:

1. Prepare the source VM from a Windows VHD:
 - a. Convert the source VHD or VHDX to a fixed-size VHD.
 - b. Use that VHD to create a new virtual machine.
2. Start the VM, and install the Windows operating system.
3. Generalize the VHD using the *sysprep* utility.
4. Copy the generalized image to Blob storage.

Prerequisites

Before you prepare a Windows VHD for use as a generalized image on an Azure Stack Edge Pro GPU device, make sure that:

- You have a VHD or a VHDX containing a supported version of Windows.

- You have access to a Windows client with Hyper-V Manager installed.
- You have access to an Azure Blob storage account to store your VHD after it is prepared.

Prepare source VM from Windows VHD

When your VM source is a Windows VHD or VHDX, you first need to convert the Windows VHD to a fixed-size VHD. You will use the fixed-size VHD to create a new virtual machine.

IMPORTANT

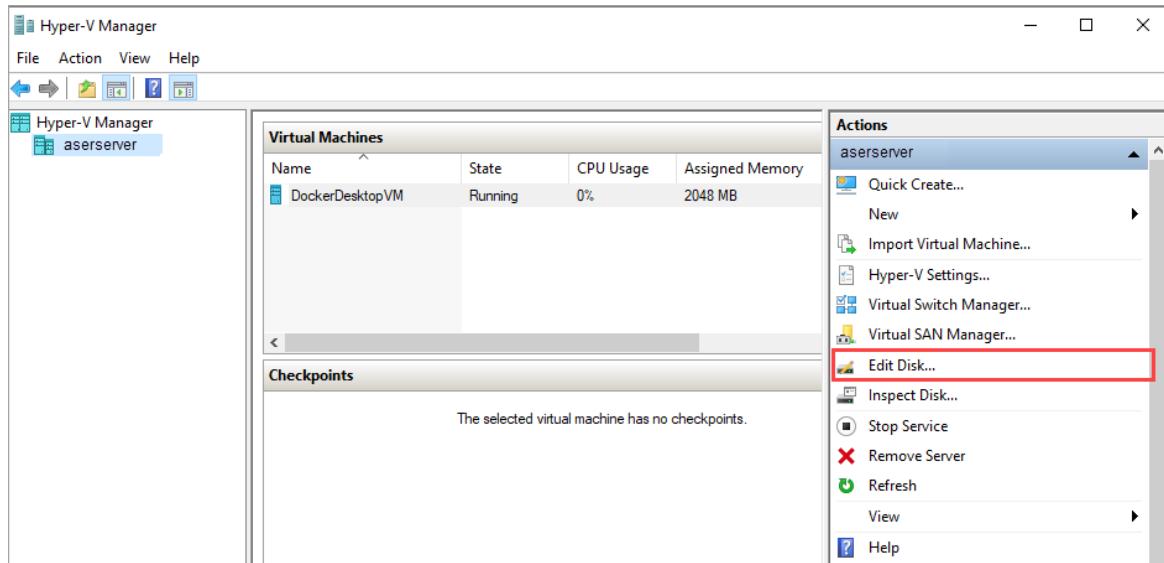
These procedures do not cover cases where the source VHD is configured with custom configurations and settings. For example, additional actions may be required to generalize a VHD containing custom firewall rules or proxy settings. For more information on these additional actions, see [Prepare a Windows VHD to upload to Azure - Azure Virtual Machines](#).

Convert source VHD to a fixed-size VHD

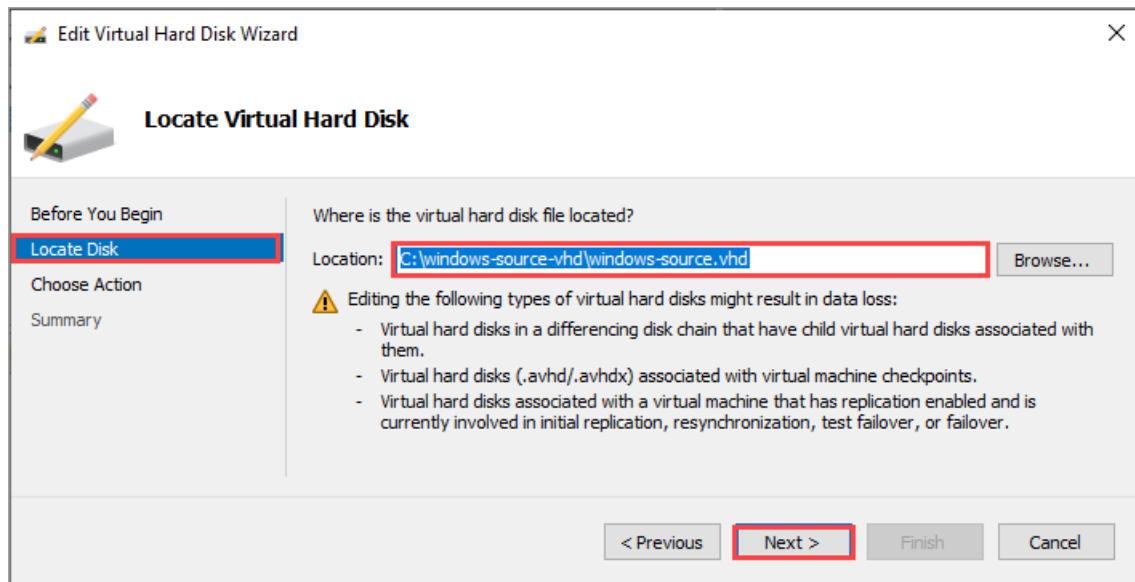
For your device, you'll need fixed-size VHDs to create VM images. You'll need to convert your source Windows VHD or VHDX to a fixed VHD.

Follow these steps:

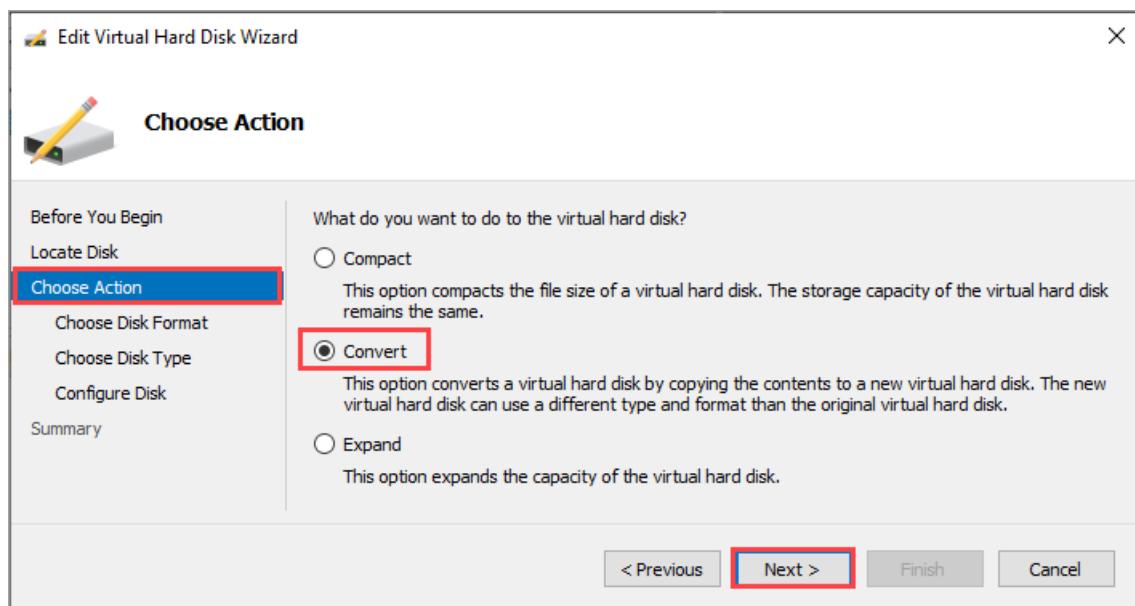
1. Open Hyper-V Manager on your client system. Go to **Edit Disk**.



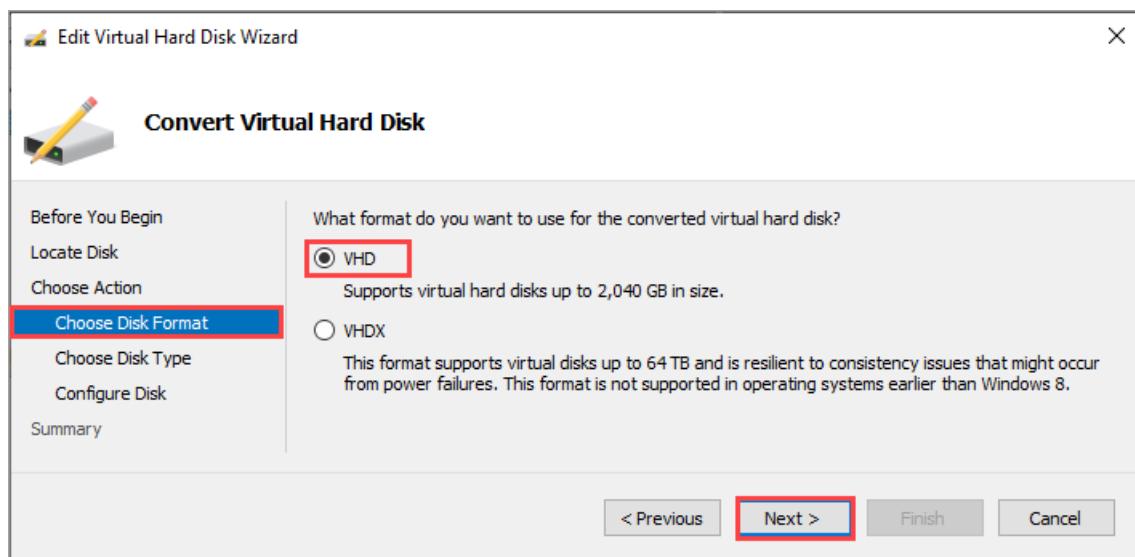
2. On the **Before you begin** page, select **Next>**.
3. On the **Locate virtual hard disk** page, browse to the location of the source Windows VHD or VHDX that you wish to convert. Select **Next>**.



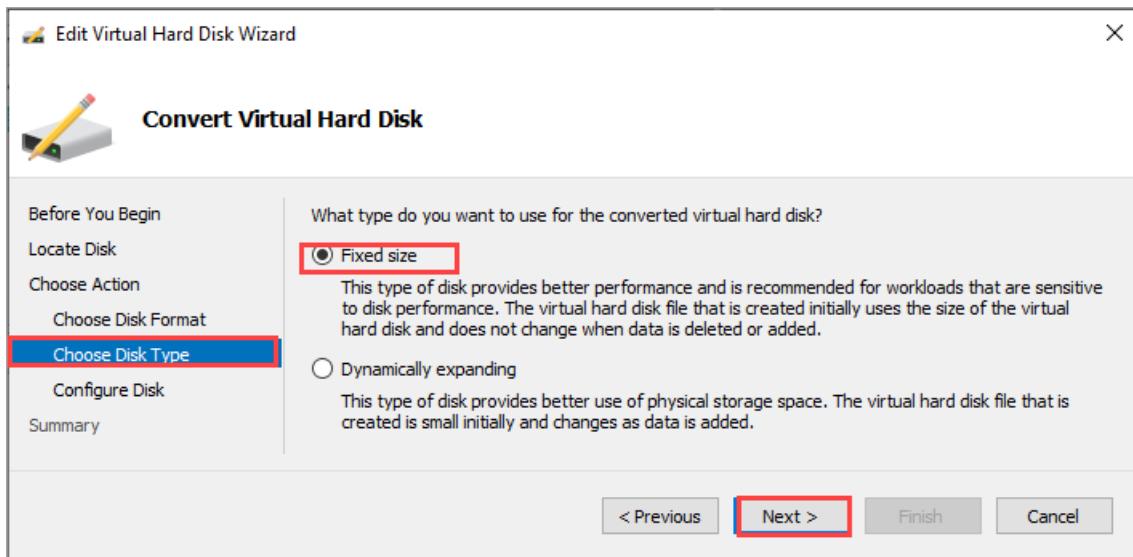
4. On the Choose action page, select Convert and select Next> .



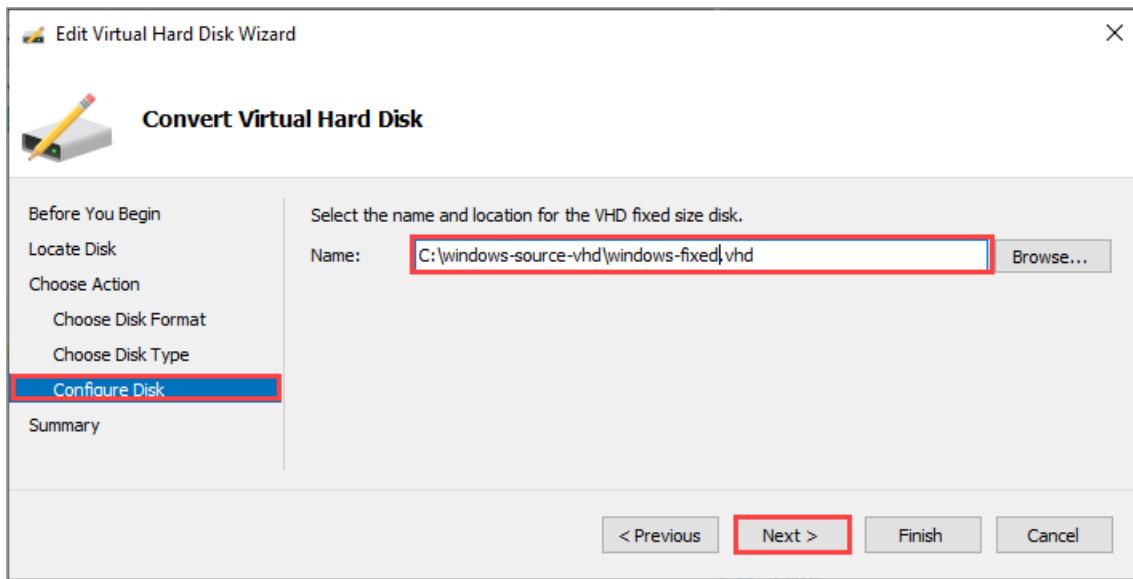
5. On the Choose disk format page, select VHD format and then select Next> .



6. On the Choose disk type page, choose Fixed size and select Next> .



7. On the **Configure disk** page, browse to the location and specify a name for the fixed size VHD disk. Select **Next >**.

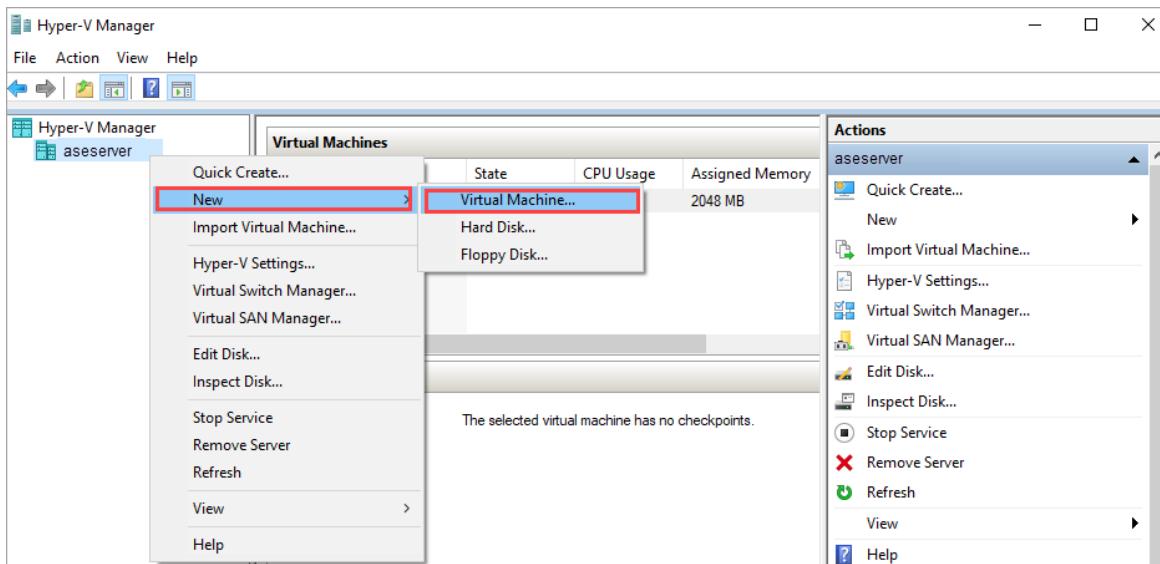


8. Review the summary and select **Finish**. The VHD or VHDX conversion takes a few minutes. The time for conversion depends on the size of the source disk.

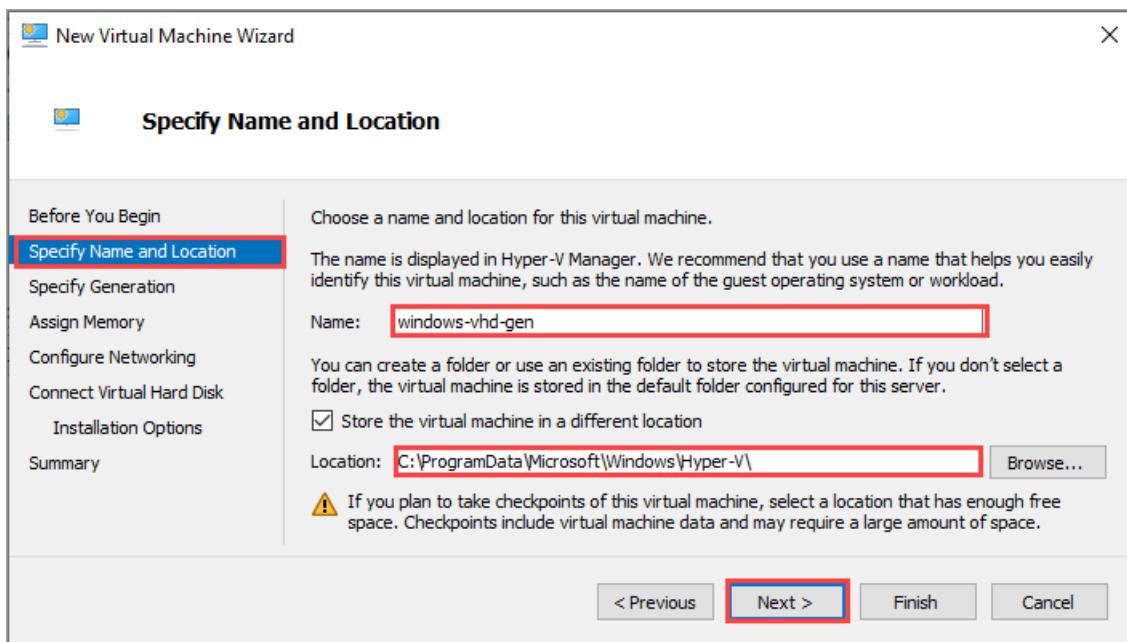
You'll use this fixed-size VHD for all the subsequent steps in this article.

Create Hyper-V VM from the fixed-size VHD

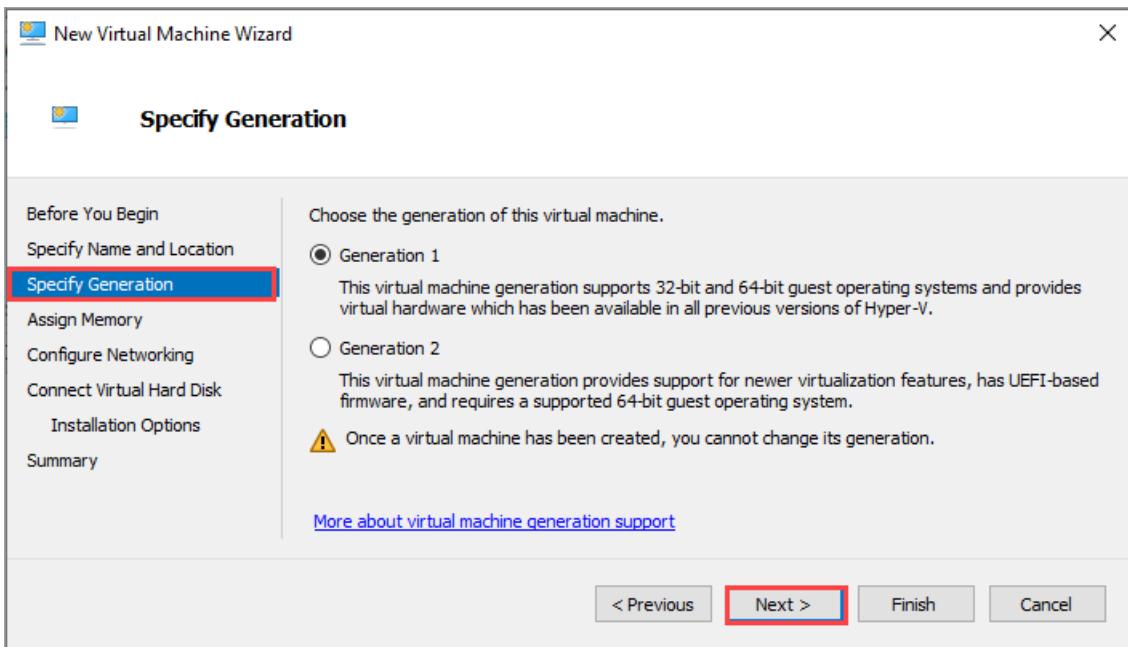
1. In **Hyper-V Manager**, in the scope pane, right-click your system node to open the context menu, and then select **New > Virtual Machine**.



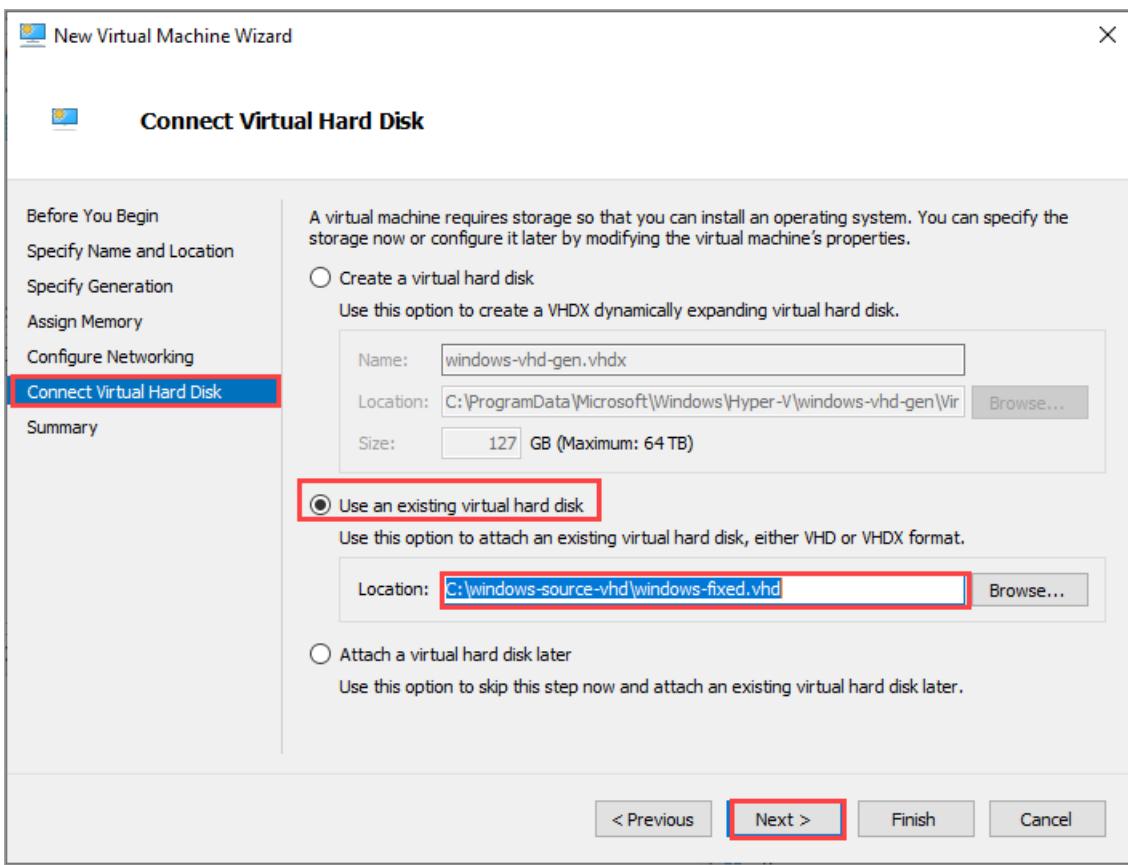
2. On the **Before you begin** page of the New Virtual Machine Wizard, select **Next**.
3. On the **Specify name and location** page, provide a **Name** and **location** for your virtual machine. Select **Next**.



4. On the **Specify generation** page, choose **Generation 1** or **Generation 2** for the .vhdx device image type, and then select **Next**.



5. Assign your desired memory and networking configurations.
6. On the **Connect virtual hard disk** page, choose **Use an existing virtual hard disk**, specify the location of the Windows fixed VHD that we created earlier, and then select **Next**.



7. Review the **Summary** and then select **Finish** to create the virtual machine.

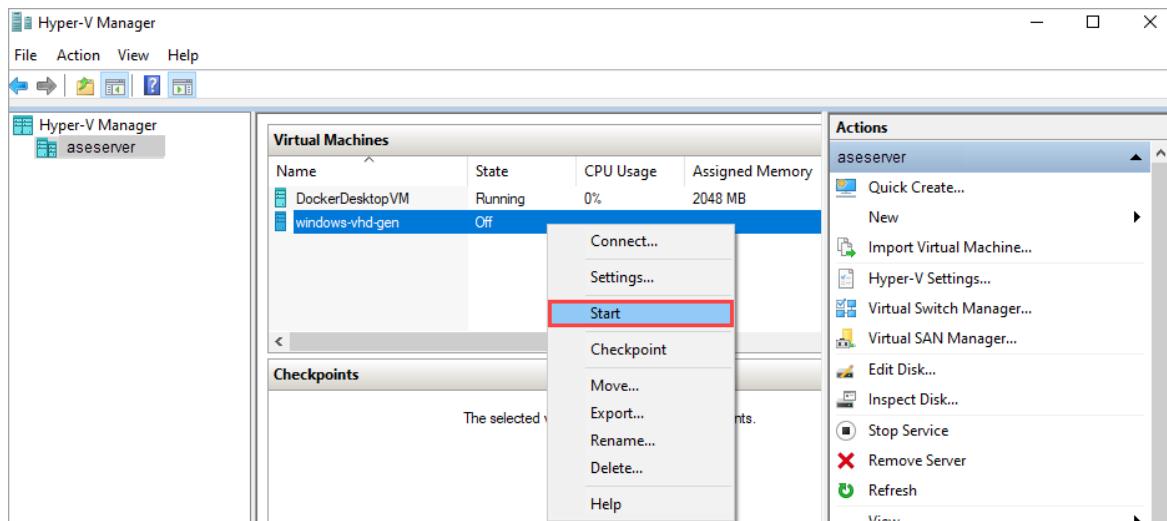
Creation of the virtual machine takes several minutes.

The VM shows in the list of the virtual machines on your client system.

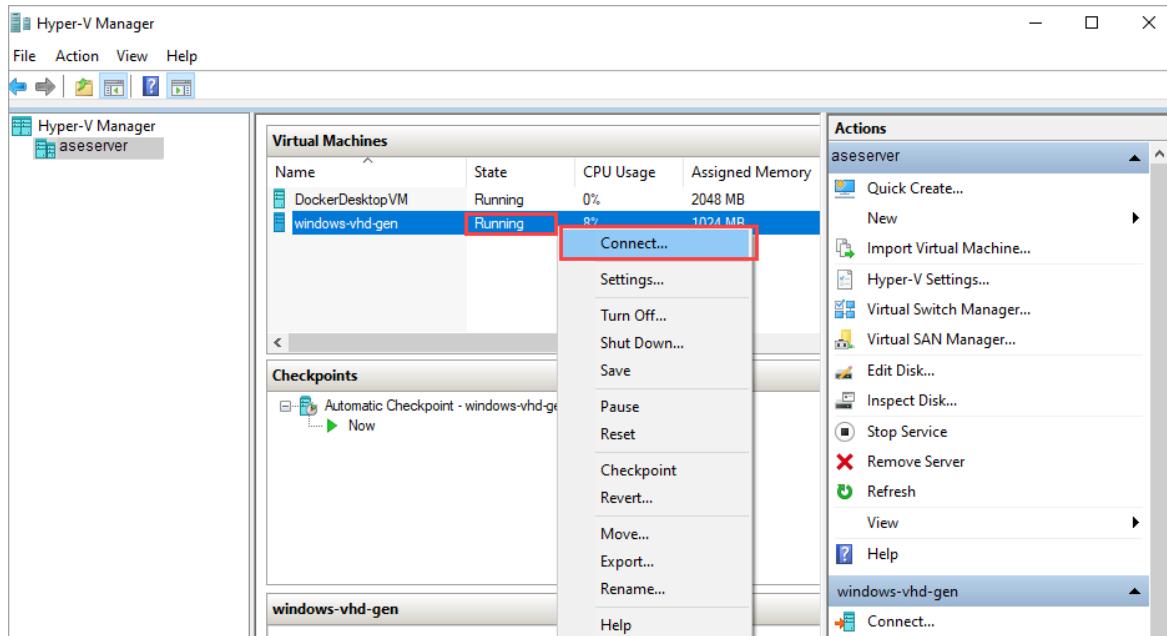
Start VM, and install operating system

To finish building your virtual machine, you need to start the virtual machine and walk through the operating system installation.

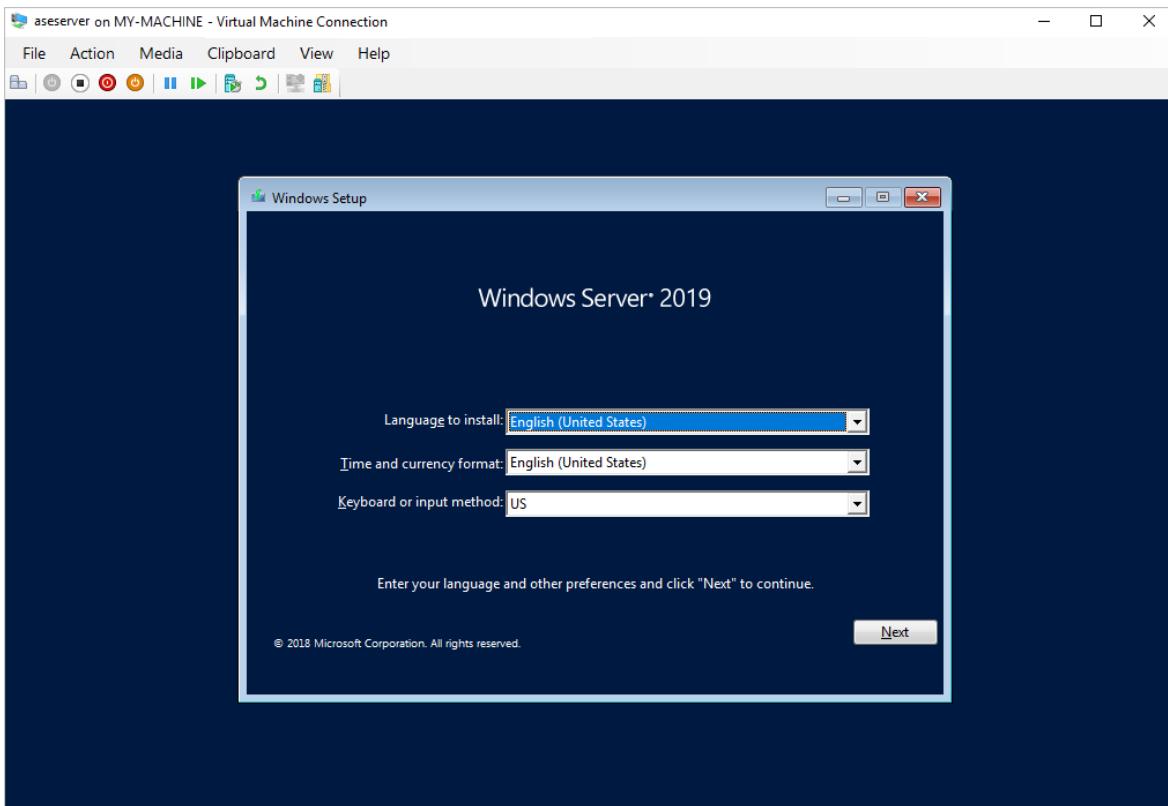
1. In Hyper-V Manager, in the scope pane, right-click the VM to open the context menu, and then select Start.



2. When the VM state is **Running**, select the VM, and then right-click and select Connect.



3. The virtual machine boots into setup, and you can walk through the installation like you would on a physical computer.



After you're connected to the VM, complete the Machine setup wizard, and then sign into the VM.

Generalize the VHD

Use the *sysprep* utility to generalize the VHD.

1. Inside the VM, open a command prompt.
2. Run the following command to generalize the VHD.

```
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown /mode:vm
```

For details, see [Sysprep \(system preparation\) overview](#).

3. After the command is complete, the VM will shutdown. **Do not restart the VM.**

Your VHD can now be used to create a generalized image to use on Azure Stack Edge Pro GPU.

Upload generalized VHD to Azure Blob storage

1. Upload the VHD to Azure blob storage. See the detailed instructions in [Upload a VHD using Azure Storage Explorer](#).
2. After the upload is complete, you can use the uploaded image to create VM images and VMs.

Next steps

Depending on the nature of deployment, you can choose one of the following procedures.

- [Deploy a VM from a generalized image via Azure portal](#)
- [Prepare a generalized image from an ISO to deploy VMs on Azure Stack Edge Pro GPU](#)
- [Prepare a specialized image and deploy VMs using the image](#)

Prepare generalized image from ISO to deploy VMs on Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

To deploy VMs on your Azure Stack Edge Pro GPU device, you need to be able to create custom virtual machine (VM) images that you can use to create VMs. This article describes how to prepare a Windows VM image using ISO installation media, and then generalize that image so you can use it to deploy multiple new VMs on your Azure Stack Edge Pro GPU device.

To prepare a generalized image created from a Windows VHD or VHDX, see [Prepare a generalized image from a Windows VHD to deploy VMs on Azure Stack Edge Pro GPU](#).

About VM images

A Windows VHD or VHDX can be used to create a *specialized* image or a *generalized* image. The following table summarizes key differences between the *specialized* and the *generalized* images.

IMAGE TYPE	GENERALIZED	SPECIALIZED
Target	Deployed on any system.	Targeted to a specific system.
Setup after boot	Setup required at first boot of the VM.	No setup needed. Platform turns on the VM.
Configuration	Hostname, admin-user, and other VM-specific settings required.	Preconfigured.
Used when	Creating multiple new VMs from the same image.	Migrating a specific machine or restoring a VM from previous backup.

Workflow

The high-level workflow to create a generalized Windows VHD using an ISO is:

1. Prepare the source VM using an ISO image:
 - a. Create a new, blank, fixed-size VHD in Hyper-V Manager.
 - b. Use that VHD to create a new virtual machine.
 - c. Mount your ISO image on the DVD drive of the new VM.
2. Start the VM, and install the Windows operating system.
3. Generalize the VHD using the *sysprep* utility.
4. Copy the generalized image to Azure Blob storage.

Prerequisites

Before you can create a generalized Windows VHD by using an ISO image, make sure that:

- You have an ISO image for the supported Windows version that you want to turn into a generalized VHD.

Windows ISO images can be downloaded from the [Microsoft Evaluation Center](#).

- You have access to a Windows client with Hyper-V Manager installed.
- You have access to an Azure blob storage account to store your VHD after it is prepared.

Prepare source VM using an ISO

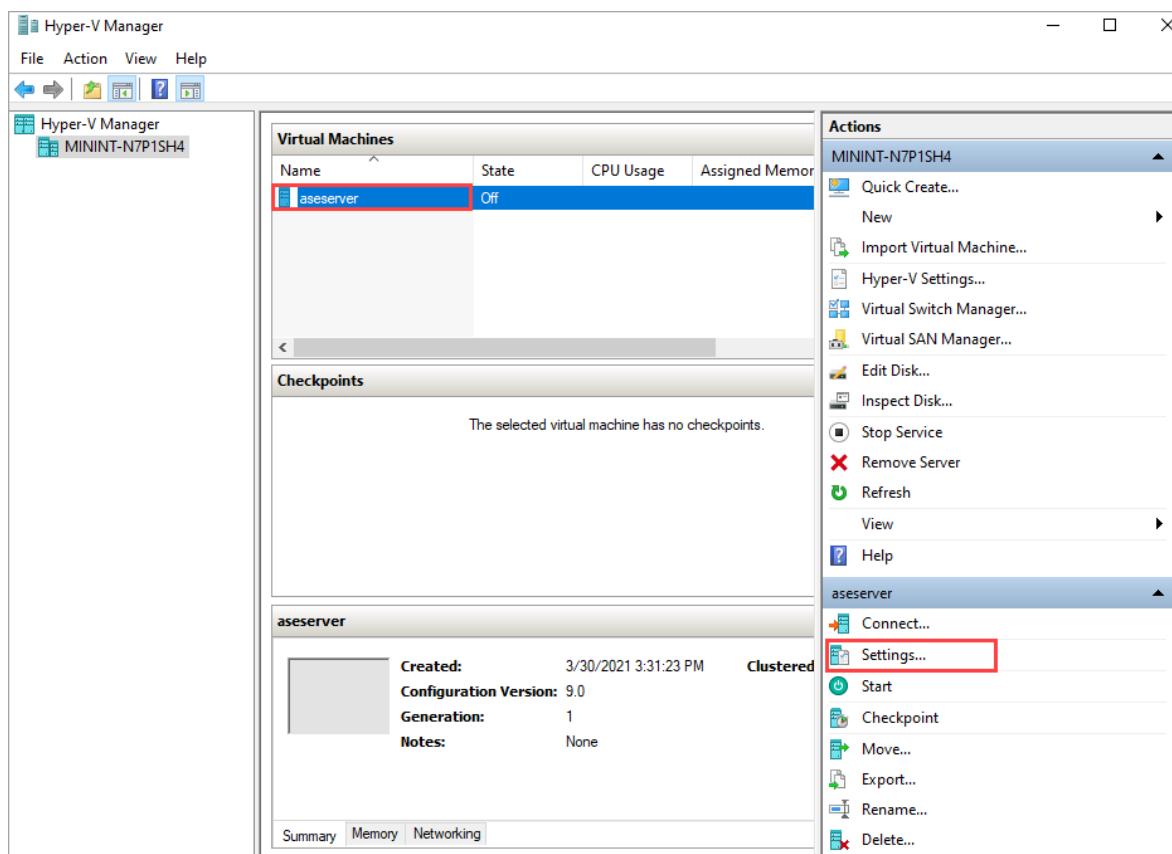
When you use an ISO image to install the operating system on your VM image, you start by creating a blank, fixed-size VHD in Hyper-V Manager. You then use that VHD to create a virtual machine. Then you attach the ISO image to the VM.

Create new VHD in Hyper-V Manager

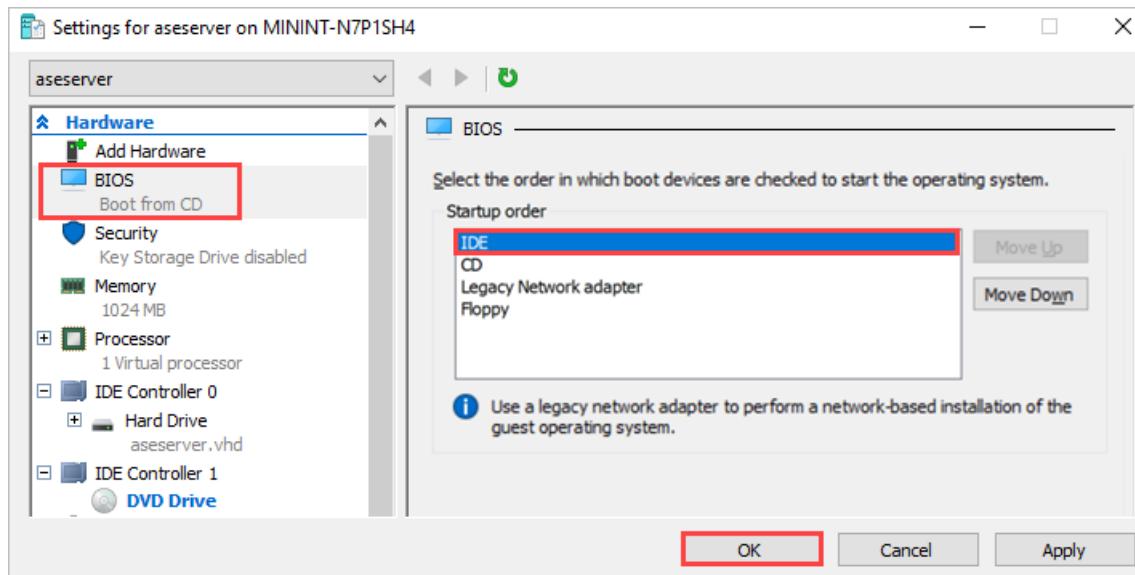
Your first step is to create a new Generation 1 VHD in Hyper-V Manager, which will be the source VHD for a new virtual machine.

To create the VHD, follow these steps:

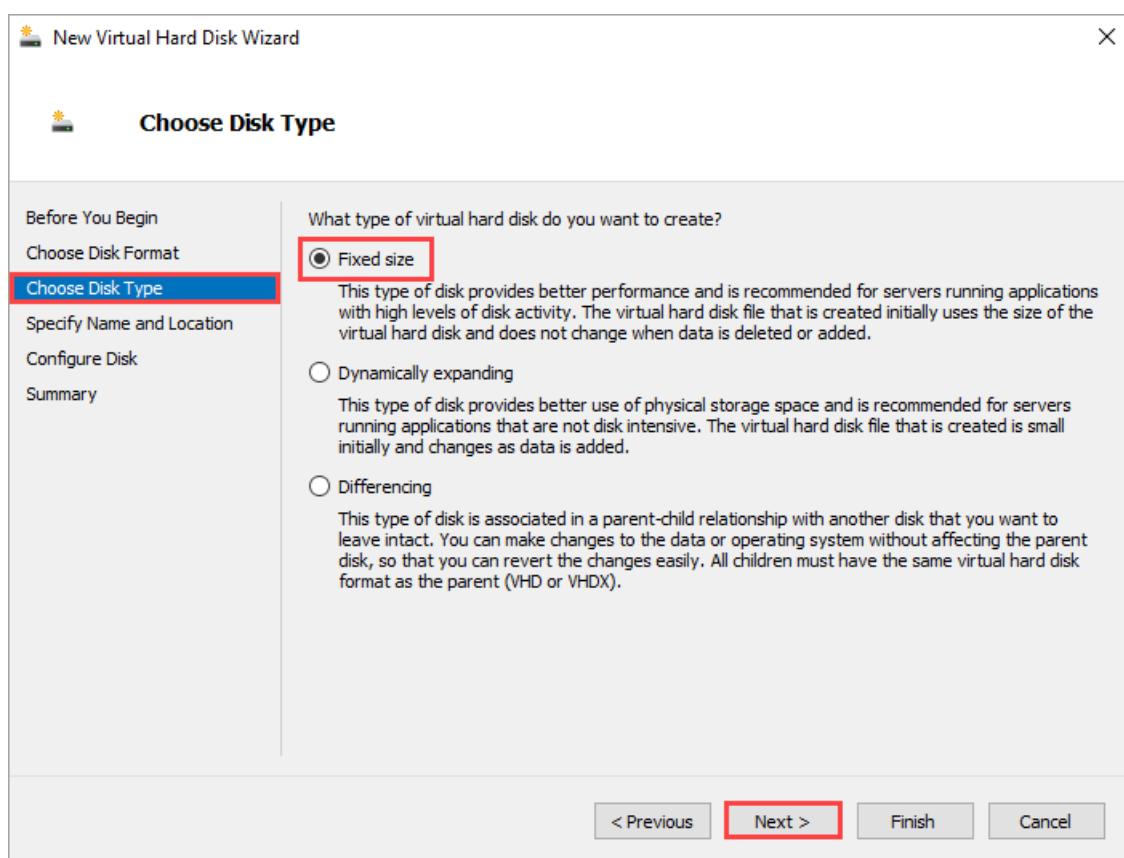
1. Open Hyper-V Manager on your client system. On the Action menu, select **New** and then **Hard Disk**.



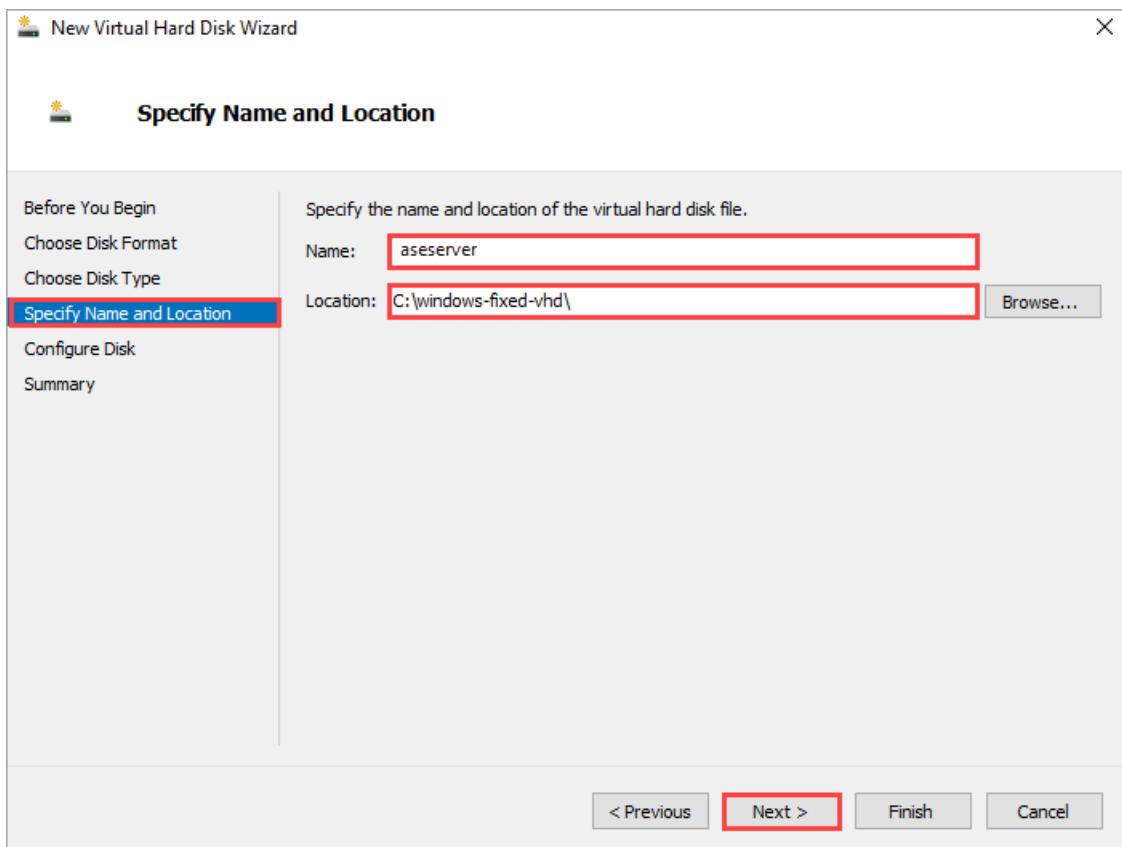
2. Under **Choose Disk Format**, select **VHD**. Then select **Next >**.



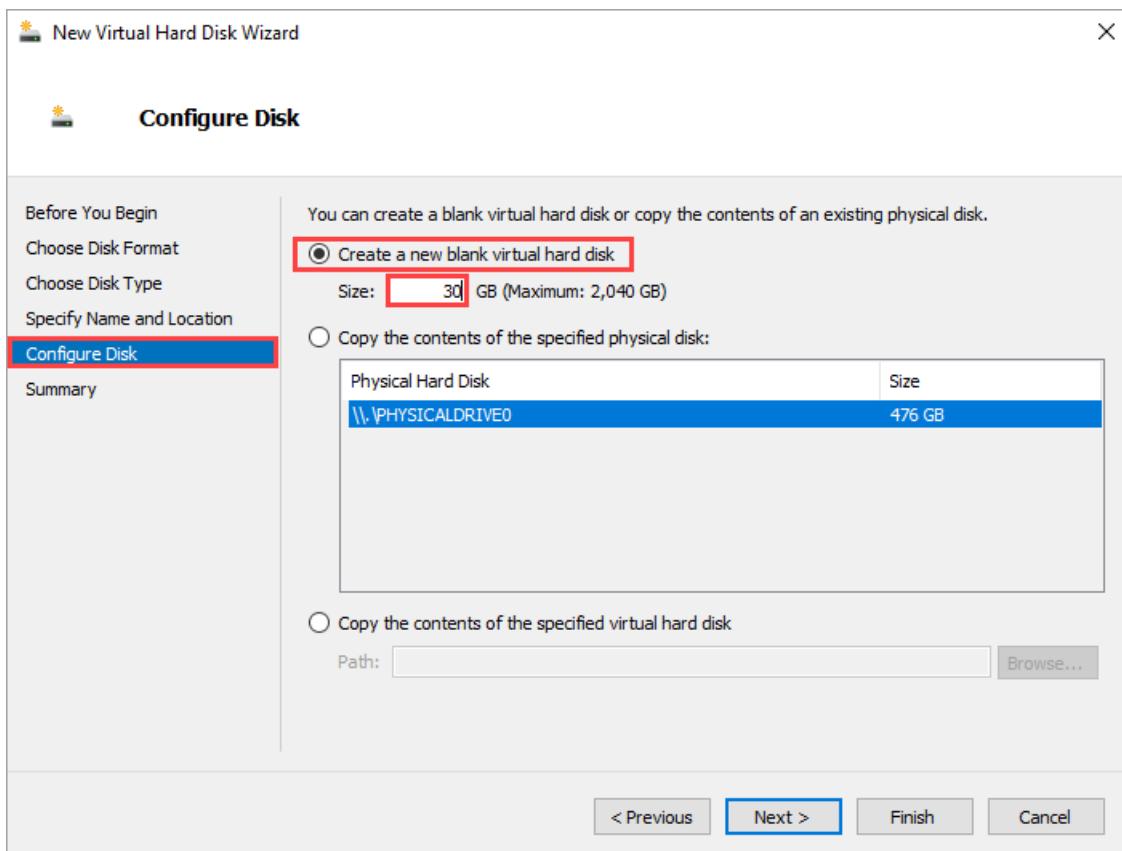
3. Under Choose Disk Type, select Fixed size. Then select Next >.



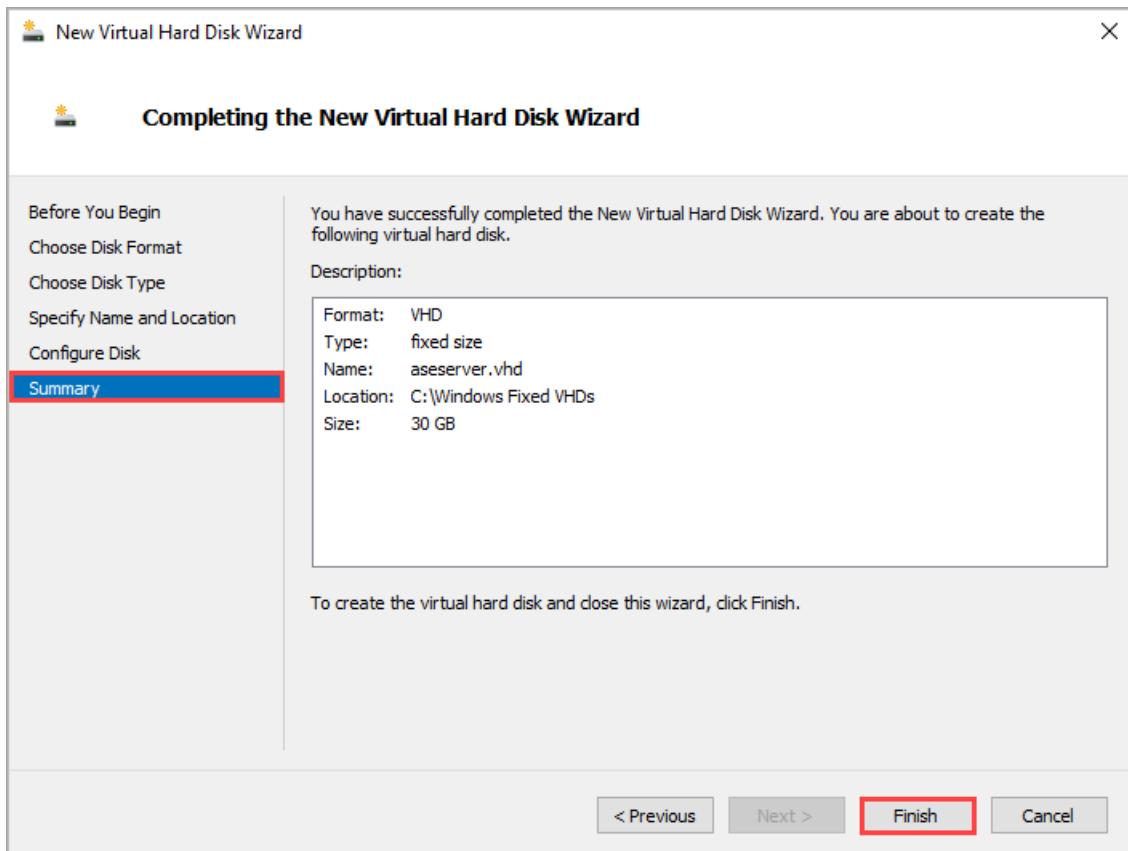
4. Under Specify Name and Location, enter a name and location for your new VHD. Then select Next >.



5. Under **Configure Disk**, select **Create a new blank virtual hard disk**, and enter the size of disk you would like to create (generally 20 GB and above for Windows Server). Then select **Next >**.



6. Under **Summary**, review your selections, and select **Finish** to create the new VHD. The process will take five or more minutes depending on the size of the VHD created.

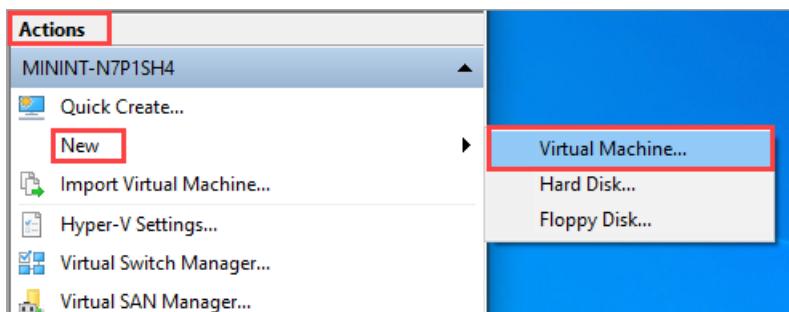


Create Hyper-V VM from VHD

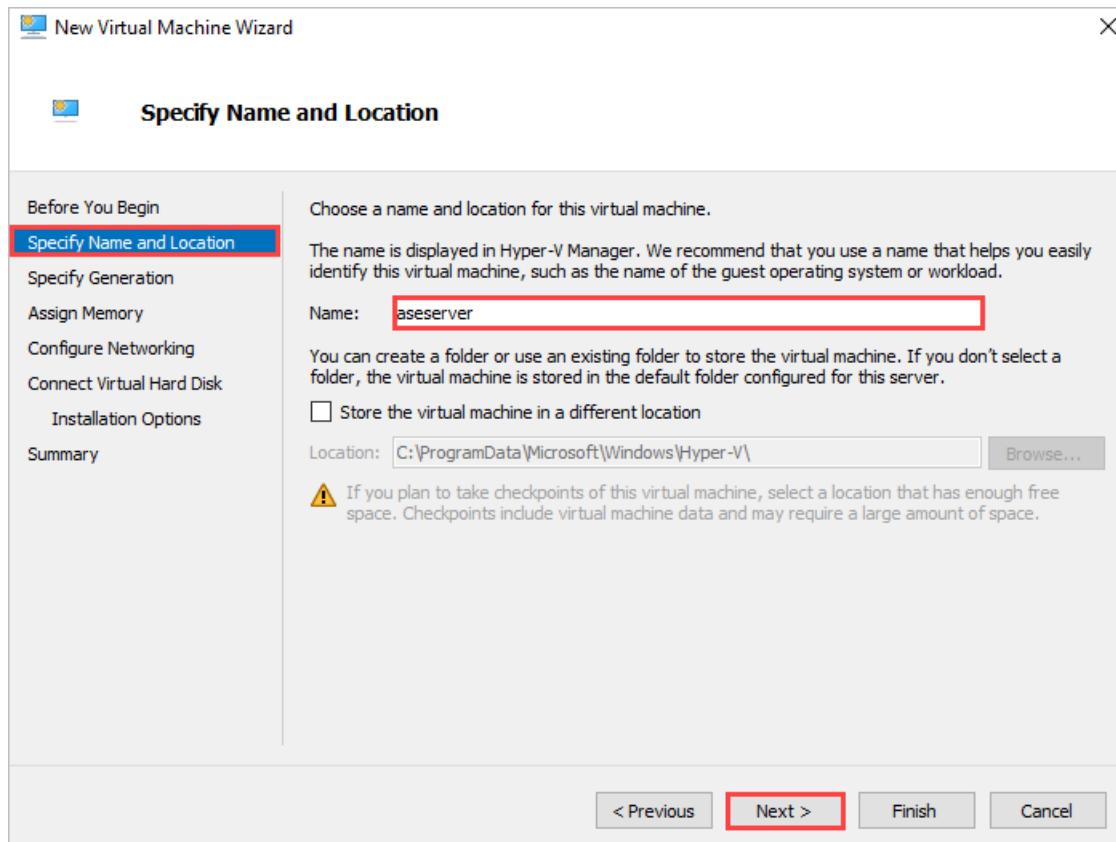
Now you'll use the VHD you just created to create a new virtual machine.

To create your new virtual machine, follow these steps:

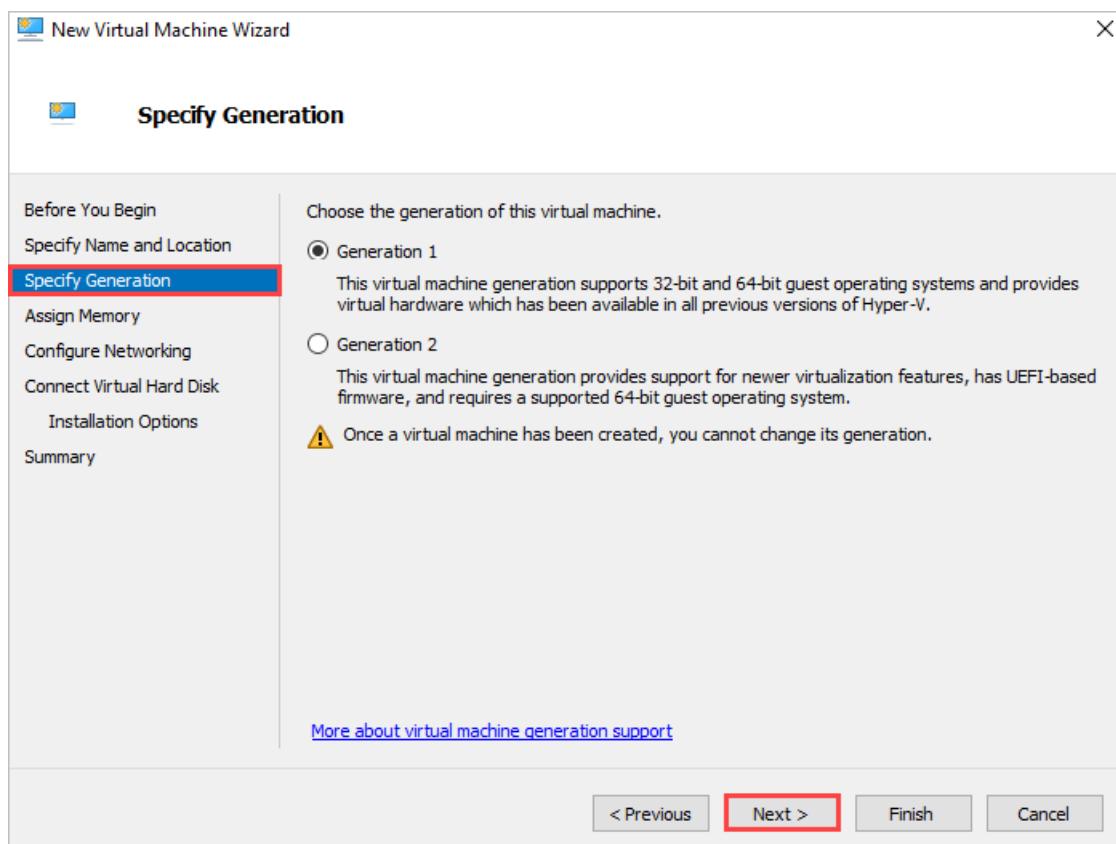
1. Open Hyper-V Manager on your Windows client.
2. On the **Actions** pane, select **New** and then **Virtual Machine...**.



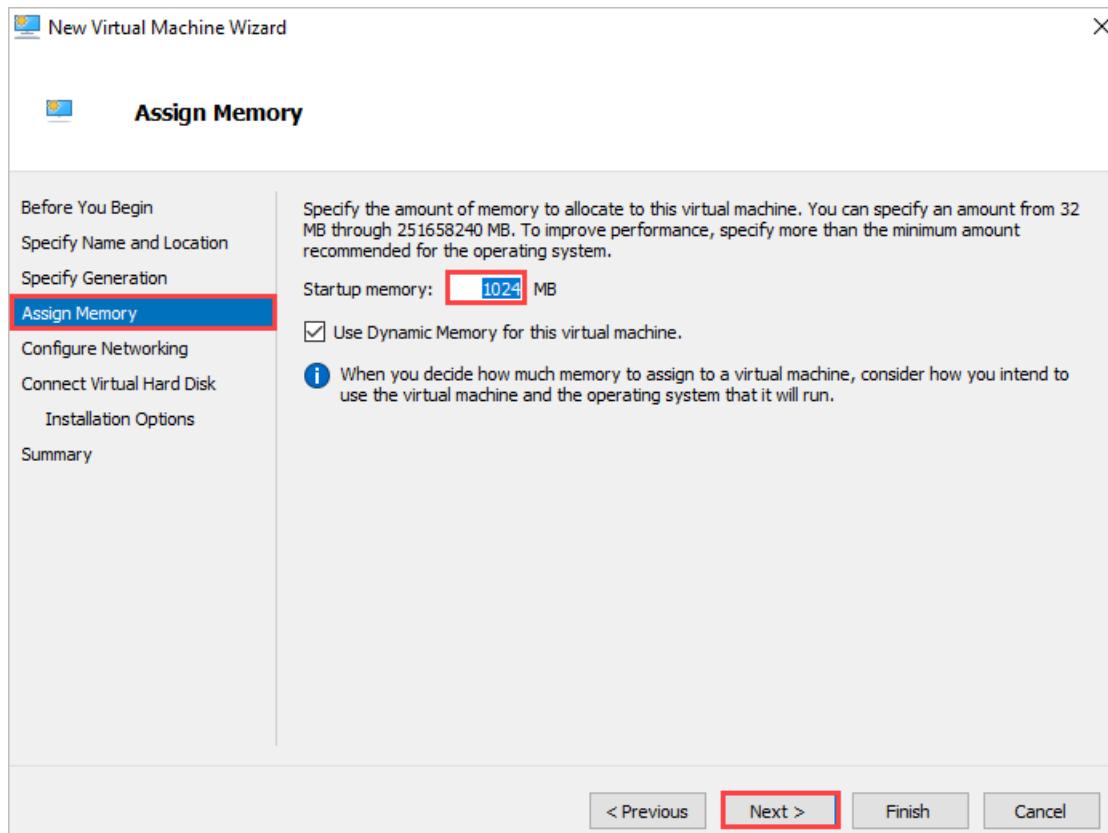
3. In the New Virtual Machine Wizard, specify the name and location of your VM.



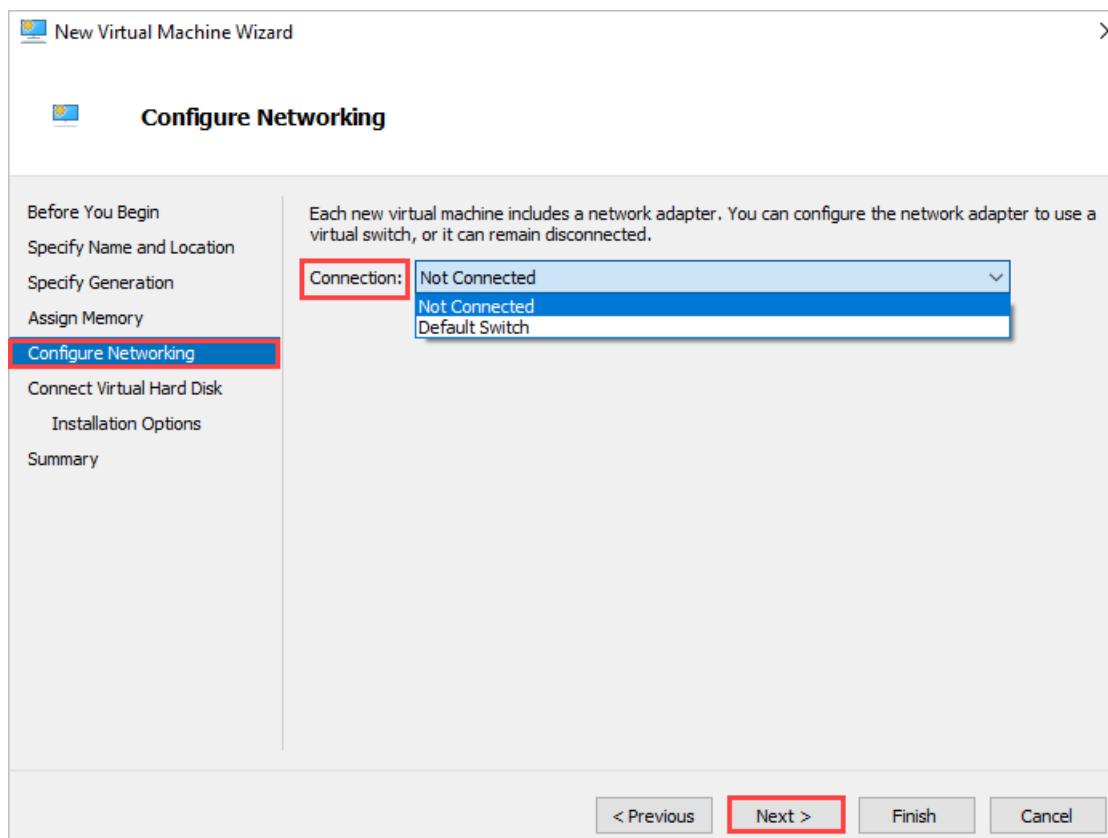
4. Under **Specify Generation**, select **Generation 1** or **Generation 2**. Then select **Next >**.



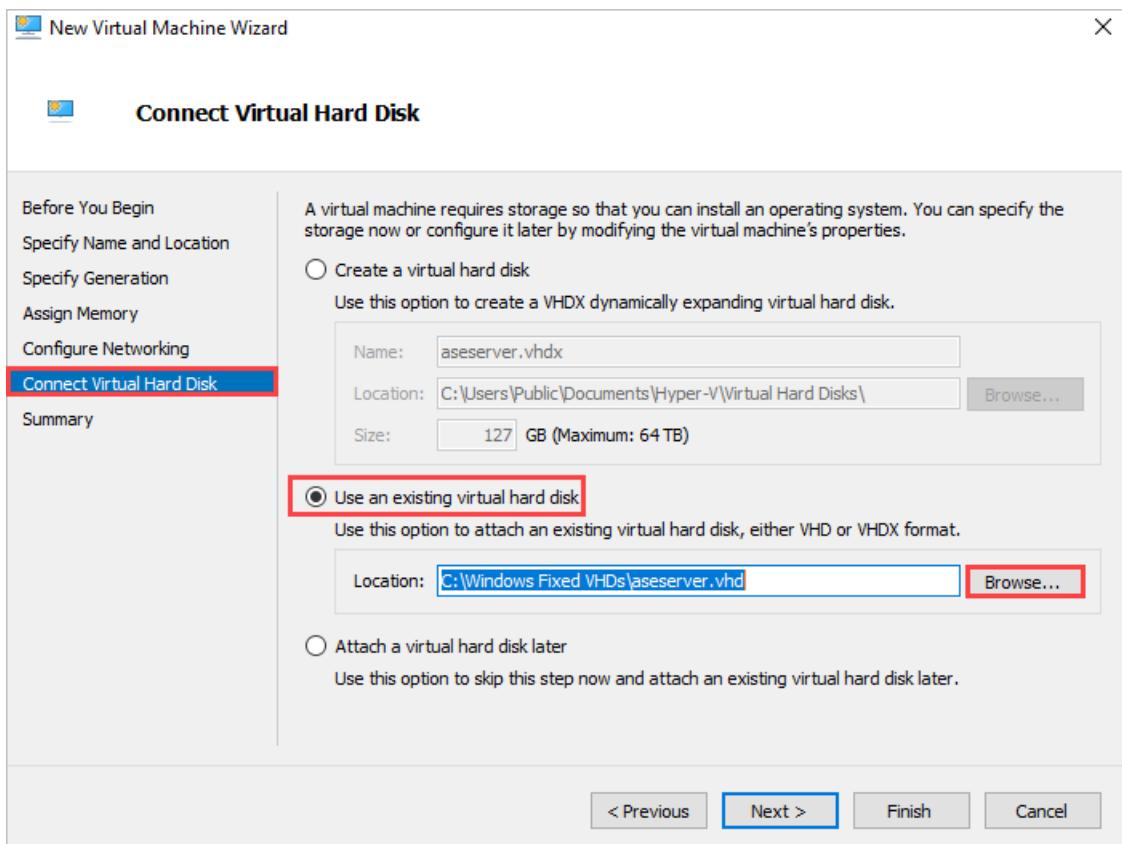
5. Under **Assign Memory**, assign the desired memory to the virtual machine. Then select **Next >**.



6. Under **Configure Networking**, enter your network configuration. Then select **Next >**.



7. Under **Connect Virtual Hard Disk**, select **Use an existing virtual hard disk** and browse to the fixed VHD you created in the previous procedure. Then select **Next >**.

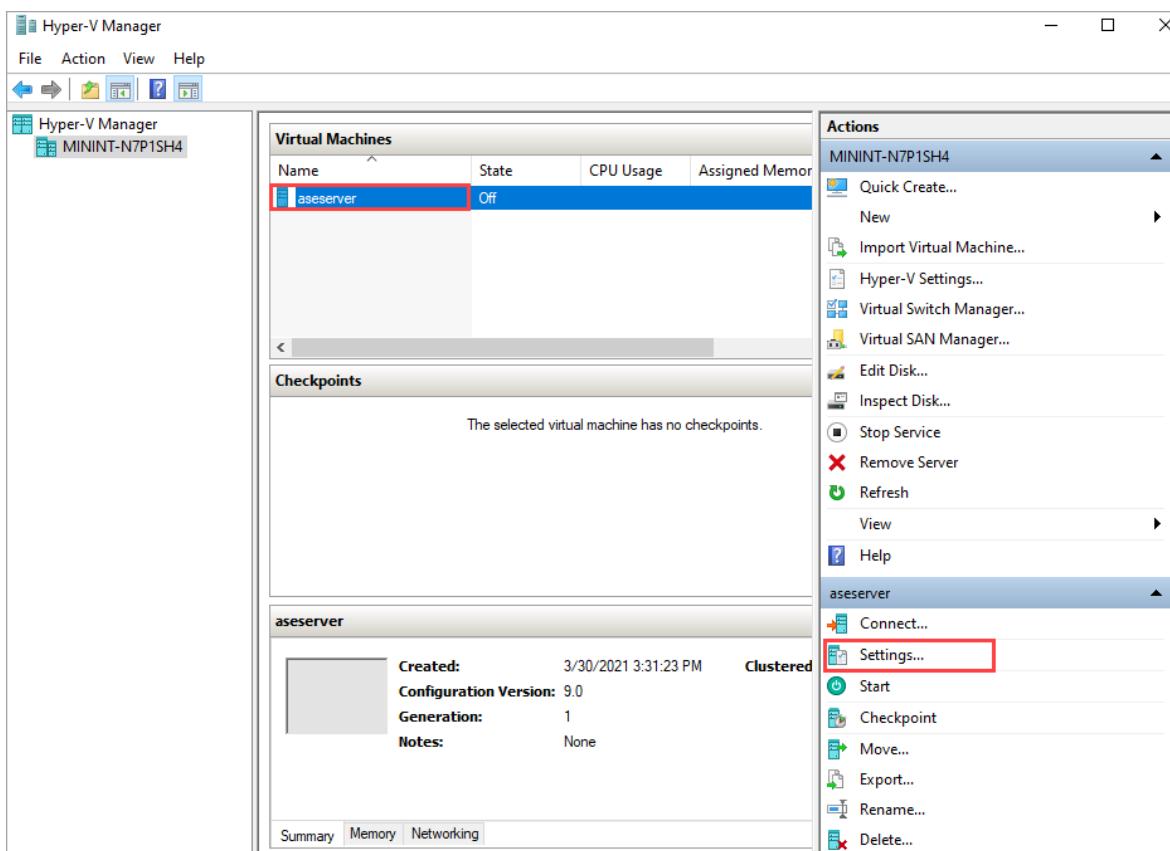


8. Review the summary, and select **Finish** to create the virtual machine.

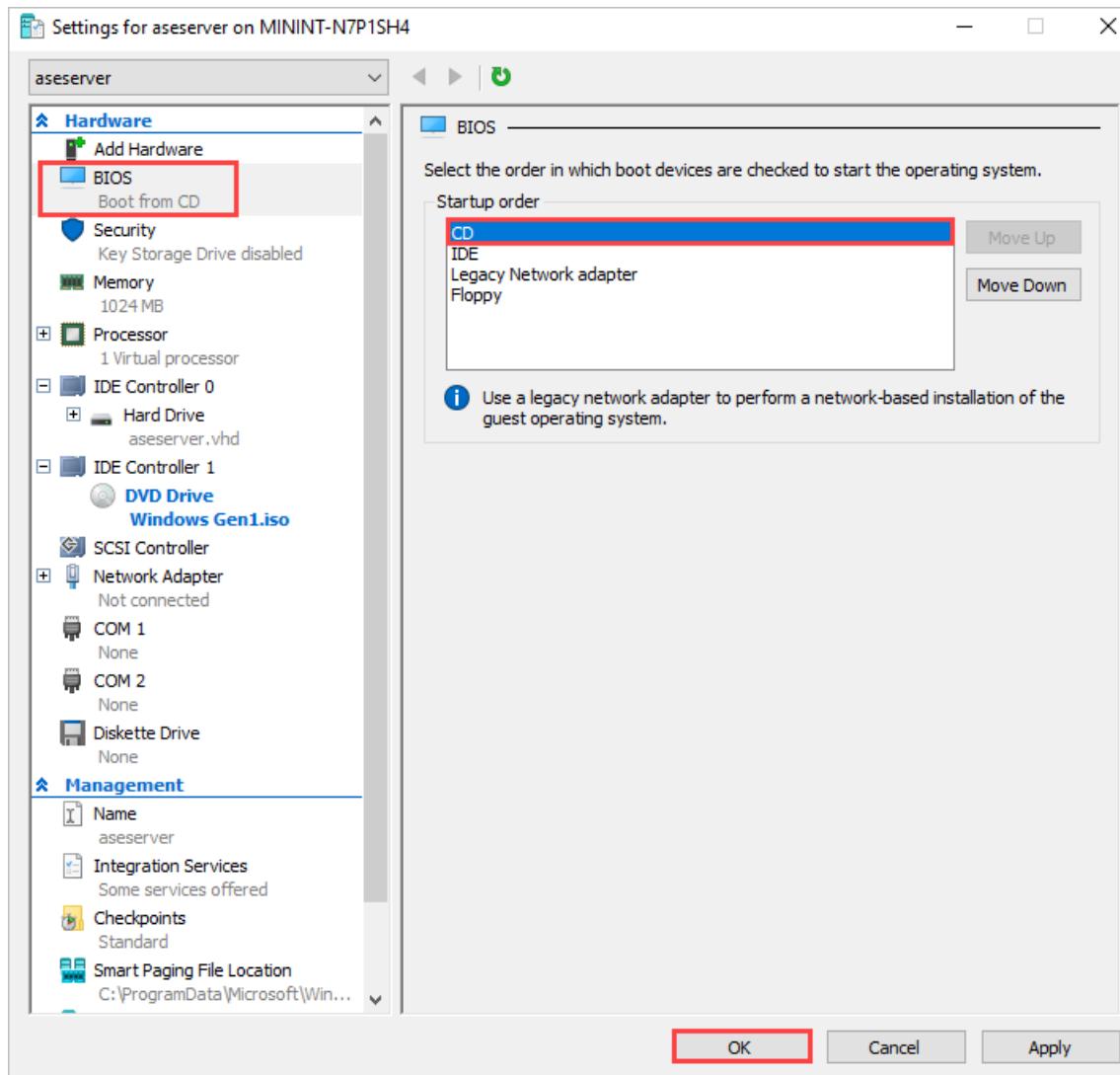
Mount ISO image on DVD drive of VM

After creating the new virtual machine, follow these steps to mount your ISO image on the DVD drive of the virtual machine:

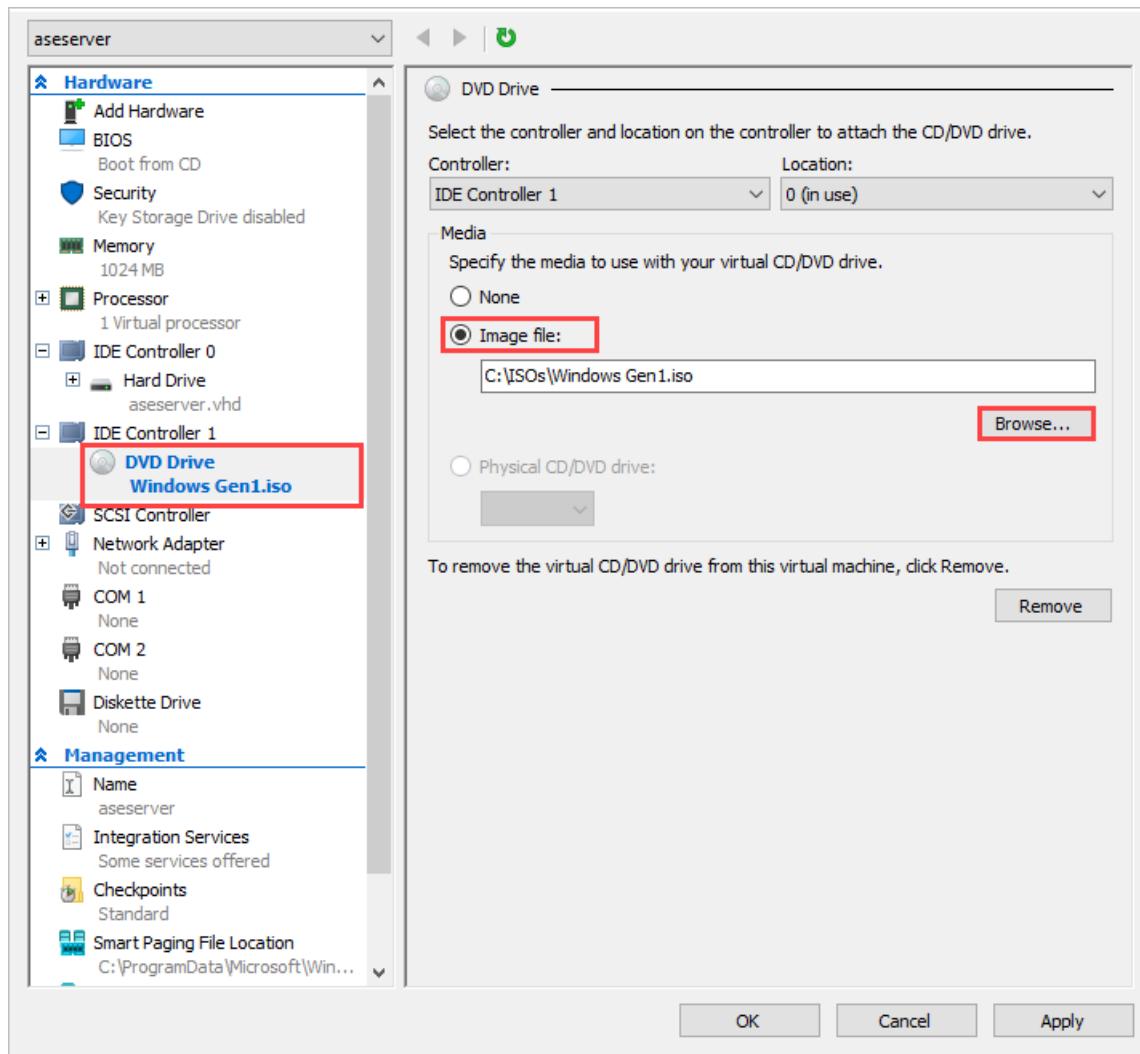
1. In Hyper-V Manager, select the VM you just created, and then select **Settings**.



2. Under BIOS, ensure that CD is at the top of the **Startup order** list.



3. Under **DVD Drive**, select **Image file**, and browse to your ISO image.

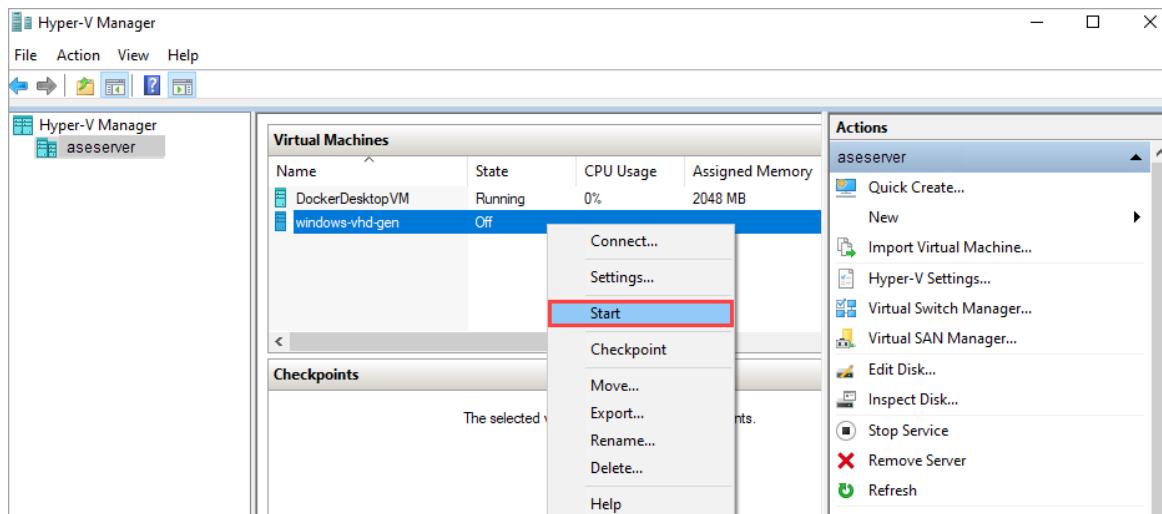


4. Select **OK** to save your VM settings.

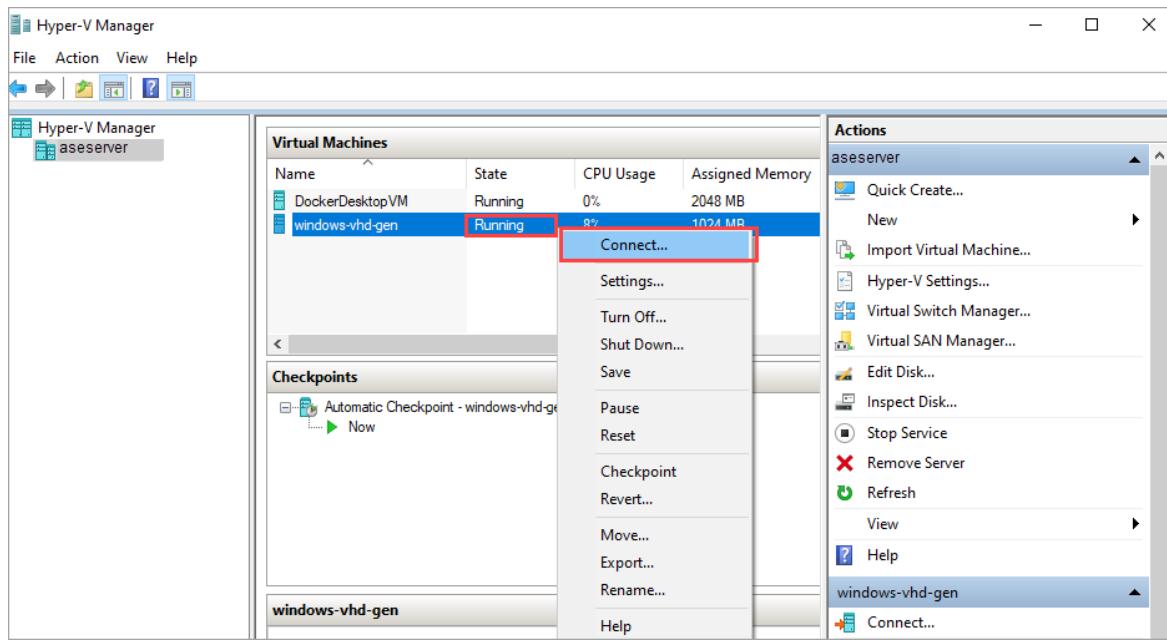
Start VM, and complete OS installation

To finish building your virtual machine, you need to start the virtual machine and walk through the operating system installation.

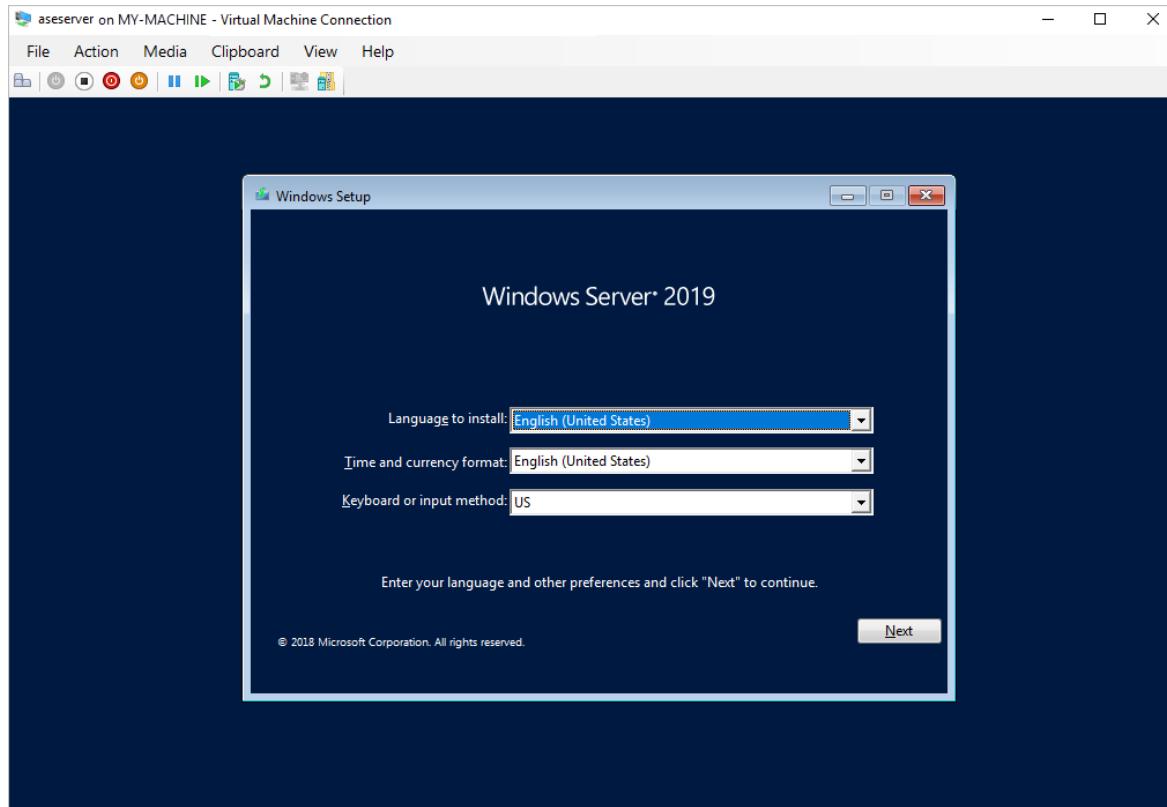
1. In **Hyper-V Manager**, in the scope pane, right-click the VM to open the context menu, and then select **Start**.



2. When the VM state is **Running**, select the VM, and then right-click and select **Connect**.



- The virtual machine boots into setup, and you can walk through the installation like you would on a physical computer.



NOTE

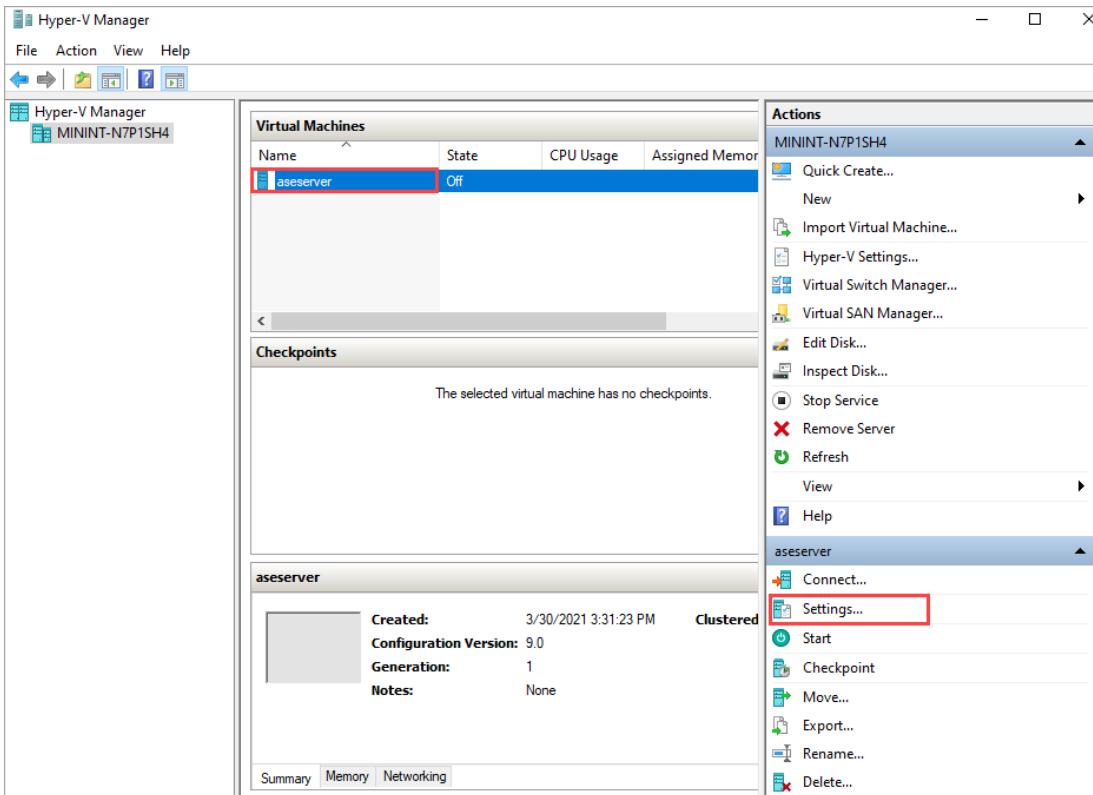
If you installed the Windows Server 2019 Standard operating system on your virtual machine, you'll need to change the BIOS setting to IDE before you [generalize the VHD](#).

Generalize the VHD

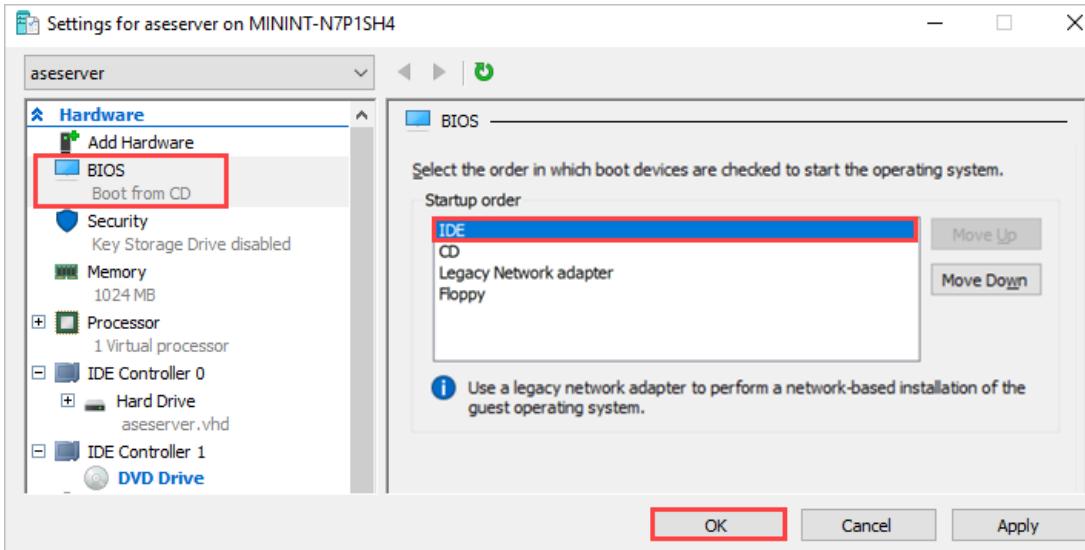
Use the *sysprep* utility to generalize the VHD.

- If you're generalizing a Windows Server 2019 Standard VM, before you generalize the VHD, make IDE the first BIOS setting for the virtual machine.

- In Hyper-V Manager, select the VM, and then select **Settings**.



- Under **BIOS**, ensure that IDE is at the top of the **Startup order** list. Then select **OK** to save the setting.



- Inside the VM, open a command prompt.
- Run the following command to generalize the VHD.

```
c:\windows\system32\sysprep\sysprep.exe /oobe /generalize /shutdown /mode:vm
```

For details, see [Sysprep \(system preparation\) overview](#).

- After the command is complete, the VM will shut down. **Do not restart the VM.**

Your VHD can now be used to create a generalized image to use on Azure Stack Edge Pro GPU.

Upload generalized VHD to Azure Blob storage

1. Upload the VHD to Azure blob storage. See the detailed instructions in [Upload a VHD using Azure Storage Explorer](#).
2. After the upload is complete, you can use the uploaded image to create VM images and VMs.

Next steps

- [Deploy a VM from a generalized image via Azure portal](#)
- [Prepare a generalized image from a Windows VHD to deploy VMs on Azure Stack Edge Pro GPU](#)
- [Prepare a specialized image and deploy VMs using the image](#)

Deploy a VM from a specialized image on your Azure Stack Edge Pro GPU device via Azure PowerShell

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the steps required to deploy a virtual machine (VM) on your Azure Stack Edge Pro GPU device from a specialized image.

To prepare a generalized image for deploying VMs in Azure Stack Edge Pro GPU, see [Prepare generalized image from Windows VHD](#) or [Prepare generalized image from an ISO](#).

About VM images

A Windows VHD or VHDX can be used to create a *specialized* image or a *generalized* image. The following table summarizes key differences between the *specialized* and the *generalized* images.

IMAGE TYPE	GENERALIZED	SPECIALIZED
Target	Deployed on any system.	Targeted to a specific system.
Setup after boot	Setup required at first boot of the VM.	No setup needed. Platform turns on the VM.
Configuration	Hostname, admin-user, and other VM-specific settings required.	Preconfigured.
Used when	Creating multiple new VMs from the same image.	Migrating a specific machine or restoring a VM from previous backup.

Workflow

The high-level workflow to deploy a VM from a specialized image is:

1. Copy the VHD to a local storage account on your Azure Stack Edge Pro GPU device.
2. Create a new managed disk from the VHD.
3. Create a new virtual machine from the managed disk and attach the managed disk.

Prerequisites

Before you can deploy a VM on your device via PowerShell, make sure that:

- You have access to a client that you'll use to connect to your device.
 - Your client runs a [Supported OS](#).
 - Your client is configured to connect to the local Azure Resource Manager of your device as per the instructions in [Connect to Azure Resource Manager for your device](#).

Verify the local Azure Resource Manager connection

Verify that your client can connect to the local Azure Resource Manager.

1. Call local device APIs to authenticate:

```
Login-AzureRMAccount -EnvironmentName <Environment Name>
```

2. Provide the username `EdgeArmUser` and the password to connect via Azure Resource Manager. If you do not recall the password, [Reset the password for Azure Resource Manager](#) and use this password to sign in.

Deploy VM from specialized image

The following sections contain step-by-step instructions to deploy a VM from a specialized image.

Copy VHD to local storage account on device

Follow these steps to copy VHD to local storage account:

1. Copy the source VHD to a local blob storage account on your Azure Stack Edge.
2. Take note of the resulting URI. You'll use this URI in a later step.

To create and access a local storage account, see the sections [Create a storage account](#) through [Upload a VHD](#) in the article: [Deploy VMs on your Azure Stack Edge device via Azure PowerShell](#).

Create a managed disk from VHD

Follow these steps to create a managed disk from a VHD that you uploaded to the storage account earlier:

1. Set some parameters.

```
$VhdURI = <URI of VHD in local storage account>
$DiskRG = <managed disk resource group>
$DiskName = <managed disk name>
```

Here is an example output.

```
PS C:\WINDOWS\system32> $VhdURI =
"https://myasevmsa.blob.myasegpuudev.wdshcsso.com/vhds/WindowsServer2016Datacenter.vhd"
PS C:\WINDOWS\system32> $DiskRG = "myasevm1rg"
PS C:\WINDOWS\system32> $DiskName = "myasemd1"
```

2. Create a new managed disk.

```
$DiskConfig = New-AzureRmDiskConfig -Location DBELocal -CreateOption Import -SourceUri $VhdURI
$disk = New-AzureRMDisk -ResourceGroupName $DiskRG -DiskName $DiskName -Disk $DiskConfig
```

Here is an example output. The location here is set to the location of the local storage account and is always `DBELocal` for all local storage accounts on your Azure Stack Edge Pro GPU device.

```
PS C:\WINDOWS\system32> $DiskConfig = New-AzureRmDiskConfig -Location DBELocal -CreateOption Import -  
SourceUri $VHDURI  
PS C:\WINDOWS\system32> $disk = New-AzureRMDisk -ResourceGroupName $DiskRG -DiskName $DiskName -Disk  
$DiskConfig  
PS C:\WINDOWS\system32>
```

Create a VM from managed disk

Follow these steps to create a VM from a managed disk:

1. Set some parameters.

```
$NicRG = <NIC resource group>  
$NicName = <NIC name>  
$IPConfigName = <IP config name>  
$PrivateIP = <IP address> #Optional  
  
$VMRG = <VM resource group>  
$VMName = <VM name>  
$VMSize = <VM size>
```

NOTE

The `PrivateIP` parameter is optional. Use this parameter to assign a static IP else the default is a dynamic IP using DHCP.

Here is an example output. In this example, the same resource group is specified for all the VM resources though you can create and specify separate resource groups for the resources if needed.

```
PS C:\WINDOWS\system32> $NicRG = "myasevm1rg"  
PS C:\WINDOWS\system32> $NicName = "myasevmnic1"  
PS C:\WINDOWS\system32> $IPConfigName = "myaseipconfig1"  
  
PS C:\WINDOWS\system32> $VMRG = "myasevm1rg"  
PS C:\WINDOWS\system32> $VMName = "myasetestvm1"  
PS C:\WINDOWS\system32> $VMSize = "Standard_D1_v2"
```

2. Get the virtual network information and create a new network interface.

This sample assumes you are creating a single network interface on the default virtual network `ASEVNET` that is associated with the default resource group `ASERG`. If needed, you could specify an alternate virtual network, or create multiple network interfaces. For more information, see [Add a network interface to a VM via the Azure portal](#).

```
$armVN = Get-AzureRMVirtualNetwork -Name ASEVNET -ResourceGroupName ASERG  
$ipConfig = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName -SubnetId $armVN.Subnets[0].Id [-  
PrivateIpAddress $PrivateIP]  
$nic = New-AzureRmNetworkInterface -Name $NicName -ResourceGroupName $NicRG -Location DBELocal -  
IpConfiguration $ipConfig
```

Here is an example output.

```

PS C:\WINDOWS\system32> $armVN = Get-AzureRMVirtualNetwork -Name ASEVNET -ResourceGroupName ASERG
PS C:\WINDOWS\system32> $ipConfig = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName -SubnetId
$armVN.Subnets[0].Id
PS C:\WINDOWS\system32> $nic = New-AzureRmNetworkInterface -Name $NicName -ResourceGroupName $NicRG -
Location DBELocal -IpConfiguration $ipConfig
WARNING: The output object type of this cmdlet will be modified in a future release.
PS C:\WINDOWS\system32>

```

3. Create a new VM configuration object.

```
$vmConfig = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
```

4. Add the network interface to the VM.

```
$vm = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $nic.Id
```

5. Set the OS disk properties on the VM.

```
$vm = Set-AzureRmVMOSDisk -VM $vm -ManagedDiskId $disk.Id -StorageAccountType StandardLRS -
CreateOption Attach -[Windows/Linux]
```

The last flag in this command will be either `-Windows` or `-Linux` depending on which OS you are using for your VM.

6. Create the VM.

```
New-AzureRmVM -ResourceGroupName $VMRG -Location DBELocal -VM $vm
```

Here is an example output.

```

PS C:\WINDOWS\system32> $vmConfig = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
PS C:\WINDOWS\system32> $vm = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $nic.Id
PS C:\WINDOWS\system32> $vm = Set-AzureRmVMOSDisk -VM $vm -ManagedDiskId $disk.Id -StorageAccountType
StandardLRS -CreateOption Attach -Windows
PS C:\WINDOWS\system32> New-AzureRmVM -ResourceGroupName $VMRG -Location DBELocal -VM $vm
WARNING: Since the VM is created using premium storage or managed disk, existing standard storage
account, myasevmsa, is used for
boot diagnostics.
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
----- -----
True          OK   OK
PS C:\WINDOWS\system32>

```

Delete VM and resources

This article used only one resource group to create all the VM resource. Deleting that resource group will delete the VM and all the associated resources.

1. First view all the resources created under the resource group.

```
Get-AzureRmResource -ResourceGroupName <Resource group name>
```

Here is an example output.

```

PS C:\WINDOWS\system32> Get-AzureRmResource -ResourceGroupName myasevm1rg

Name          : myasemd1
ResourceGroupName : myasevm1rg
 ResourceType    : Microsoft.Compute/disks
 Location       : dbelocal
 ResourceId     : /subscriptions/992601bc-b03d-4d72-598e-
d24eac232122/resourceGroups/myasevm1rg/providers/Microsoft.Compute/disk
s/myasemd1

Name          : myasetestvm1
ResourceGroupName : myasevm1rg
 ResourceType    : Microsoft.Compute/virtualMachines
 Location       : dbelocal
 ResourceId     : /subscriptions/992601bc-b03d-4d72-598e-
d24eac232122/resourceGroups/myasevm1rg/providers/Microsoft.Compute/virt
ualMachines/myasetestvm1

Name          : myasevnnic1
ResourceGroupName : myasevm1rg
 ResourceType    : Microsoft.Network/networkInterfaces
 Location       : dbelocal
 ResourceId     : /subscriptions/992601bc-b03d-4d72-598e-
d24eac232122/resourceGroups/myasevm1rg/providers/Microsoft.Network/netw
orkInterfaces/myasevnnic1

Name          : myasevmsa
ResourceGroupName : myasevm1rg
 ResourceType    : Microsoft.Storage/storageaccounts
 Location       : dbelocal
 ResourceId     : /subscriptions/992601bc-b03d-4d72-598e-
d24eac232122/resourceGroups/myasevm1rg/providers/Microsoft.Storage/stor
ageaccounts/myasevmsa

PS C:\WINDOWS\system32>

```

2. Delete the resource group and all the associated resources.

```
Remove-AzureRmResourceGroup -ResourceGroupName <Resource group name>
```

Here is an example output.

```

PS C:\WINDOWS\system32> Remove-AzureRmResourceGroup -ResourceGroupName myasevm1rg

Confirm
Are you sure you want to remove resource group 'myasevm1rg'
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
True
PS C:\WINDOWS\system32>

```

3. Verify that the resource group has deleted. Get all the resource groups that exist on the device.

```
Get-AzureRmResourceGroup
```

Here is an example output.

```
PS C:\WINDOWS\system32> Get-AzureRmResourceGroup

ResourceGroupName : ase-image-resourcegroup
Location         : dbelocal
ProvisioningState : Succeeded
Tags              :
ResourceId       : /subscriptions/992601bc-b03d-4d72-598e-d24eac232122/resourceGroups/ase-image-
resourcegroup

ResourceGroupName : ASERG
Location         : dbelocal
ProvisioningState : Succeeded
Tags              :
ResourceId       : /subscriptions/992601bc-b03d-4d72-598e-d24eac232122/resourceGroups/ASERG

ResourceGroupName : myaserg
Location         : dbelocal
ProvisioningState : Succeeded
Tags              :
ResourceId       : /subscriptions/992601bc-b03d-4d72-598e-d24eac232122/resourceGroups/myaserg

PS C:\WINDOWS\system32>
```

Next steps

- Prepare a generalized image from a Windows VHD to deploy VMs on Azure Stack Edge Pro GPU
- Prepare a generalized image from an ISO to deploy VMs on Azure Stack Edge Pro GPU

Use Azure Marketplace image to create VM image for your Azure Stack Edge Pro GPU

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

To deploy VMs on your Azure Stack Edge Pro GPU device, you need to create a VM image that you can use to create VMs. This article describes the steps that are required to create a VM image starting from an Azure Marketplace image. You can then use this VM image to deploy VMs on your Azure Stack Edge Pro GPU device.

VM image workflow

The following steps describe the VM image workflow using an Azure Marketplace workflow:

1. Connect to the Azure Cloud Shell or a client with Azure CLI installed.
2. Search the Azure Marketplace and identify your preferred image.
3. Create a new managed disk from the Marketplace image.
4. Export a VHD from the managed disk to Azure Storage account.
5. Clean up the managed disk.

For more information, go to [Deploy a VM on your Azure Stack Edge Pro device using Azure PowerShell](#).

Prerequisites

Before you can use Azure Marketplace images for Azure Stack Edge, make sure you're connected to Azure in either of the following ways.

You can use either the Azure Cloud Shell or a local Azure CLI.

- [Azure Cloud Shell](#) with the Bash environment. Or launch the Cloud Shell here.

[Launch Cloud Shell](#)

- Local Azure CLI, see how to [install the Azure CLI](#). If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
 - Sign in to the Azure CLI by using the `az login` command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
 - When you first use Azure CLI, install the Azure CLI extension. For more information about extensions, see [Use extensions with the Azure CLI](#).
 - Run `az version` to find the version and dependent libraries that are installed. To upgrade to the latest version, run `az upgrade`.

Search for Azure Marketplace images

You'll now identify a specific Azure Marketplace image that you wish to use. Azure Marketplace hosts thousands of VM images.

To find some of the most commonly used Marketplace images that match your search criteria, run the following command.

```
az vm image list --all [--publisher <Publisher>] [--offer <Offer>] [--sku <SKU>]
```

The last three flags are optional but excluding them returns a long list.

Some example queries are:

```
#Returns all images of type "Windows Server"  
az vm image list --all --publisher "MicrosoftWindowsServer" --offer "WindowsServer"  
  
#Returns all Windows Server 2019 Datacenter images from West US published by Microsoft  
az vm image list --all --location "westus" --publisher "MicrosoftWindowsServer" --offer "WindowsServer" --  
sku "2019-Datacenter"  
  
#Returns all VM images from a publisher  
az vm image list --all --publisher "Canonical"
```

Here is an example output when VM images of a certain publisher, offer, and SKU were queried.

```
PS /home/user> az vm image list --all --publisher "Canonical" --offer "UbuntuServer" --sku "12.04.4-LTS"
```

```
[
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201402270",
  "version": "12.04.201402270"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201404080",
  "version": "12.04.201404080"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201404280",
  "version": "12.04.201404280"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201405140",
  "version": "12.04.201405140"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201406060",
  "version": "12.04.201406060"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201406190",
  "version": "12.04.201406190"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201407020",
  "version": "12.04.201407020"
},
{
  "offer": "UbuntuServer",
  "publisher": "Canonical",
  "sku": "12.04.4-LTS",
  "urn": "Canonical:UbuntuServer:12.04.4-LTS:12.04.201407170",
  "version": "12.04.201407170"
}
]
```

PS /home/user>

In this example, we will select Windows Server 2019 Datacenter Core, version 2019.0.20190410. We will identify this image by its Universal Resource Number ("URN").

```
{
  "offer": "WindowsServer",
  "publisher": "MicrosoftWindowsServer",
  "sku": "2019-Datacenter-Core",
  "urn": "MicrosoftWindowsServer:WindowsServer:2019-Datacenter-Core:2019.0.20190410",
  "version": "2019.0.20190410"
},
{
  "offer": "WindowsServer",
  "publisher": "MicrosoftWindowsServer",
  "sku": "2019-datacenter-core-g2",
  "urn": "MicrosoftWindowsServer:WindowsServer:2019-datacenter-core-g2:17763.1158.2004131759",
  "version": "17763.1158.2004131759"
},
{
  "offer": "WindowsServer",
  "publisher": "MicrosoftWindowsServer",
  "sku": "2019-datacenter-core-g2",
  "urn": "MicrosoftWindowsServer:WindowsServer:2019-datacenter-core-g2:17763.1217.2005081535",
  "version": "17763.1217.2005081535"
},
```

Commonly used Marketplace images

Below is a list of URNs for some of the most commonly used images. If you just want the latest version of a particular OS, the version number can be replaced with "latest" in the URN. For example, "MicrosoftWindowsServer:WindowsServer:2019-Datacenter:Latest".

OS	SKU	VERSION	URN
Windows Server	2019 Datacenter	17763.1879.2104091832	MicrosoftWindowsServer:WindowsServer:2019-Datacenter:17763.1879.2104091832
Windows Server	2019 Datacenter (30 GB small disk)	17763.1879.2104091832	MicrosoftWindowsServer:WindowsServer:2019-Datacenter-smalldisk:17763.1879.2104091832
Windows Server	2019 Datacenter Core	17763.1879.2104091832	MicrosoftWindowsServer:WindowsServer:2019-Datacenter-Core:17763.1879.2104091832
Windows Server	2019 Datacenter Core (30 GB small disk)	17763.1879.2104091832	MicrosoftWindowsServer:WindowsServer:2019-Datacenter-Core-smalldisk:17763.1879.2104091832
Windows Desktop	Windows 10 20H2 Pro	19042.928.2104091209	MicrosoftWindowsDesktop:Windows-10:20h2-pro:19042.928.2104091209
Ubuntu Server	Canonical Ubuntu Server 18.04 LTS	18.04.202002180	Canonical:UbuntuServer:18.04-LTS:18.04.202002180
Ubuntu Server	Canonical Ubuntu Server 16.04 LTS	16.04.202104160	Canonical:UbuntuServer:16.04-LTS:16.04.202104160
CentOS	CentOS 8.1	8.1.2020062400	OpenLogic:CentOS:8_1:8.1.2020062400

OS	SKU	VERSION	URN
CentOS	CentOS 7.7	7.7.2020062400	OpenLogic:CentOS:7.7:7.7.2 020062400

Create a new managed disk from the Marketplace image

Create an Azure Managed Disk from your chosen Marketplace image.

1. Set some parameters.

```
$urn = <URN of the Marketplace image> #Example: "MicrosoftWindowsServer:WindowsServer:2019-Datacenter:Latest"
$diskName = <disk name> #Name for new disk to be created
$diskRG = <resource group> #Resource group that contains the new disk
```

2. Create the disk and generate a SAS access URL.

```
az disk create -g $diskRG -n $diskName --image-reference $urn
$sas = az disk grant-access --duration-in-seconds 36000 --access-level Read --name $diskName --
resource-group $diskRG
$diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

Here is an example output:

```
PS /home/user> $urn = "MicrosoftWindowsServer:WindowsServer:2019-Datacenter:Latest"
PS /home/user> $diskName = "newmanageddisk1"
PS /home/user> $diskRG = "newrgmd1"
PS /home/user> az disk create -g $diskRG -n $diskName --image-reference $urn
{
  "burstingEnabled": null,
  "creationData": {
    "createOption": "FromImage",
    "galleryImageReference": null,
    "imageReference": {
      "id": "/Subscriptions/db4e2fdb-6d80-4e6e-b7cd-736098270664/Providers/Microsoft.Compute/Locations/eastus/Publishers/MicrosoftWindowsServer/ArtifactTypes/VMImage/Offers/WindowsServer/Skus/2019-Datacenter/Versions/17763.1935.2105080716",
      "lun": null
    },
    "logicalSectorSize": null,
    "sourceResourceId": null,
    "sourceUniqueId": null,
    "sourceUri": null,
    "storageAccountId": null,
    "uploadSizeBytes": null
  },
  "diskAccessId": null,
  "diskIopsReadOnly": null,
  "diskIopsReadWrite": 500,
  "diskMBpsReadOnly": null,
  "diskMBpsReadWrite": 100,
  "diskSizeBytes": 136367308800,
  "diskSizeGb": 127,
  "diskState": "Unattached",
  "encryption": {
    "diskEncryptionSetId": null,
    "type": "EncryptionAtRestWithPlatformKey"
  },
  "encryptionSettingsCollection": null,
  "extendedLocation": null,
```

```

"hyperVGeneration": "V1",
"id": "/subscriptions/db4e2fdb-6d80-4e6e-b7cd-
736098270664/resourceGroups/newrgmd1/providers/Microsoft.Compute/disks/NewManagedDisk1",
"location": "eastus",
"managedBy": null,
"managedByExtended": null,
"maxShares": null,
"name": "NewManagedDisk1",
"networkAccessPolicy": "AllowAll",
"osType": "Windows",
"propertyUpdatesInProgress": null,
"provisioningState": "Succeeded",
"purchasePlan": null,
"resourceGroup": "newrgmd1",
"securityProfile": null,
"shareInfo": null,
"sku": {
  "name": "Premium_LRS",
  "tier": "Premium"
},
"supportsHibernation": null,
"tags": {},
"tier": "P10",
"timeCreated": "2021-06-08T00:39:34.205982+00:00",
"type": "Microsoft.Compute/disks",
"uniqueId": "1a649ad4-3b95-471e-89ef-1d2ed1f51525",
"zones": null
}

PS /home/user> $sas = az disk grant-access --duration-in-seconds 36000 --access-level Read --name $diskName
--resource-group $diskRG
PS /home/user> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
PS /home/user>

```

Export a VHD from the managed disk to Azure Storage

This step will export a VHD from the managed disk to your preferred Azure blob storage account. This VHD can then be used to create VM images on Azure Stack Edge.

1. Set the destination storage account where the VHD will be copied.

```

$storageAccountName = <destination storage account name>
$containerName = <destination container name>
$destBlobName = <blobname.vhd> #Blob that will be created, including .vhd extension
$storageAccountKey = <storage account key>

```

2. Copy the VHD to the destination storage account.

```

$destContext = New-AzureStorageContext -StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS -DestContainer $containerName -DestContext
$destContext -DestBlob $destBlobName

```

The VHD copy will take several minutes to complete. Ensure the copy has completed before proceeding by running the following command. The status field will show "Success" when complete.

```
Get-AzureStorageBlobCopyState -Container $containerName -Context $destContext -Blob $destBlobName
```

Here is an example output:

```

PS /home/user> $storageAccountName = "edgeazurevmeus"
PS /home/user> $containerName = "azurevmmmp"
PS /home/user> $destBlobName = "newblobmp.vhd"
PS /home/user> $storageAccountKey =
"n9sCytWLdTBz0F4Sco9SkPGWp6BJBtf7BJBk79msf1PfxJGQdqSfu6TboZWZ10xyZdc4y+Att08cC9B79jB0YA=="

PS /home/user> $destContext = New-AzureStorageContext -StorageAccountName $storageAccountName -
StorageAccountKey $storageAccountKey
PS /home/user> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS -DestContainer $containerName -
DestContext $destContext -DestBlob $destBlobName

    AccountName: edgeazurevmeus, ContainerName: azurevmmmp



| Name          | BlobType     | Length | ContentType | LastModified         |
|---------------|--------------|--------|-------------|----------------------|
| AccessTier    | SnapshotTime |        | IsDeleted   | VersionId            |
| ----          | -----        | -----  | -----       | -----                |
| newblobmp.vhd | PageBlob     | -1     |             | 2021-06-08 00:50:10Z |
|               |              |        | False       |                      |



PS /home/user> Get-AzureStorageBlobCopyState -Container $containerName -Context $destContext -Blob
$destBlobName

CopyId : 24a1e3f5-886a-490d-9dd7-562bb4acff58
CompletionTime :
Status : Pending
Source : https://md-lfn221fppr2c.blob.core.windows.net/d4tb2hp5ff2q/abcd?sv=2018-03-
28&sr=b&si=4f588db1-9aac-44d9-9607-35497cc08a7f
BytesCopied : 696254464
TotalBytes : 136367309312
StatusDescription :
DestinationSnapshotTime :

PS /home/user> Get-AzureStorageBlobCopyState -Container $containerName -Context $destContext -Blob
$destBlobName

CopyId : 24a1e3f5-886a-490d-9dd7-562bb4acff58
CompletionTime : 6/8/2021 12:57:26 AM +00:00
Status : Success
Source : https://md-lfn221fppr2c.blob.core.windows.net/d4tb2hp5ff2q/abcd?sv=2018-03-
28&sr=b&si=4f588db1-9aac-44d9-9607-35497cc08a7f
BytesCopied : 136367309312
TotalBytes : 136367309312
StatusDescription :
DestinationSnapshotTime :

```

Clean up the managed disk

To delete the managed disk you created, follow these steps:

```

az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes

```

The deletion takes a couple minutes to complete.

Next steps

[Deploy VMs on your Azure Stack Edge Pro GPU device.](#)

Deploy VMs on your Azure Stack Edge Pro GPU device via the Azure portal

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

You can create and manage virtual machines (VMs) on an Azure Stack Edge Pro GPU device by using the Azure portal, templates, and Azure PowerShell cmdlets, and via the Azure CLI or Python scripts. This article describes how to create and manage a VM on your Azure Stack Edge Pro GPU device by using the Azure portal.

IMPORTANT

You will need to enable multifactor authentication for the user who manages the VMs and images that are deployed on your device from the cloud. The cloud operations will fail if the user doesn't have multifactor authentication enabled. For steps to enable multifactor authentication, see [Manage authentication methods for Azure AD Multi-Factor Authentication](#).

VM deployment workflow

The high-level summary of the deployment workflow is as follows:

1. Enable a network interface for compute on your Azure Stack Edge device. This step creates a virtual switch on the specified network interface.
2. Enable cloud management of VMs from the Azure portal.
3. Upload a VHD to an Azure Storage account by using Azure Storage Explorer.
4. Use the uploaded VHD to download the VHD onto the device, and create a VM image from the VHD.
5. Use the resources created in the previous steps:

- a. VM image that you created.
- b. Virtual switch associated with the network interface on which you enabled compute.
- c. Subnet associated with the virtual switch.

And create or specify the following resources inline:

- a. VM name, choose a supported VM size, sign-in credentials for the VM.
- b. Create new data disks or attach existing data disks.
- c. Configure static or dynamic IP for the VM. If you're providing a static IP, choose from a free IP in the subnet range of the network interface enabled for compute.

Use the preceding resources to create a VM.

Prerequisites

Before you begin to create and manage VMs on your device via the Azure portal, make sure that:

1. You've completed the network settings on your Azure Stack Edge Pro GPU device as described in [Step 1: Configure an Azure Stack Edge Pro GPU device](#).
 - a. You've enabled a network interface for compute. This network interface IP is used to create a

virtual switch for the VM deployment. In the local UI of your device, go to **Compute**. Select the network interface that you'll use to create a virtual switch.

IMPORTANT

You can configure only one port for compute.

- b. Enable compute on the network interface. Azure Stack Edge Pro GPU creates and manages a virtual switch corresponding to that network interface.
2. You have access to a Windows or Linux VHD that you'll use to create the VM image for the VM you intend to create.

Deploy a VM

Follow these steps to create a VM on your Azure Stack Edge Pro GPU device.

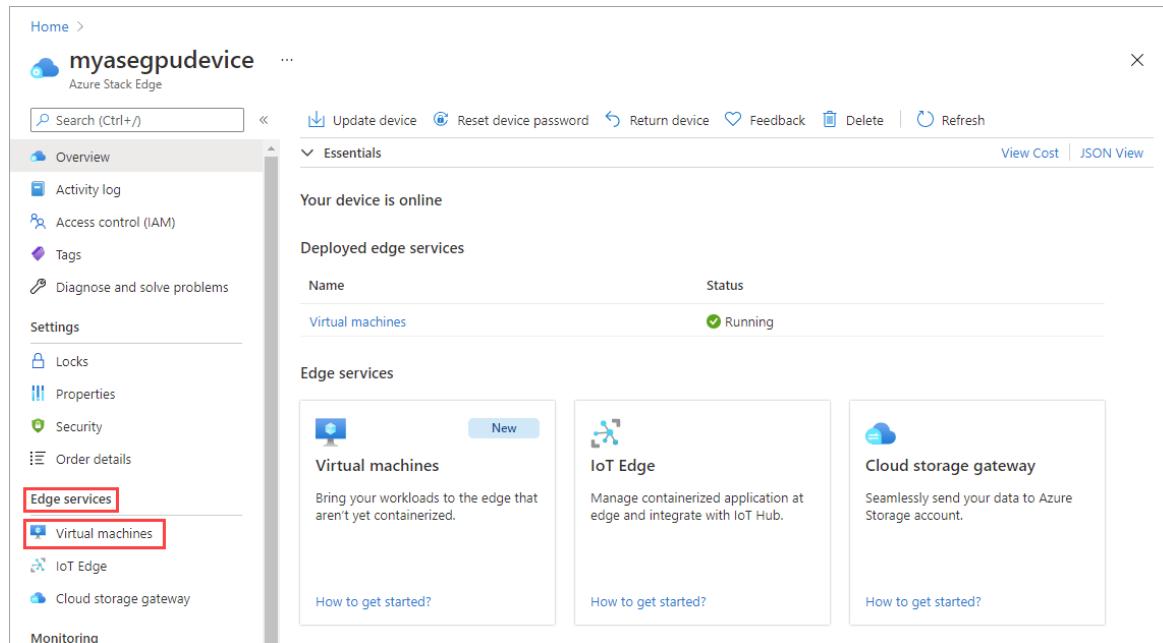
Add a VM image

1. Upload a VHD to an Azure Storage account. Follow the steps in [Use Storage Explorer for upload](#).

For information about preparing the VHD, see [Prepare a generalized image from a Windows VHD](#).

[Troubleshoot VM image uploads](#).

2. In the Azure portal, go to the Azure Stack Edge resource for your device. Then go to **Edge services > Virtual machines**.



The screenshot shows the Azure Stack Edge Overview page for the device 'myasegpudevice'. The left sidebar has a 'Edge services' section with 'Virtual machines' highlighted and a red box around it. Other options like 'IoT Edge' and 'Cloud storage gateway' are also listed. The main content area shows 'Your device is online' and a table for 'Deployed edge services' with a single row for 'Virtual machines' which is 'Running'. Below this is a section for 'Edge services' with three cards: 'Virtual machines' (New), 'IoT Edge', and 'Cloud storage gateway'.

3. On the **Overview** page. Select **Enable** to enable virtual machine cloud management.

The screenshot shows the 'Virtual machines | Overview' page. The 'Overview' tab is selected, indicated by a red box. The left sidebar includes links for Activity log, Images, Virtual machines, Resources, and Deployments. The main area has two sections: 'Images' (showing 1 total image named 'myaselinuxvminimage1') and 'Virtual machines' (with a note about ensuring the correct image is available). A large blue 'Add virtual machine' button is at the bottom.

4. The first step is to add a VM image. You've already uploaded a VHD into the storage account in the earlier step. You'll use this VHD to create a VM image.

Select **+ Add image** to download the VHD from the storage account and add it to the device. The download process takes several minutes depending on the size of the VHD and the internet bandwidth available for the download.

This screenshot is identical to the one above, but the 'Add image' button in the top navigation bar is highlighted with a red box.

5. On the **Add image** pane, make the following field entries. Then select **Add**.

FIELD	DESCRIPTION
Download from storage blob	Browse to the location of the storage blob in the storage account where you uploaded the VHD.
Download to	Automatically set to the current device where you're deploying the VM.
Edge resource group	Select the resource group to add the image to.
Save image as	The name for the VM image that you're creating from the VHD you uploaded to the storage account.
OS type	Choose from Windows or Linux as the operating system of the VHD you'll use to create the VM image.
VM generation	Choose Gen 1 or Gen 2 as the generation of the image you'll use to create the VM.

Add image

...

Prepare the VHDs that you'll use to create images on your Azure Stack Edge device. [Learn more](#) about how to prepare the VHD.

To download VHD from storage account to the device, enter the details of the associated storage account. After the download is complete, the VHD is converted to a VM image. Depending on the file size and internet connection speed, this step may take hours.

Download from storage blob [①](#)

[Browse](#)

Download to

PortalAseDevice3 (This device)

Edge resource group [* ①](#)

▼
[Create new](#)Save image as [* ①](#)

OS type [* ①](#)
 Windows Linux
VM generation [* ①](#)
 Gen 1 Gen 2
[Add](#)

- The VHD is downloaded, and the VM image is created. Image creation takes several minutes to complete. You'll see a notification for the successful completion of the VM image.

Virtual machines | Overview

Manage your virtual machines from the cloud

Images

Total 2

myaselinuxvimage1	Linux
myaselinuxvimage2	Linux

Virtual machines

Ensure you have the correct image is available on the device. If not download the right image file, then proceed with creating a virtual machine.

[Add virtual machine](#)

Steps to deploy virtual machine

- After the VM image is successfully created, it's added to the list of images on the **Images** pane.

The screenshot shows a table of images. The columns are: Image name, Status, OS, Edge resource group, and VM generation. The data includes:

Image name	Status	OS	Edge resource group	VM generation
arctest	Downloaded	Linux	ASERG	V1
ubuntu18gen2image2	Downloaded	Linux	GVANB-RG	V2
ubuntu18image1	Downloaded	Linux	GVANB-RG	V1
Ubuntugen2test1	Downloaded	Linux	RG1	V2
windows2019gen2image1	Downloaded	Windows	GVANB-RG	V2
windowsimage1	Downloaded	Windows	GVANB-RG	V1
wingen1image1	Downloaded	Windows	GVANB-RG	V1

The **Deployments** pane updates to indicate the status of the deployment.

The screenshot shows a table of deployments. The columns are: Name, Type, Status, Last modified, and Duration. The data includes:

Name	Type	Status	Last modified	Duration
myaselinuxvimage2	Image	Completed	6/9/2021 5:09:12 PM	10 minutes 0 seconds
myaselinuxvimage1	Image	Completed	6/8/2021 2:09:04 PM	8 minutes 6 seconds

The newly added image is also displayed on the **Overview** page.

The screenshot shows the Overview page. On the left, the sidebar has 'Overview' selected. In the main area, there's a 'Images' section with a total count of 2. The images listed are 'myaselinuxvimage1' and 'myaselinuxvimage2'. To the right, there's a 'Virtual machines' section with a note about ensuring the correct image is available.

Add a VM

Follow these steps to create a VM after you've created a VM image.

1. On the **Overview** page for **Virtual machines**, select **+ Add virtual machine**.

The screenshot shows the Overview page. The sidebar has 'Overview' selected. The main area features a 'Virtual machines' section with a note about ensuring the correct image is available. Below it is a 'Add virtual machine' button.

2. On the **Basics** tab, input the following parameters.

PARAMETER	DESCRIPTION
Virtual machine name	Enter a name for the new virtual machine.
Edge resource group	Create a new resource group for all the resources associated with the VM.
Image	Select from the VM images available on the device.
Size	Choose from the Supported VM sizes . For a GPU VM, select a VM size from NCsT4-v3-series .
Username	Use the default username azureuser for the admin to sign in to the VM.
Authentication type	Choose from an SSH public key or a user-defined password.
SSH public key	Displayed when you select the SSH public key authentication type. Paste in the SSH public key.
Password	Displayed when you select the Password authentication type. Enter a password to sign in to the VM. The password must be at least 12 characters long and meet the defined complexity requirements .
Confirm password	Enter the password again.

Home > myasegpudev > Virtual machines >

Add a virtual machine

myasegpudev

Basics Disks Networking Advanced Review + create

To create a Linux or Windows VM, use a VM image from your device. [Learn more](#)

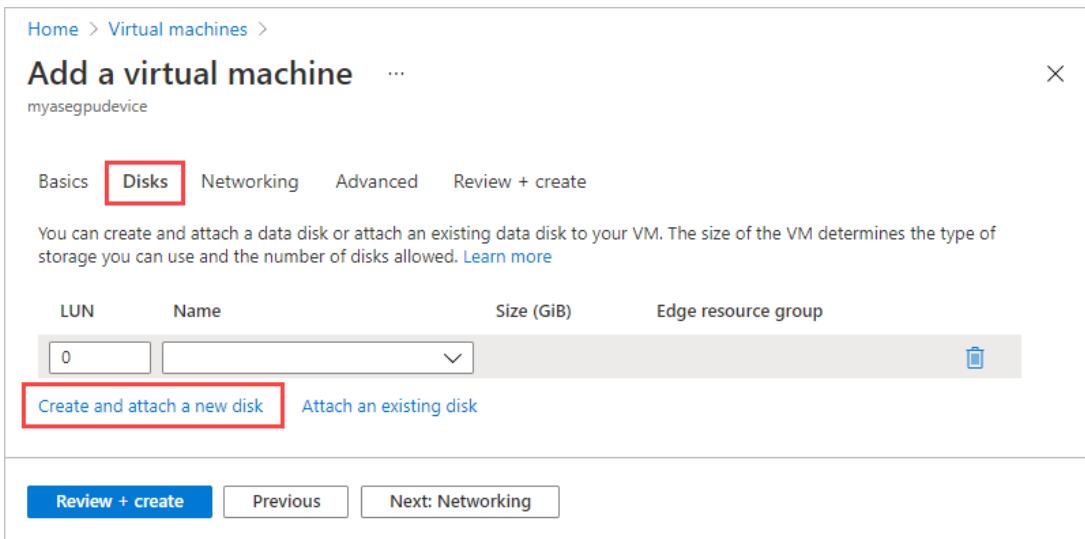
Virtual machine name *	myasewindowsvm1
Edge resource group *	myaserg
Image *	linuxvmimg (Linux)
Size *	Standard_D1_v2 - 1 vcpus, 3.58 GB memory
Administrator account	
Username *	azureuser
Authentication type *	SSH public key Password
Password *
Confirm password *

[Review + create](#) [Previous](#) [Next: Disks](#)

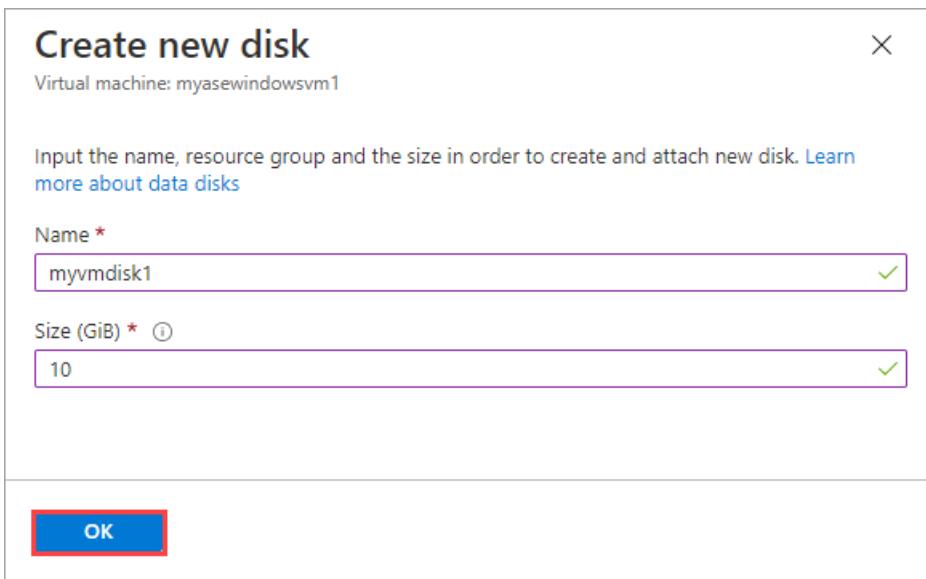
Select **Next: Disks**.

3. On the **Disks** tab, you'll attach disks to your VM.

a. You can choose to **Create and attach a new disk** or **Attach an existing disk**.



b. Select **Create and attach a new disk**. On the **Create new disk** pane, provide a name for the disk and the size in GiB.



c. Repeat the preceding process to add more disks. After the disks are created, they show up on the **Disks** tab. Select **Next: Networking**.

4. On the **Networking** tab, you'll configure the network connectivity for your VM.

PARAMETER	DESCRIPTION
Virtual network	From the dropdown list, select the virtual switch created on your Azure Stack Edge device when you enabled compute on the network interface.
Subnet	This field is automatically populated with the subnet associated with the network interface on which you enabled compute.

PARAMETER	DESCRIPTION
IP address	Provide a static or a dynamic IP for your VM. The static IP should be an available, free IP from the specified subnet range.

Home > myasegpudev > Virtual machines >

Add a virtual machine

myasegpudev

Basics Disks **Networking** Advanced Review + create

To configure the network connectivity for your VM, specify a virtual network and an IP address. The subnet is automatically populated based on the subnet of the device network interface enabled for compute. [Learn more](#)

Network interface
When creating a virtual machine, a network interface will be created for you.

Virtual network* ⓘ ASEVNET

Subnet ⓘ ASEVNETsubNet (10.57.48.0/21)

IP address * ⓘ Static Dynamic

Review + create **Previous** **Next: Advanced**

Select **Next: Advanced**. On the Advanced tab, you can select an extension to install during VM deployment, and you can specify a `cloud-init` script to customize your VM.

5. If you want to install an extension on your VM when you create it, choose **Select an extension to install**. Then select the extension on the **Add extension** screen.

For detailed steps to install a GPU extension during VM deployment, see [Deploy GPU VMs](#).

Home > Virtual machines >

Add a virtual machine

myasegpudevice

Basics Disks Networking **Advanced** Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions
Extensions provide post-deployment configuration and automation.

For a Red Hat image, follow the [steps to add the GPU extension](#) to the VM. Add the extension after the VM is created.

Extensions ⓘ **1 Select an extension to install**

Custom data and cloud init
Pass a cloud-init script, configuration file, or other saved on the VM in a known location. [Learn more](#)

Custom data

2

NVIDIA GPU Driver Extension
Microsoft Corp.

Review + create **Previous** **Next: Review + create**

6. If you want to use the `cloud-init` utility to customize the new VM on its first boot, on the **Advanced** tab, paste your `cloud-init` script into the **Custom data** box under **Custom data and cloud init**.

For more information about using `cloud-init`, see [Cloud-init overview](#).

The screenshot shows the 'Add a virtual machine' wizard with the 'Advanced' tab selected. In the 'Custom data and cloud init' section, a red box highlights the following cloud-init script:

```
#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
```

A tooltip message at the bottom left of the 'Custom data' box states: "Custom data on the selected image will be processed by cloud-init. Learn more about custom data and cloud init".

At the bottom, there are three buttons: 'Review + create' (highlighted in blue), 'Previous', and 'Next: Review + create'.

Select **Next: Review + Create**.

7. On the **Review + Create** tab, review the specifications for the VM. Then select **Create**.

Home > Virtual machines >

Add a virtual machine

myasegpudevice

✓ All validations have passed.

Basics Disks Networking Advanced **Review + create**

Review the details before you create your virtual machine.

Basics

Virtual machine name	myaselinuxvm3
Edge resource group	myaserg
Image	myaseazlinuxvmimage
Size	Standard_NC4as_T4_v3
Username	azureuser

Disks

Data disks	1
------------	---

Networking

Virtual network	ASEVNET
Subnet	ASEVNETsubNet
IP address	NA
IP address assignment	Dynamic

Advanced

Extensions	NVIDIA GPU Driver Extension
Cloud init	Yes

Create Previous Next

- The VM creation starts and can take up to 20 minutes. You can go to **Deployments** to monitor the VM creation.

Home > myasegpudev > Virtual machines

Virtual machines | Deployments

PREVIEW

Search (Ctrl+ /) Refresh

Overview Images Virtual machines Deployments

Filter by name Type :All Status :All Last modified :All

Name ↑↓	Type ↑↓	Status ↑↓	Last modified ↑↓	Duration
myaselinuxvm3	Virtual machine	Completed	3/29/2021 3:47:19 PM	4 minutes 55 seconds
linuxvmimg	Image	Completed	3/29/2021 2:34:18 PM	8 minutes 24 seconds
windowsvmimg	Image	Completed	3/29/2021 11:15:34 AM	11 minutes 52 seconds

- After the VM is successfully created, you'll see your new VM on the **Overview** pane.

The screenshot shows the 'Virtual machines | Overview' page. At the top, there's a search bar and buttons for 'Add virtual machine', 'Add image', and 'Refresh'. A red box highlights the 'Overview' tab in the left sidebar. Below the sidebar are two main sections: 'Images' (Total 2, listing 'linuxvmmimg' as Linux and 'windowsvmmimg' as Windows) and 'Virtual machines' (Total 1, listing 'myasewindowsvm1'). A red box highlights 'myasewindowsvm1' in the 'Virtual machines' section.

10. Select the newly created VM to go to **Virtual machines**.

The screenshot shows the 'Virtual machines | Virtual machines' page. The left sidebar has tabs for 'Overview', 'Images', 'Virtual machines' (which is selected and highlighted with a red box), and 'Deployments'. The main area lists the VM 'myasewindowsvm1' with details: Name (myasewindowsvm1), Status (Running, highlighted with a red box), Size (Standard_D1_v2), Disks (2), and Edge resource group (MYASERG). A red box highlights the 'myasewindowsvm1' row.

Select the VM to see the details.

The screenshot shows the 'Virtual machine | Overview' page for 'myasewindowsvm1'. The top navigation bar includes 'Start', 'Restart', 'Stop', 'Delete', and 'Refresh' buttons. The left sidebar has tabs for 'Virtual machine' (selected and highlighted with a red box), 'Size', 'Networking', and 'Disks'. The 'Virtual machine' section displays details: Computer name (myasewindowsvm1), OS (Linux), and Status (Running). The 'Size' section shows VM Size (D1_v2). The 'Networking' section shows a table for Network interface (myasewindowsvm1nic (primary)) with IP Address (10.57.53.186), Virtual network (ASEVNET), Subnet (ASEVNETsubNet), and IP allocation method (Dynamic). A red box highlights the 'Network interface' row in the networking table. The 'Disks' section shows an OS disk (myasewindowsvm1_disk1_6c2f7d3) with Storage type (Standard) and Size (30 GB), and a Data disk (myvmdisk1) with LUN (0), Storage type (Standard), and Size (10 GB).

You'll use the IP address for the network interface to connect to the VM.

Connect to a VM

Depending on whether you created a Linux or Windows VM, the steps to connect can be different. You can't connect to the VMs deployed on your device via the Azure portal. Follow the steps to connect to your Linux or Windows VM.

Connect to a Linux VM

Follow these steps to connect to a Linux VM.

Connect to the VM by using the private IP that you passed during the VM creation.

1. Open an SSH session to connect with the IP address.

```
ssh -l <username> <ip address>
```

2. At the prompt, provide the password that you used when you created the VM.

If you need to provide the SSH key, use this command.

```
ssh -i c:/users/Administrator/.ssh/id_rsa Administrator@5.5.41.236
```

Here's an example output when you connect to the VM:

```
PS C:\WINDOWS\system32> ssh -l myazuser "10.126.76.60"
The authenticity of host '10.126.76.60 (10.126.76.60)' can't be established.
ECDSA key fingerprint is SHA256:V649Zbo58zAYMKreeP7M6w7Na0Yf9QPg4SM7JZVV0E4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.126.76.60' (ECDSA) to the list of known hosts.
myazuser@10.126.76.60's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-1013-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information disabled due to load higher than 1.0

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

284 packages can be updated.
192 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

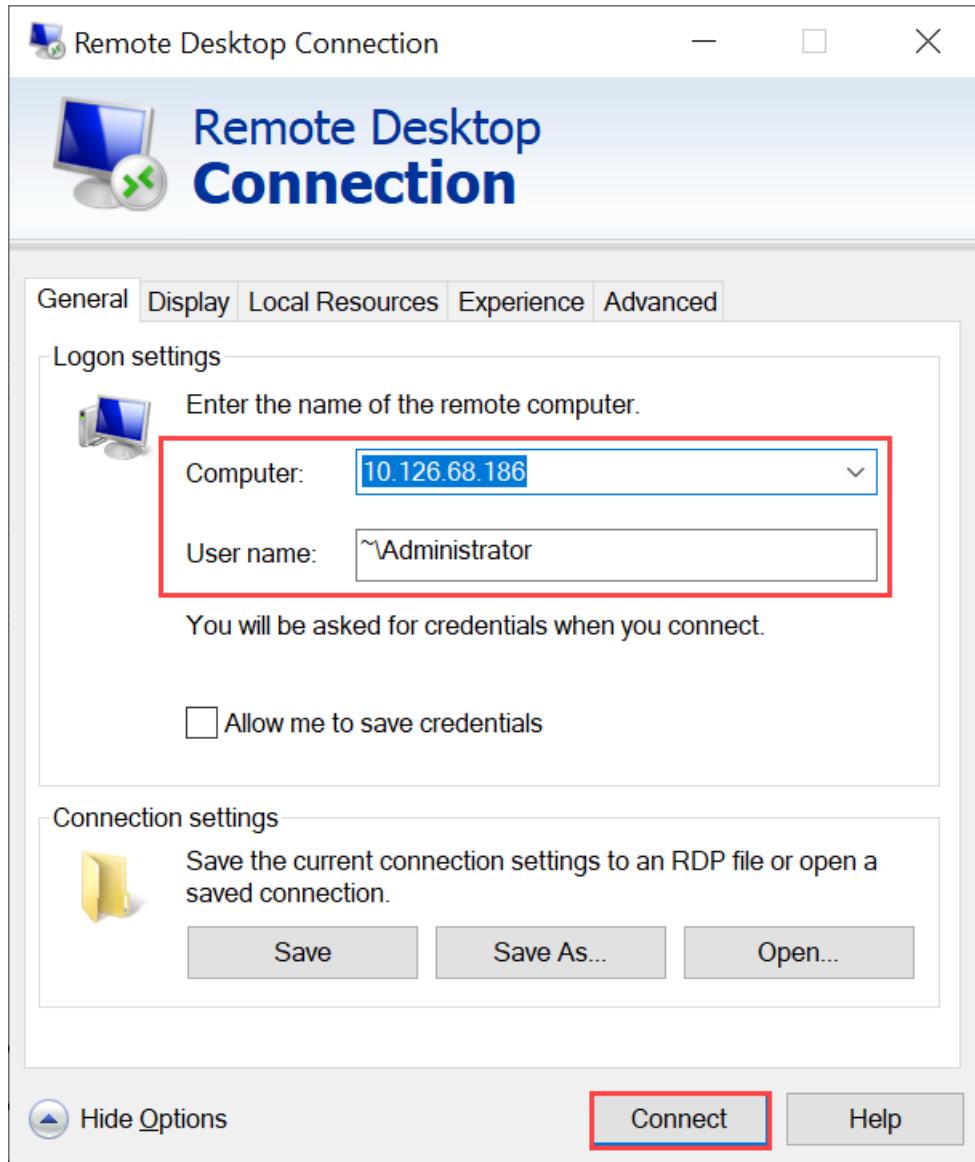
myazuser@myazvmfriendlyname:~$ client_loop: send disconnect: Connection reset
PS C:\WINDOWS\system32>
```

Connect to a Windows VM

Follow these steps to connect to a Windows VM.

Connect to your Windows VM by using the Remote Desktop Protocol (RDP) via the IP that you passed during the VM creation.

1. On your client, open RDP.
2. Go to **Start**, and then enter **mstsc**.
3. On the **Remote Desktop Connection** pane, enter the IP address of the VM and the access credentials you used in the VM template parameters file. Then select **Connect**.



NOTE

You might need to approve connecting to an untrusted machine.

You're now signed in to your VM that runs on the appliance.

Next steps

- Deploy a cloud managed VM via a script
- Deploy a GPU VM
- Troubleshoot VM deployment
- Monitor VM activity on your device
- Monitor CPU and memory on a VM

Deploy VMs on your Azure Stack Edge Pro GPU device via templates

9/21/2022 • 21 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This tutorial describes how to create and manage a VM on your Azure Stack Edge Pro device using templates. These templates are JavaScript Object Notation (JSON) files that define the infrastructure and configuration for your VM. In these templates, you specify the resources to deploy and the properties for those resources.

Templates are flexible in different environments as they can take parameters as input at runtime from a file. The standard naming structure is `TemplateName.json` for the template and `TemplateName.parameters.json` for the parameters file. For more information on ARM templates, go to [What are Azure Resource Manager templates?](#).

In this tutorial, we'll use pre-written sample templates for creating resources. You won't need to edit the template file and you can modify just the `.parameters.json` files to customize the deployment to your machine.

VM deployment workflow

To deploy Azure Stack Edge Pro VMs across many devices, you can use a single sysprep VHD for your full fleet, the same template for deployment, and just make minor changes to the parameters to that template for each deployment location (these changes could be by hand as we're doing here, or programmatic.)

The high level summary of the deployment workflow using templates is as follows:

1. Configure prerequisites - There are three types of prerequisites: device, client, and for the VM.

a. Device prerequisites

- a. [Connect to Azure Resource Manager on device.](#)
- b. Enable compute via the local UI.

b. Client prerequisites

- a. Download the VM templates and associated files on client.
- b. Optionally configure TLS 1.2 on client.
- c. [Download and install Microsoft Azure Storage Explorer](#) on your client.

c. VM prerequisites

- a. Create a resource group in the device location that will contain all the VM resources.
- b. Create a storage account to upload the VHD used to create VM image.
- c. Add local storage account URI to DNS or hosts file on the client accessing your device.
- d. Install the blob storage certificate on the device and on the local client accessing your device.

 Optionally install the blob storage certificate on the Storage Explorer.

- e. Create and upload a VHD to the storage account created earlier.

2. Create VM from templates

- a. Create a VM image using `CreateImage.parameters.json` parameters file and `CreateImage.json` deployment template.
- b. Create a VM with previously created resources using `CreateVM.parameters.json` parameters file and

`CreateVM.json` deployment template.

Device prerequisites

Configure these prerequisites on your Azure Stack Edge Pro device.

Before you can deploy VMs on your Azure Stack Edge device, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

Make sure that you can use the following steps to access the device from your client. You've already done this configuration when you connected to Azure Resource Manager, and now you're verifying that the configuration was successful.

1. Verify that Azure Resource Manager communication is working by running the following command:

- [Az](#)
- [AzureRM](#)

```
Add-AzEnvironment -Name <Environment Name> -ARMEndpoint "https://management.<appliance name>. <DNSDomain>"
```

2. To call the local device APIs to authenticate, enter:

- [Az](#)
- [AzureRM](#)

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

To connect via Azure Resource Manager, provide the username *EdgeArmUser* and your password.

3. If you configured compute for Kubernetes, you can skip this step. Otherwise, ensure that you've enabled a network interface for compute by doing the following:

- a. On your local user interface, go to **Compute** settings.
- b. Select the network interface that you want to use to create a virtual switch. The VMs you create will be attached to a virtual switch that's attached to this port and the associated network. Be sure to choose a network that matches the IP address you'll use for the VM.

The screenshot shows the Azure Stack Edge Commercial Compute settings. The 'Compute' tab is selected in the sidebar. The main pane displays network interface configuration. Network interface Port 2 is highlighted with a red box. The 'Enable for compute' checkbox is set to 'Yes'. The 'Compute IPs' section shows static IP ranges for Kubernetes node and external services. The 'Apply' button is at the bottom right.

c. Under **Enable for compute** on the network interface, select Yes. Azure Stack Edge will create and manage a virtual switch that corresponds to that network interface. Don't enter specific IPs for Kubernetes at this time. It can take several minutes to enable compute.

NOTE

If you're creating GPU VMs, select a network interface that's connected to the internet. Doing so enables you to install a GPU extension on your device.

Client prerequisites

Configure these prerequisites on your client that will be used to access the Azure Stack Edge Pro device.

1. [Download Storage Explorer](#) if you're using it to upload a VHD. Alternatively, you can download AzCopy to upload a VHD. You may need to configure TLS 1.2 on your client machine if running older versions of AzCopy.
2. [Download the VM templates and parameters files](#) to your client machine. Unzip it into a directory you'll use as a working directory.

VM prerequisites

Configure these prerequisites to create the resources needed for VM creation.

Create a resource group

- [Az](#)
- [AzureRM](#)

Create an Azure resource group with [New-AzResourceGroup](#). A resource group is a logical container into which the Azure resources such as storage account, disk, managed disk are deployed and managed.

IMPORTANT

All the resources are created in the same location as that of the device and the location is set to **DBELocal**.

```
New-AzResourceGroup -Name <Resource group name> -Location DBELocal
```

Here's a sample output:

```
PS C:\WINDOWS\system32> New-AzResourceGroup -Name myaserg1 -Location DBELocal

ResourceGroupName : myaserg1
Location         : dbelocal
ProvisioningState : Succeeded
Tags              :
ResourceId       : /subscriptions/04a485ed-7a09-44ab-6671-66db7f111122/resourceGroups/myaserg1

PS C:\WINDOWS\system32>
```

Create a storage account

- [Az](#)
- [AzureRM](#)

Create a new storage account using the resource group created in the previous step. This account is a **local storage account** that will be used to upload the virtual disk image for the VM.

```
New-AzStorageAccount -Name <Storage account name> -ResourceGroupName <Resource group name> -Location DBELocal -SkuName Standard_LRS
```

NOTE

Only the local storage accounts such as Locally redundant storage (Standard_LRS or Premium_LRS) can be created via Azure Resource Manager. To create tiered storage accounts, see the steps in [Add, connect to storage accounts on your Azure Stack Edge Pro](#).

Here's a sample output:

```
PS C:\WINDOWS\system32>New-AzStorageAccount -Name myasesa1 -ResourceGroupName myaserg1 -Location DBELocal -SkuName Standard_LRS

StorageAccountName ResourceGroupName PrimaryLocation SkuName Kind AccessTier CreationTime ProvisioningState
EnableHttpsTrafficOnly
-----
myasesa1          myaserg1  DBELocal  Standard_LRS Storage 4/18/2022 8:35:09 PM Succeeded False

PS C:\WINDOWS\system32>
```

To get the storage account key, run the `Get-AzStorageAccountKey` command. Here's a sample output:

```

PS C:\WINDOWS\system32> Get-AzStorageAccountKey

cmdlet Get-AzStorageAccountKey at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ResourceGroupName: myaserg1
Name: myasesa1

KeyName Value
----- -----
key1    7a707uIh43qADXvuhwqtw39mwq3M97r1Bf1hoF2yZ6W9FNkGOCblxb7nDSiYVGQprpkKk0Au2AjmpgUXUT6yCog== Full
key2    2v1VQ6qh1CJ9b0jB15p4jg9Ejn7iazU95Qe8hAGE22MTL21Ac5skA6kZnE3nbe+rdiXiORBeVh9OpJcMOfoaZg== Full

PS C:\WINDOWS\system32>

```

Add blob URI to hosts file

Make sure that you've already added the blob URI in hosts file for the client that you're using to connect to Blob storage. **Run Notepad as administrator** and add the following entry for the blob URI in the

`C:\windows\system32\drivers\etc\hosts :`

`<Device IP> <storage account name>.blob.<Device name>.<DNS domain>`

In a typical environment, you would have your DNS configured so that all storage accounts would point to the Azure Stack Edge Pro device with a `*.blob.devicename.domainname.com` entry.

(Optional) Install certificates

Skip this step if you'll connect via Storage Explorer using *http*. If you're using *https*, then you need to install appropriate certificates in Storage Explorer. In this case, install the blob endpoint certificate. For more information, see how to create and upload certificates in [Manage certificates](#).

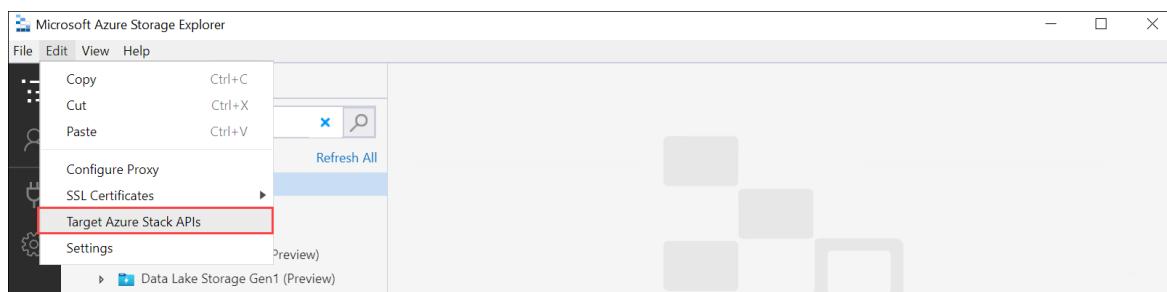
Create and upload a VHD

Make sure that you have a virtual disk image that you can use to upload in the later step. Follow the steps in [Create a VM image](#).

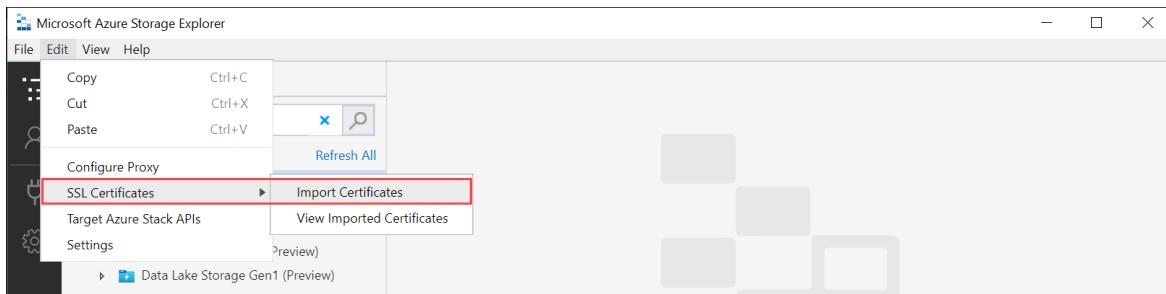
Copy any disk images to be used into page blobs in the local storage account that you created in the earlier steps. You can use a tool such as [Storage Explorer](#) or [AzCopy to upload the VHD to the storage account](#) that you created in earlier steps.

Use Storage Explorer for upload

1. Open Storage Explorer. Go to **Edit** and make sure that the application is set to **Target Azure Stack APIs**.



2. Install the client certificate in PEM format. Go to **Edit > SSL Certificates > Import certificates**. Point to the client certificate.

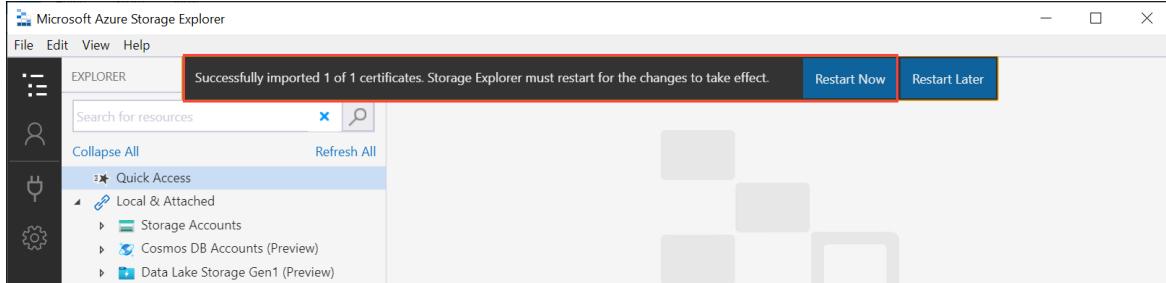


- If you're using device generated certificates, download and convert the blob storage endpoint .cer certificate to a .pem format. Run the following command.

```
PS C:\windows\system32> Certutil -encode 'C:\myasegpu1_Blob storage (1).cer'  
.blobstoragecert.pem  
Input Length = 1380  
Output Length = 1954  
CertUtil: -encode command completed successfully.
```

- If you're bringing your own certificate, use the signing chain root certificate in .pem format.

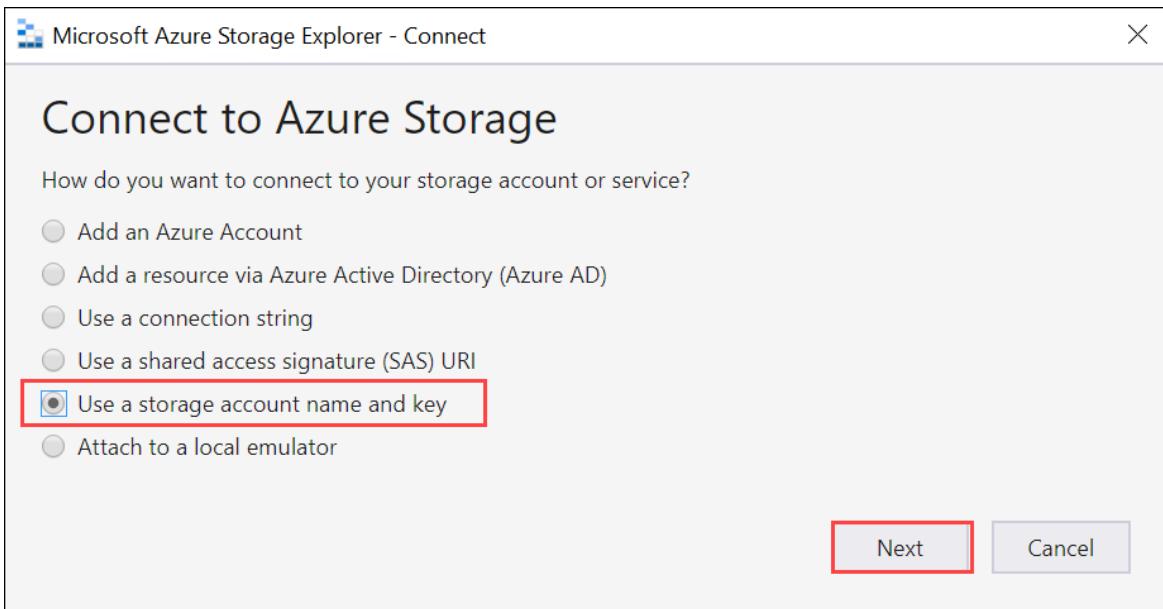
3. After you've imported the certificate, restart Storage Explorer for the changes to take effect.



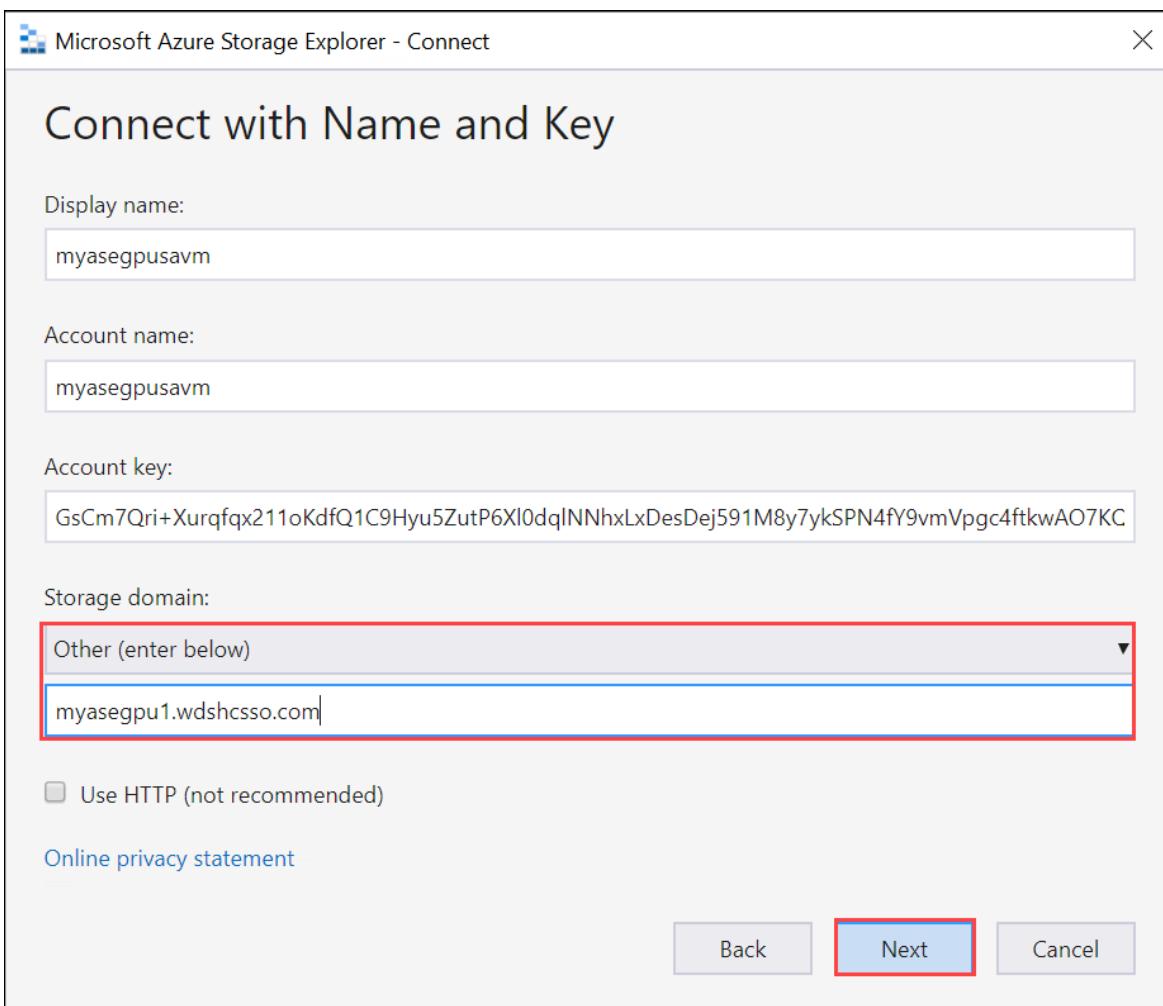
4. In the left pane, right-click Storage accounts and select Connect to Azure Storage.



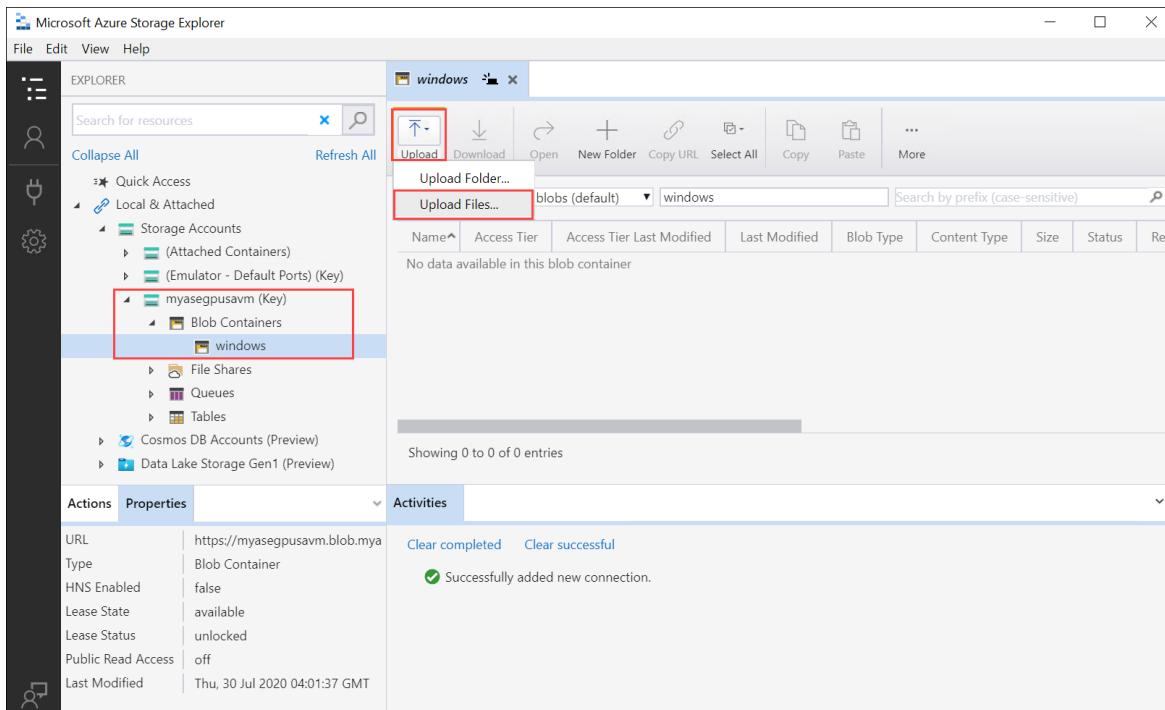
5. Select Use a storage account name and key. Select Next.



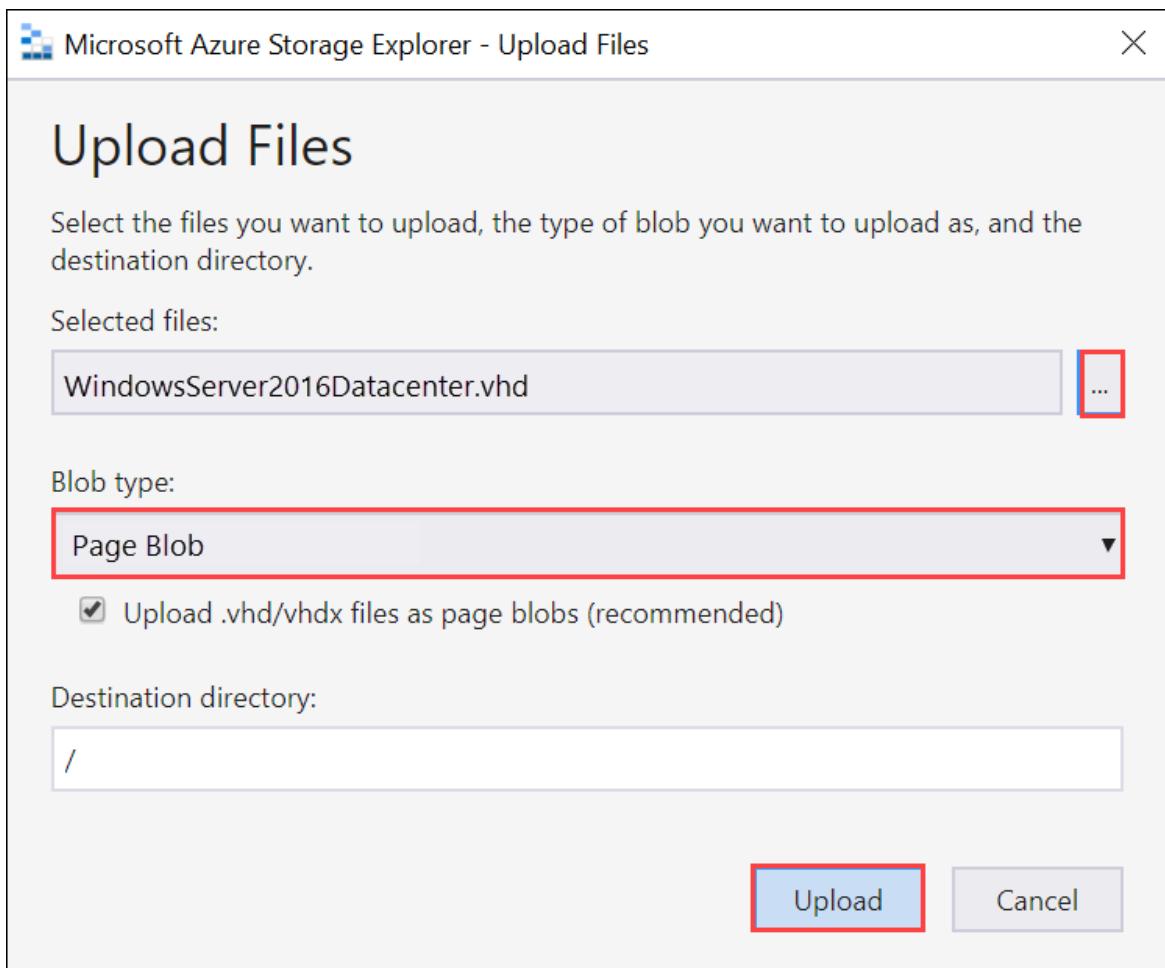
6. In the **Connect with Name and Key**, provide the **Display name**, **Storage account name**, Azure Storage Account key. Select **Other** Storage domain and then provide the <device name>. <DNS domain> connection string. If you didn't install a certificate in Storage Explorer, check the **Use HTTP** option. Select **Next**.



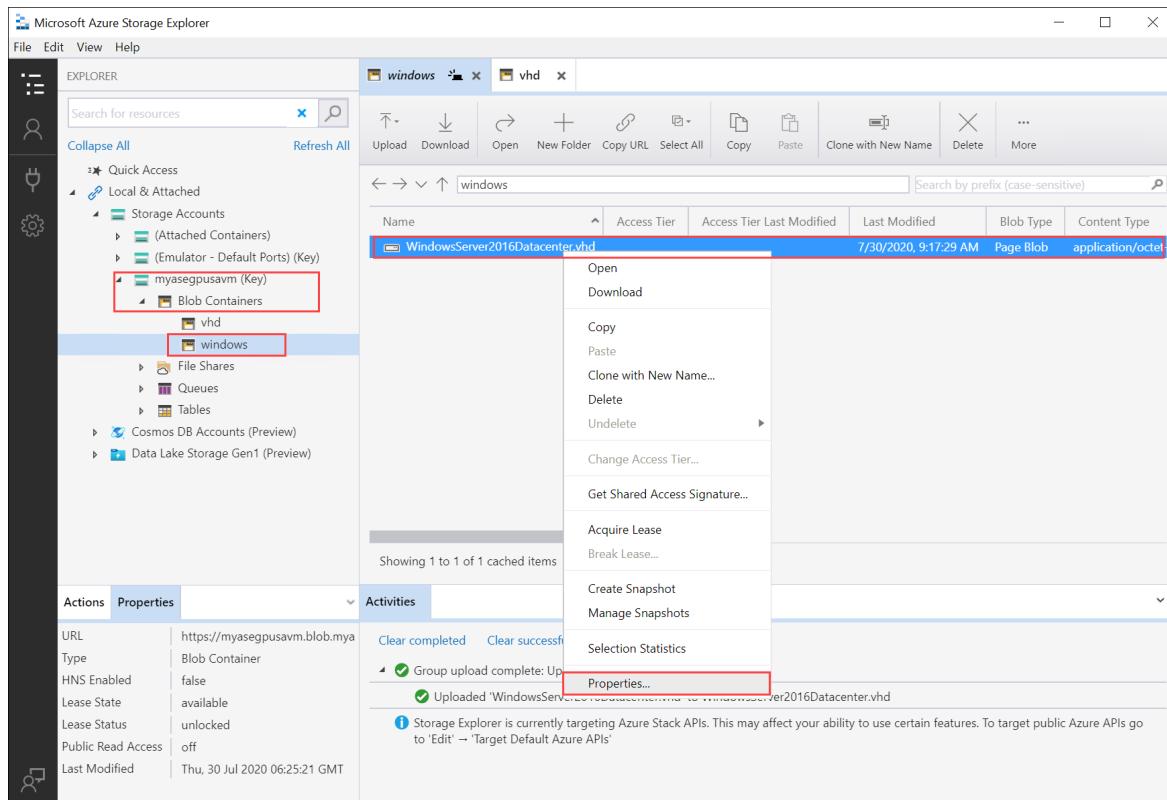
7. Review the **Connection summary** and select **Connect**.
8. The storage account appears in the left-pane. Select and expand the storage account. Select **Blob containers**, right-click, and select **Create Blob Container**. Provide a name for your blob container.
9. Select the container you just created, and then in the right-pane, select **Upload > Upload files**.



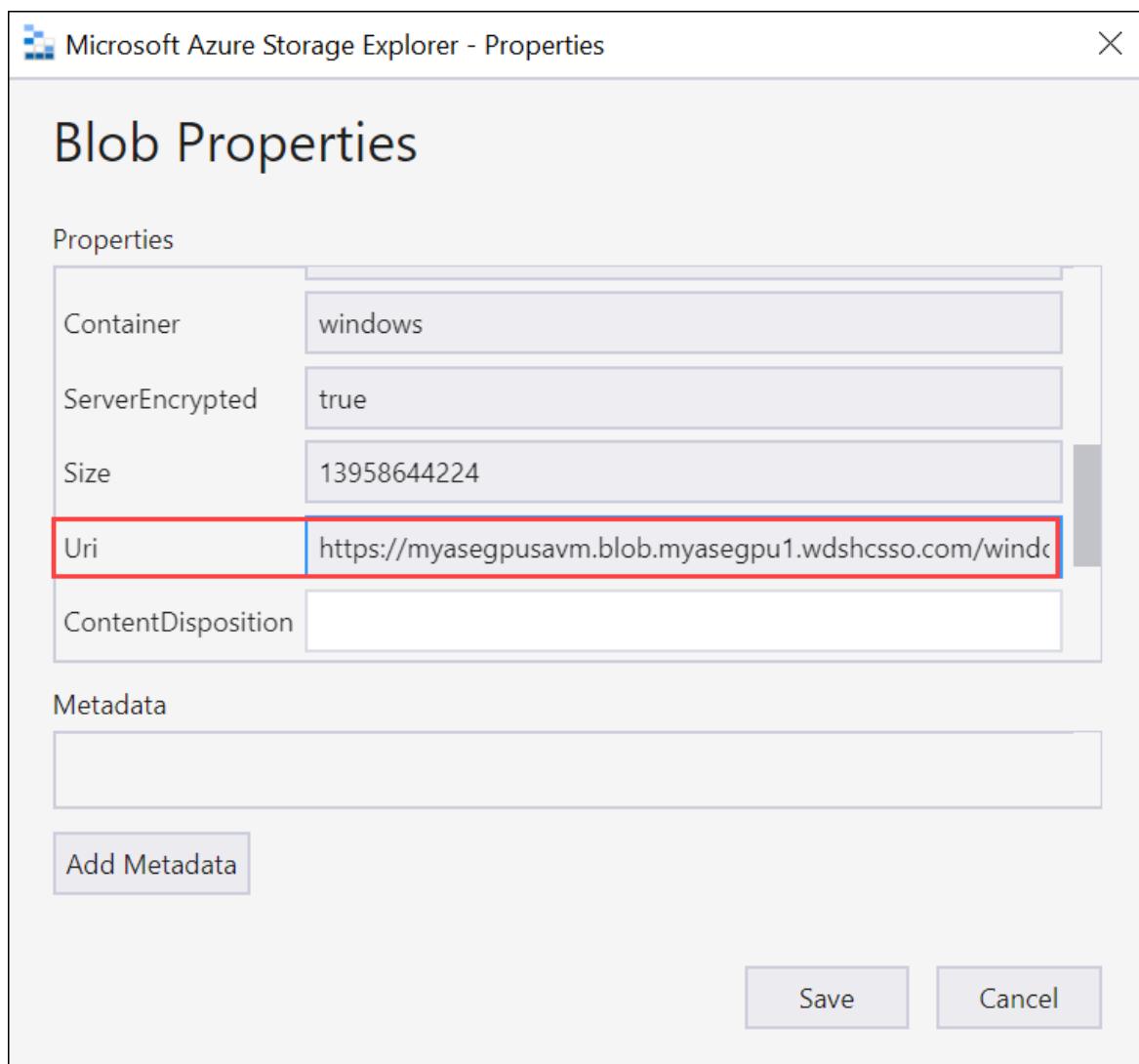
10. Browse and point to the VHD that you want to upload in the **Selected files**. Select **Blob type** as **Page blob** and select **Upload**.



11. Once the VHD is loaded to the blob container, select the VHD, right-click, and then select **Properties**.



12. Copy and save the Uri, which you'll use in later steps.



Create image for your VM

To create image for your VM, edit the `CreateImage.parameters.json` parameters file and then deploy the template `CreateImage.json` that uses this parameter file.

Edit parameters file

The file `CreateImage.parameters.json` takes the following parameters:

```
"parameters": {  
    "osType": {  
        "value": "<Operating system corresponding to the VHD you upload can be Windows or Linux>"  
    },  
    "imageName": {  
        "value": "<Name for the VM image>"  
    },  
    "imageUri": {  
        "value": "<Path to the VHD that you uploaded in the Storage account>"  
    },  
    "hyperVGeneration": {  
        "type": "string",  
        "value": "<Generation of the VM, V1 or V2>"  
    },  
}
```

Edit the file `CreateImage.parameters.json` to include the following values for your Azure Stack Edge Pro device:

1. Provide the OS type and Hyper V Generation corresponding to the VHD you'll upload. The OS type can be Windows or Linux and the VM Generation can be V1 or V2.

```
"parameters": {  
    "osType": {  
        "value": "Windows"  
    },  
    "hyperVGeneration": {  
        "value": "V2"  
    },  
}
```

2. Change the image URI to the URI of the image you uploaded in the earlier step:

```
"imageUri": {  
    "value":  
    "https://myasegpusavm.blob.myasegpu1.wdshcsso.com/windows/WindowsServer2016Datacenter.vhd"  
},
```

If you're using *http* with Storage Explorer, change the URI to an *http* URI.

3. Provide a unique image name. This image is used to create VM in the later steps.

Here's a sample json that is used in this article.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "osType": {
            "value": "Linux"
        },
        "hyperVGeneration": {
            "value": "V1"
        },
        "imageName": {
            "value": "myaselinuximg"
        },
        "imageUri": {
            "value": "https://sa2.blob.myasegpuvm.wdshcsso.com/con1/ubuntu18.04waagent.vhd"
        }
    }
}
```

4. Save the parameters file.

Deploy template

- [Az](#)
- [AzureRM](#)

Deploy the template `CreateImage.json`. This template deploys the image resources that will be used to create VMs in the later step.

NOTE

When you deploy the template if you get an authentication error, your Azure credentials for this session may have expired. Rerun the `login-Az` command to connect to Azure Resource Manager on your Azure Stack Edge Pro device again.

1. Run the following command:

```
$templateFile = "Path to CreateImage.json"
$templateParameterFile = "Path to CreateImage.parameters.json"
$RGName = "<Name of your resource group>"
New-AzResourceGroupDeployment ` 
    -ResourceGroupName $RGName ` 
    -TemplateFile $templateFile ` 
    -TemplateParameterFile $templateParameterFile ` 
    -Name "<Name for your deployment>"
```

This command deploys an image resource.

2. To query the resource, run the following command:

```
Get-AzImage -ResourceGroupName <Resource Group Name> -name <Image Name>
```

Here's a sample output:

```

PS C:\WINDOWS\system32> $templateFile = "C:\12-09-2020\CreateImage\CreateImage.json"
PS C:\WINDOWS\system32> $templateParameterFile = "C:\12-09-
2020\CreateImage\CreateImage.parameters.json"
PS C:\WINDOWS\system32> $RGName = "myaserg1"
PS C:\WINDOWS\system32> New-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile
$templateFile -TemplateParameterFile $templateParameterFile -Name "deployment1"

DeploymentName      : deployment1
ResourceGroupName   : myaserg1
ProvisioningState   : Succeeded
Timestamp          : 4/18/2022 9:24:26 PM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name          Type          Value
    =====        =====        =====
    osType        String        Linux
    imageName     String        myaselinuximg1
    imageUri      String        https://myasepro2stor.blob.dmc1176047910p.wdshcsso.com/myasepro2cont1/ubuntu13.vhd

Outputs            :
DeploymentLogLevel :
PS C:\WINDOWS\system32>

```

Create VM

Edit parameters file to create VM

- [Az](#)
- [AzureRM](#)

To create a VM, use the `CreateVM.parameters.json` parameter file. It takes the following parameters.

```
"vmName": {
    "value": "<Name for your VM>"
},
"adminUsername": {
    "value": "<Username to log into the VM>"
},
"Password": {
    "value": "<Password to log into the VM>"
},
"imageName": {
    "value": "<Name for your image>"
},
"vmSize": {
    "value": "<A supported size for your VM>"
},
"vnetName": {
    "value": "<Name for the virtual network, use ASEVNET>"
},
"subnetName": {
    "value": "<Name for the subnet, use ASEVNETsubNet>"
},
"vnetRG": {
    "value": "<Resource group for Vnet, use ASERG>"
},
"nicName": {
    "value": "<Name for the network interface>"
},
"privateIPAddress": {
    "value": "<Private IP address, enter a static IP in the subnet created earlier or leave empty to assign DHCP>"
},
"IPConfigName": {
    "value": "<Name for the ipconfig associated with the network interface>"
}
```

Assign appropriate parameters in `createVM.parameters.json` for your Azure Stack Edge Pro device.

1. Provide a unique name, network interface name, and ipconfig name.
2. Enter a username, password, and a supported VM size.
3. When you enabled the network interface for compute, a virtual switch and a virtual network were automatically created on that network interface. You can query the existing virtual network to get the Vnet name, Subnet name, and Vnet resource group name.

Run the following command:

```
Get-AzVirtualNetwork
```

Here's the sample output:

```

PS C:\WINDOWS\system32> Get-AzVirtualNetwork

Name          : ASEVNET
ResourceGroupName : ASERG
Location       : dbelocal
Id            : /subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/ASERG/providers/Microsoft
                      .Network/virtualNetworks/ASEVNET
Etag          : W/"990b306d-18b6-41ea-a456-b275efe21105"
ResourceGuid   : f8309d81-19e9-42fc-b4ed-d573f00e61ed
ProvisioningState : Succeeded
Tags          :
AddressSpace    :
DhcpOptions     : null
Subnets        :
{
    "Name": "ASEVNETsubNet",
    "Etag": "W/"990b306d-18b6-41ea-a456-b275efe21105"",
    "Id": "/subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/ASERG/provider
                      s/Microsoft.Network/virtualNetworks/ASEVNET/subnets/ASEVNETsubNet",
    "AddressPrefix": "10.57.48.0/21",
    "IpConfigurations": [],
    "ResourceNavigationLinks": [],
    "ServiceEndpoints": [],
    "ProvisioningState": "Succeeded"
}
]
VirtualNetworkPeerings : []
EnableDDoSProtection : false
EnableVmProtection    : false

PS C:\WINDOWS\system32>

```

Use ASEVNET for Vnet name, ASEVNETsubNet for Subnet name, and ASERG for Vnet resource group name.

4. Now you'll need a static IP address to assign to the VM that is in the subnet network defined above. Replace **PrivateIPAddress** with this address in the parameter file. To have the VM get an IP address from your local DHCP server, leave the **privateIPAddress** value blank.

```

"privateIPAddress": {
    "value": "5.5.153.200"
},

```

5. Save the parameters file.

Here is a sample json used in this article.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "value": "vm1"
        },
        "adminUsername": {
            "value": "Administrator"
        },
        "Password": {
            "value": "Password1"
        },
        "imageName": {
            "value": "myaselinuximg1"
        },
        "vmSize": {
            "value": "Standard_NC4as_T4_v3"
        },
        "vnetName": {
            "value": "vswitch1"
        },
        "subnetName": {
            "value": "vswitch1subNet"
        },
        "vnetRG": {
            "value": "myaserg1"
        },
        "nicName": {
            "value": "nic1"
        },
        "privateIPAddress": {
            "value": ""
        },
        "IPConfigName": {
            "value": "ipconfig1"
        }
    }
}
```

Deploy template to create VM

Deploy the VM creation template `CreateVM.json`. This template creates a network interface from the existing VNet and creates VM from the deployed image.

- [Az](#)
- [AzureRM](#)

1. Run the following command:

Command:

```
$templateFile = "<Path to CreateVM.json>"
$templateParameterFile = "<Path to CreateVM.parameters.json>"
$RGName = "<Resource group name>

New-AzResourceGroupDeployment ` 
    -ResourceGroupName $RGName ` 
    -TemplateFile $templateFile ` 
    -TemplateParameterFile $templateParameterFile ` 
    -Name "<DeploymentName>"
```

The VM creation will take 15-20 minutes. Here's a sample output of a successfully created VM:

```

PS C:\WINDOWS\system32> $templateFile = "C:\12-09-2020\CreateVM\CreateVM.json"
PS C:\WINDOWS\system32> $templateParameterFile = "C:\12-09-2020\CreateVM\CreateVM.parameters.json"
PS C:\WINDOWS\system32> $RGName = "myaserg1"
PS C:\WINDOWS\system32> New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile
$templateFile -TemplateParameterFile $templateParameterFile -Name "Deployment2"

DeploymentName      : Deployment2
ResourceGroupName   : myaserg1
ProvisioningState   : Succeeded
Timestamp          : 04/18/2022 1:51:28 PM
Mode                : Incremental
TemplateLink        :
Parameters          :

          Name           Type            Value
          ======        ======          =====
vmName             String          vm1
adminUsername      String          Administrator
password           String          Password1
imageName           String          myaselinuximg
vmSize              String          Standard_NC4as_T4_v3
vnetName            String          vswitch1
vnetRG              String          myaserg1
subnetName          String          vswitch1subNet
nicName              String          nic1
ipConfigName        String          ipconfig1
privateIPAddress    String         

Outputs             :
DeploymentLogLevel  :

PS C:\WINDOWS\system32

```

You can also run the `New-AzResourceGroupDeployment` command asynchronously with `-AsJob` parameter. Here's a sample output when the cmdlet runs in the background. You can then query the status of job that is created using the `Get-Job` cmdlet.

```

PS C:\WINDOWS\system32> New-AzResourceGroupDeployment ` 
>>     -ResourceGroupName $RGName ` 
>>     -TemplateFile $templateFile ` 
>>     -TemplateParameterFile $templateParameterFile ` 
>>     -Name "Deployment4" ` 
>>     -AsJob

Id      Name           PSJobTypeName  State       HasMoreData  Location    Command
--      --          -----          -----      -----      -----      -----
4      Long Running... AzureLongRun...  Running     True        localhost  New-
AzureRmResourceGro...

PS C:\WINDOWS\system32> Get-Job -Id 4

Id      Name           PSJobTypeName  State       HasMoreData  Location    Command
--      --          -----          -----      -----      -----      -----

```

2. Check if the VM is successfully provisioned. Run the following command:

`Get-AzVm`

Connect to a VM

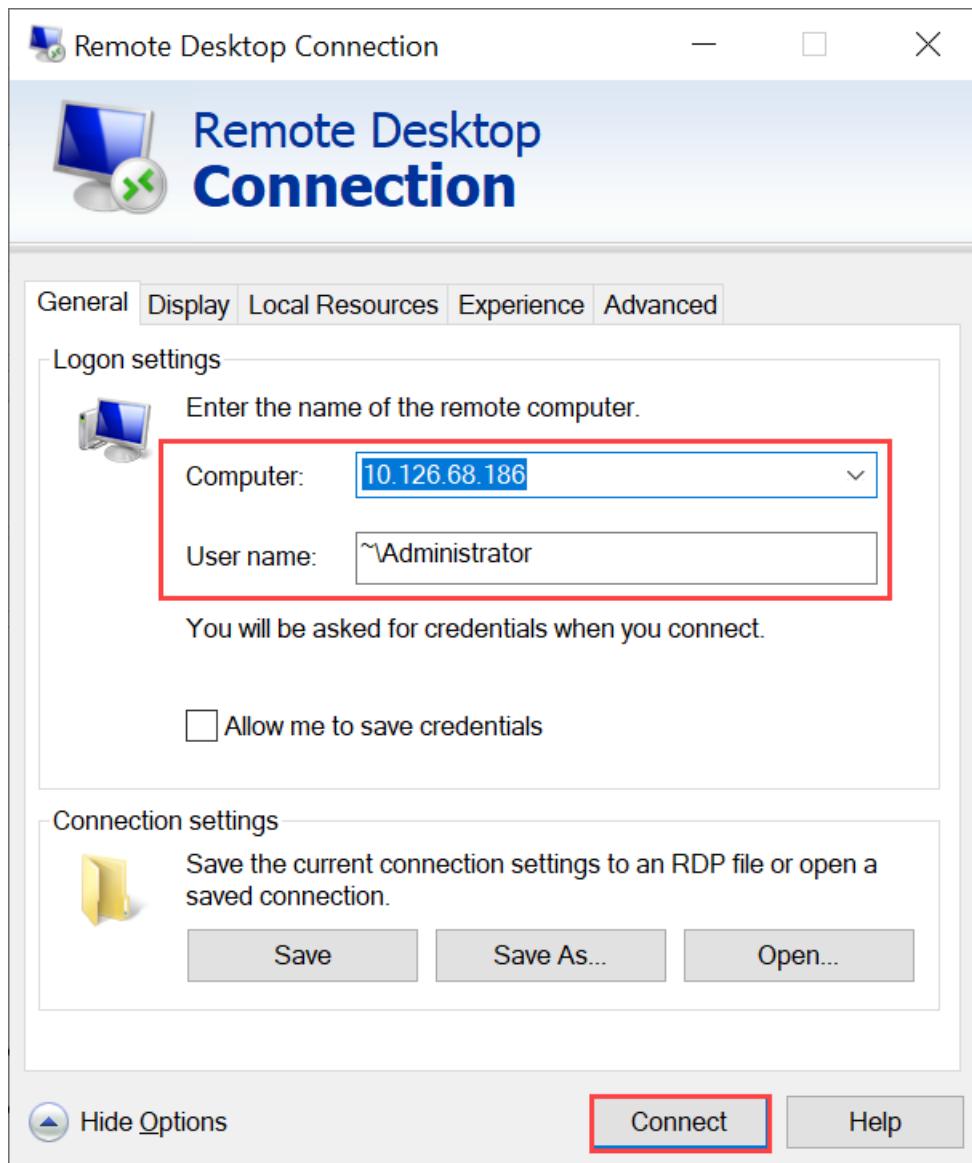
Depending on whether you created a Windows or a Linux VM, the steps to connect can be different.

Connect to Windows VM

Follow these steps to connect to a Windows VM.

Connect to your Windows VM by using the Remote Desktop Protocol (RDP) via the IP that you passed during the VM creation.

1. On your client, open RDP.
2. Go to **Start**, and then enter `mstsc`.
3. On the **Remote Desktop Connection** pane, enter the IP address of the VM and the access credentials you used in the VM template parameters file. Then select **Connect**.



NOTE

You might need to approve connecting to an untrusted machine.

You're now signed in to your VM that runs on the appliance.

Connect to Linux VM

Follow these steps to connect to a Linux VM.

Connect to the VM by using the private IP that you passed during the VM creation.

1. Open an SSH session to connect with the IP address.

```
ssh -l <username> <ip address>
```

- At the prompt, provide the password that you used when you created the VM.

If you need to provide the SSH key, use this command.

```
ssh -i c:/users/Administrator/.ssh/id_rsa Administrator@5.5.41.236
```

Here's an example output when you connect to the VM:

```
PS C:\WINDOWS\system32> ssh -l myazuser "10.126.76.60"
The authenticity of host '10.126.76.60 (10.126.76.60)' can't be established.
ECDSA key fingerprint is SHA256:V649Zbo58zAYMKreeP7M6w7Na0Yf9QPg4SM7JJZVV0E4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.126.76.60' (ECDSA) to the list of known hosts.
myazuser@10.126.76.60's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-1013-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information disabled due to load higher than 1.0

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

284 packages can be updated.
192 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

myazuser@myazvmfriendlyname:~$ client_loop: send disconnect: Connection reset
PS C:\WINDOWS\system32>
```

Next steps

[Azure Resource Manager cmdlets](#)

Deploy GPU VMs on your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

This article describes how to create a GPU VM in the Azure portal or by using the Azure Resource Manager templates.

Use the Azure portal to quickly deploy a single GPU VM. You can install the GPU extension during or after VM creation. Or use Azure Resource Manager templates to efficiently deploy and manage multiple GPU VMs.

Create GPU VMs

You can deploy a GPU VM via the portal or using Azure Resource Manager templates.

For a list of supported operating systems, drivers, and VM sizes for GPU VMs, see [What are GPU virtual machines?](#) For deployment considerations, see [GPU VMs and Kubernetes](#).

IMPORTANT

- Gen2 VMs are not supported for GPU.
- If your device will be running Kubernetes, do not configure Kubernetes before you deploy your GPU VMs. If you configure Kubernetes first, it claims all the available GPU resources, and GPU VM creation will fail. For Kubernetes deployment considerations on 1-GPU and 2-GPU devices, see [GPU VMs and Kubernetes](#).
- If you're running a Windows 2016 VHD, you must enable TLS 1.2 inside the VM before you install the GPU extension on 2205 and higher. For detailed steps, see [Troubleshoot GPU extension issues for GPU VMs on Azure Stack Edge Pro GPU](#).

- [Portal](#)
- [Templates](#)

Follow these steps when deploying GPU VMs on your device via the Azure portal:

1. To create GPU VMs, follow all the steps in [Deploy VM on your Azure Stack Edge using Azure portal](#), with these configuration requirements:
 - On the **Basics** tab, select a **VM size from N-series, optimized for GPUs**. Based on the GPU model on your device, Nvidia T4 or Nvidia A2, the dropdown list will display the corresponding supported GPU VM sizes.

Add a virtual machine

X

myasegpudevice

Basics

Disks

Networking

Advanced

Review + create

To create a Linux or Windows VM, use a VM image from your device. [Learn more](#)

Virtual machine name * ⓘ

myasegpu1



Edge resource group * ⓘ

ase-image-resourcegroup



[Create new](#)

Image * ⓘ

myaseazlinuxvmimage (Linux)



Size * ⓘ

Standard_NC4as_T4_v3 - 4 vcpus, 28.67 GB memory



Administrator account

Username * ⓘ

azureuser



Authentication type * ⓘ

SSH public key Password

SSH public key * ⓘ

[Review + create](#)

[Previous](#)

[Next: Disks](#)

- To install the GPU extension during deployment, on the **Advanced** tab, choose **Select an extension to install**. Then select a GPU extension to install. GPU extensions are only available for a virtual machine with a [VM size from N-series](#).

NOTE

If you're using a Red Hat image, you'll need to install the GPU extension after VM deployment. Follow the steps in [Install GPU extension](#).

Add a virtual machine

myasेग्पुदेवी

[Basics](#) [Disks](#) [Networking](#) [Advanced](#) [Review + create](#)

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

For a Red Hat image, follow the [steps to add the GPU extension](#) to the VM. Add the extension after the VM is created.Extensions (1)**1****Select an extension to install****Custom data and cloud init**Pass a cloud-init script, configuration file, or other saved on the VM in a known location. [Learn more](#)

Custom data

Home > Virtual machines > Add a virtual machine >

Add extension



NVIDIA GPU Driver Extension

Microsoft Corp.

2i Custom data on the selected image will be pro...[Review + create](#)[Previous](#)[Next: Review + create](#)The **Advanced** tab shows the extension you selected.

Add a virtual machine

myasegpudevice

X

Basics Disks Networking Advanced Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

For a Red Hat image, follow the steps to add the GPU extension to the VM. Add the extension after the VM is created.

Extensions ①

NVIDIA GPU Driver Extension
Microsoft.HpcCompute

Select an extension to install

Custom data and cloud initPass a cloud-init script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data

i Custom data on the selected image will be processed by cloud-init. [Learn more about custom data and cloud init](#)

Review + create

Previous

Next: Review + create

- Once the GPU VM is successfully created, you can view this VM in the list of virtual machines in your Azure Stack Edge resource in the Azure portal.

Virtual machines | Virtual machines

X

PREVIEW

Search (Ctrl+ /)

Add virtual machine

Refresh

Overview

Images

Virtual machines

Deployments

Name ↑↓

Status ↑↓

Size ↑↓

Disks ↑↓

VM1

Running

Standard_NC4as_T4_v3

1

Select the VM, and drill down to the details. Make sure the GPU extension has **Succeeded** status.

The screenshot shows the Azure portal interface for managing a virtual machine. The top navigation bar includes 'Home', 'PortalPhysicalDevice5', and 'Virtual machines'. Below this, the specific VM details are shown: Computer name (ubuntu1804vm), Image name (ubuntu1804waagent), Operating system (Linux), and Status (Running). The 'Size' section indicates a VM Size (NC4as_T4_v3) with 4 vCPUs and 28.67 GB of RAM. The 'Networking' section lists the network interface (ubuntu1804vmnic primary) with IP Address 10.57.50.57, Virtual network (ASEVNET), Subnet (ASEVNETSubNet), and IP allocation method (Dynamic). The 'Disks' section shows an OS disk (ubuntu1804vm_disk1_870e37d3318540e98032a6de3023) with Standard IOPS storage type. On the right, the 'Installed extensions' section displays the NvidiaGpuDriverLinux extension with a status of 'Succeeded'. A red box highlights the 'Add extension' button at the top of the page.

NOTE

When updating your device software version from 2012 to later, you will need to manually stop the GPU VMs.

Install GPU extension after deployment

To take advantage of the GPU capabilities of Azure N-series VMs, Nvidia GPU drivers must be installed. From the Azure portal, you can install the GPU extension during or after VM deployment. If you're using templates, you'll install the GPU extension after you create the VM.

- [Portal](#)
- [Templates](#)

If you didn't install the GPU extension when you created the VM, follow these steps to install it on the deployed VM:

1. Go to the virtual machine you want to add the GPU extension to.

The screenshot shows the 'Virtual machines' blade in the Azure portal. The left sidebar includes 'Overview', 'Activity log', 'Images', 'Virtual machines' (which is highlighted with a red box), 'Resources', and 'Deployments'. The main area displays a table of virtual machines with columns for Name, Status, Size, Disks, and Edge resource group. The 'myasegpuvm' row is selected, showing it's running on a Standard_D1_v2 size with 3 disks and assigned to the MYASERG edge resource group. Other listed VMs include 'myazvm' and 'testvm01v-dalc'.

2. In **Details**, select **+ Add extension**. Then select a GPU extension to install.

GPU extensions are only available for a virtual machine with a [VM size from N-series](#). If you prefer, you can [install the GPU extension after deployment](#).

The screenshot shows the Azure portal interface for managing a virtual machine named 'myasewindowsvm2'. The main window displays basic details like computer name, image name, operating system, and status. A red box labeled '1' highlights the 'Add extension' button in the top navigation bar. A secondary window titled 'Add extension' is open, showing the 'NVIDIA GPU Driver Extension' by Microsoft Corp., which is also highlighted with a red box and labeled '2'.

NOTE

You can't remove a GPU extension via the portal. Instead, use the [Remove-AzureRmVMExtension](#) cmdlet in Azure PowerShell. For instructions, see [Remove GPU extension](#)

Next steps

- [Troubleshoot VM deployment](#)
- [Troubleshoot GPU extension issues](#)
- [Monitor VM activity on your device](#)
- [Monitor CPU and memory on a VM](#)

Deploy high performance network VMs on your Azure Stack Edge Pro GPU device

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

You can create and manage virtual machines (VMs) on an Azure Stack Edge Pro GPU device by using the Azure portal, templates, and Azure PowerShell cmdlets, and via the Azure CLI or Python scripts. This article describes how to create and manage a high-performance network (HPN) VM on your Azure Stack Edge Pro GPU device.

About HPN VMs

A non-uniform memory access (NUMA) architecture is used to increase processor speeds. In a NUMA system, CPUs are arranged in smaller systems called nodes. Each node has its own processors and memory. Processors are typically allocated memory that they are close to so the access is quicker. For more information, see [NUMA Support](#).

On your Azure Stack Edge device, logical processors are distributed on NUMA nodes and high speed network interfaces can be attached to these nodes. An HPN VM has a dedicated set of logical processors. These processors are first picked from the NUMA node that has high speed network interface attached to it, and then picked from other nodes. An HPN VM can only use the memory of the NUMA node that is assigned to its processors.

To run low latency and high throughput network applications on the HPN VMs deployed on your device, make sure to reserve vCPUs that reside in NUMA node 0. This node has Mellanox high speed network interfaces, Port 5 and Port 6, attached to it.

HPN VM deployment workflow

The high-level summary of the HPN deployment workflow is as follows:

1. Enable a network interface for compute on your Azure Stack Edge device. This step creates a virtual switch on the specified network interface.
2. Enable cloud management of VMs from the Azure portal.
3. Upload a VHD to an Azure Storage account by using Azure Storage Explorer.
4. Use the uploaded VHD to download the VHD onto the device, and create a VM image from the VHD.
5. Reserve vCPUs on the device for HPN VMs.
6. Use the resources created in the previous steps:
 - a. VM image that you created.
 - b. Virtual switch associated with the network interface on which you enabled compute.
 - c. Subnet associated with the virtual switch.

And create or specify the following resources inline:

- a. VM name, choose a supported HPN VM size, sign-in credentials for the VM.
- b. Create new data disks or attach existing data disks.

- c. Configure static or dynamic IP for the VM. If you're providing a static IP, choose from a free IP in the subnet range of the network interface enabled for compute.

Use the preceding resources to create an HPN VM.

Prerequisites

Before you begin to create and manage VMs on your device via the Azure portal, make sure that:

- You've completed the network settings on your Azure Stack Edge Pro GPU device as described in [Step 1: Configure an Azure Stack Edge Pro GPU device](#).
- 1. You've enabled a network interface for compute. This network interface IP is used to create a virtual switch for the VM deployment. In the local UI of your device, go to **Compute**. Select the network interface that you'll use to create a virtual switch.

IMPORTANT

You can configure only one port for compute.

- 2. Enable compute on the network interface. Azure Stack Edge Pro GPU creates and manages a virtual switch corresponding to that network interface.
- You have access to a Windows or Linux VHD that you'll use to create the VM image for the VM you intend to create.

In addition to the above prerequisites that are used for VM creation, you'll also need to configure the following prerequisite specifically for the HPN VMs:

- Reserve vCPUs for HPN VMs on the Mellanox interface. Follow these steps:
 1. [Connect to the PowerShell interface of the device](#).
 2. Identify all the VMs running on your device. This includes Kubernetes VMs, or any VM workloads that you may have deployed.

```
get-vm
```

3. Stop all the running VMs.

```
stop-vm -force
```

4. Get the `hostname` for your device. This should return a string corresponding to the device hostname.

```
hostname
```

5. Get the logical processor indexes to reserve for HPN VMs.

```
Get-HcsNumaLpMapping -MapType HighPerformanceCapable -NodeName <Output of hostname command>
```

Here is an example output:

```
[dbe-1cspfq2.microsoftdatabox.com]: PS>hostname  
1CSPHQ2  
[dbe-1cspfq2.microsoftdatabox.com]: P> Get-HcsNumaLpMapping -MapType HighPerformanceCapable -  
NodeName 1CSPHQ2  
{ Numa Node #0 : CPUs [4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19] }  
{ Numa Node #1 : CPUs [24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39] }  
  
[dbe-1cspfq2.microsoftdatabox.com]: PS>
```

6. Reserve vCPUs for HPN VMs. The number of vCPUs reserved here determines the available vCPUs that could be assigned to the HPN VMs. For the number of cores that each HPN VM size uses, see the [Supported HPN VM sizes](#). On your device, Mellanox ports 5 and 6 are on NUMA node 0.

```
Set-HcsNumaLpMapping -CpusForHighPerfVmsCommaSeparated <Logical indexes from the Get-  
HcsNumaLpMapping cmdlet> -AssignAllCpusToRoot $false
```

After this command is run, the device restarts automatically.

Here is an example output:

```
[dbe-1cspfq2.microsoftdatabox.com]: PS>Set-HcsNumaLpMapping -CpusForHighPerfVmsCommaSeparated  
"4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39" -  
AssignAllCpusToRoot $false  
Requested Configuration requires a reboot...  
Machine will reboot in some time. Please be patient.  
[dbe-1cspfq2.microsoftdatabox.com]: PS>
```

NOTE

- You can choose to reserve all the logical indexes from both NUMA nodes shown in the example or a subset of the indexes. If you choose to reserve a subset of indexes, pick the indexes from the device node that has a Mellanox network interface attached to it, for best performance. For Azure Stack Edge Pro GPU, the NUMA node with Mellanox network interface is #0.
- The list of logical indexes must contain a paired sequence of an odd number and an even number. For example, ((4,5)(6,7)(10,11)). Attempting to set a list of numbers such as `5,6,7` or pairs such as `4,6` will not work.
- Using two `Set-HcsNuma` commands consecutively to assign vCPUs will reset the configuration. Also, do not free the CPUs using the Set-HcsNuma cmdlet if you have deployed an HPN VM.

7. Wait for the device to finish rebooting. Once the device is running, open a new PowerShell session. [Connect to the PowerShell interface of the device](#).

8. Validate the vCPU reservation.

```
Get-HcsNumaLpMapping -MapType MinRootAware -NodeName <Output of hostname command>
```

The output should not show the indexes you set. If you see the indexes you set in the output, the `Set` command did not complete successfully. Retry the command and if the problem persists, contact Microsoft Support.

Here is an example output.

```
[dbe-1cspfq2.microsoftdatabox.com]: PS> Get-HcsNumaLpMapping -MapType MinRootAware -NodeName 1CSPHQ2
{ Numa Node #0 : CPUs [0, 1, 2, 3] }
{ Numa Node #1 : CPUs [20, 21, 22, 23] }
[dbe-1cspfq2.microsoftdatabox.com]: PS>
```

9. Restart the VMs that you had stopped in the earlier step.

```
start-vm
```

Deploy a VM

Follow these steps to create an HPN VM on your device.

1. In the Azure portal of your Azure Stack Edge resource, [Add a VM image](#). You'll use this VM image to create a VM in the next step. You can choose either Gen1 or Gen2 for the VM.
2. Follow all the steps in [Add a VM](#) with this configuration requirement.

On the Basics tab, select a VM size from [DSv2 or F-series supported for HPN](#).

The screenshot shows the 'Add a virtual machine' wizard in the Azure portal, specifically the 'Basics' tab. The page title is 'Add a virtual machine' under 'myase2109 > Virtual machines'. The 'Basics' tab is selected, indicated by a red border. The form fields are as follows:

- Virtual machine name ***: myasehpnvm1
- Edge resource group ***: myasehpnvmrg (dropdown menu)
- Image ***: hpnlinuxvm (Linux) (dropdown menu)
- Size ***: Standard_DS2_v2_HPN - 2 vcpus, 7.17 GB memory (dropdown menu)
- Administrator account**
 - Username ***: azureuser
 - Authentication type ***: Password (radio button selected)
 - Password ***: (redacted)
 - Confirm password ***: (redacted)

At the bottom of the screen, there are navigation buttons: 'Review + create' (blue), 'Previous' (grey), and 'Next: Disks' (red border).

3. Finish the remaining steps in the VM creation. The VM will take approximately 30 minutes to be created.

Home > Virtual machines >

Add a virtual machine

myase2109

All validations have passed.

Basics Disks Networking Advanced Review + create

TERMS
By clicking "Create", I agree to the legal terms and privacy statement(s) associated with preview services. See the [Preview Terms Of Use | Microsoft Azure](#) for additional details.

Basics

Virtual machine name	myasehpnvm1
Edge resource group	myasehpnvmrg
Image	hpnlinuxvms
Size	Standard_DS2_v2_HPN
Username	azureuser

Disks

Data disks	1
------------	---

Networking

Virtual network	ASEVNET
Subnet	ASEVNETsubNet
IP address	NA
IP address assignment	Dynamic

Advanced

Cloud init	No
------------	----

Create Previous Next

This screenshot shows the final step of creating a virtual machine. It displays a summary of the configuration: a virtual machine named 'myasehpnvm1' in the 'myasehpnvmrg' edge resource group, using the 'hpnlinuxvms' image, size 'Standard_DS2_v2_HPN', and one data disk. The networking section specifies 'ASEVNET' as the virtual network and 'ASEVNETsubNet' as the subnet. The advanced section has 'Cloud init' set to 'No'. At the bottom, there are 'Create', 'Previous', and 'Next' buttons, with 'Create' being highlighted.

4. After the VM is successfully created, you'll see your new VM on the **Overview** pane. Select the newly created VM to go to **Virtual machines**.

Home > myase2109 > Virtual machines

Virtual machines | Virtual machines

PREVIEW

Search (Ctrl+ /) << Add virtual machine Refresh

Overview Activity log Images

Virtual machines Resources Deployments

Name ↑↓	Status ↑↓	Size ↑↓	Disks ↑↓	Edge resource group ↑↓
myasehpnvm1	Running	Standard_DS2_v2_HPN	2	MYASEHPNVMRG

This screenshot shows the 'Virtual machines' overview page. On the left, there's a sidebar with links for Overview, Activity log, Images, Virtual machines (which is selected and highlighted with a red box), Resources, and Deployments. The main area is a table showing the details of existing VMs. One VM, 'myasehpnvm1', is highlighted with a red box. The table columns include Name, Status, Size, Disks, and Edge resource group. The status for 'myasehpnvm1' is 'Running'.

Select the VM to see the details.

Home > myase2109 > Virtual machines >

myasehpnvvm1

Virtual machine

Start Restart Stop Delete Add extension Refresh

Details Metrics

Virtual machine

Computer name	myasehpnvvm1
Image name	hpnluxvm
Operating system	Linux
Status	Running

Size

VM Size (Change)	DS2_v2_HPN
Offering	Standard
vCPUs	2
RAM	7.17 GB

Installed extensions

Name	Status
No results.	

Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group
myasehpnvvm1nic (primary)	10.126.77.141	ASEVNET	ASEVNETsubNet	Dynamic	MYASEHPNVMRG

Disks

OS disk

Disk name	myasehpnvvm1_disk1_b393370ae2d247cb 800726793fd8936f
Storage type	Standard_LRS
Size	30 GB

Data disks

Disk name	LUN	Storage type	Size
myhpnvmdisk1	1	Standard	10 GB

You'll use the IP address for the network interface to connect to the VM.

NOTE

If the vCPUs are not reserved for HPN VMs prior to the deployment, the deployment will fail with

`FabricVmPlacementErrorInsufficientNumaNodeCapacity` error.

Next steps

- [Troubleshoot VM deployment](#)
- [Monitor VM activity on your device](#)
- [Monitor CPU and memory on a VM](#)

Deploy VMs on your Azure Stack Edge device via Azure PowerShell

9/21/2022 • 22 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to create and manage a virtual machine (VM) on your Azure Stack Edge device by using Azure PowerShell.

VM deployment workflow

The high-level deployment workflow of the VM deployment is as follows:

1. Connect to the local Azure Resource Manager of your device.
2. Identify the built-in subscription on the device.
3. Bring your VM image.
4. Create a resource group in the built-in subscription. The resource group will contain the VM and all the related resources.
5. Create a local storage account on the device to store the VHD that will be used to create a VM image.
6. Upload a Windows/Linux source image into the storage account to create a managed disk.
7. Use the managed disk to create a VM image.
8. Enable compute on a device port to create a virtual switch.
9. This creates a virtual network using the virtual switch attached to the port on which you enabled compute.
10. Create a VM using the previously created VM image, virtual network, and virtual network interface(s) to communicate within the virtual network and assign a public IP address to remotely access the VM. Optionally include data disks to provide more storage for your VM.

Prerequisites

Before you can deploy VMs on your Azure Stack Edge device, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

Make sure that you can use the following steps to access the device from your client. You've already done this configuration when you connected to Azure Resource Manager, and now you're verifying that the configuration was successful.

1. Verify that Azure Resource Manager communication is working by running the following command:

- [Az](#)
- [AzureRM](#)

```
Add-AzEnvironment -Name <Environment Name> -ARMEndpoint "https://management.<appliance name>.<DNSDomain>"
```

2. To call the local device APIs to authenticate, enter:

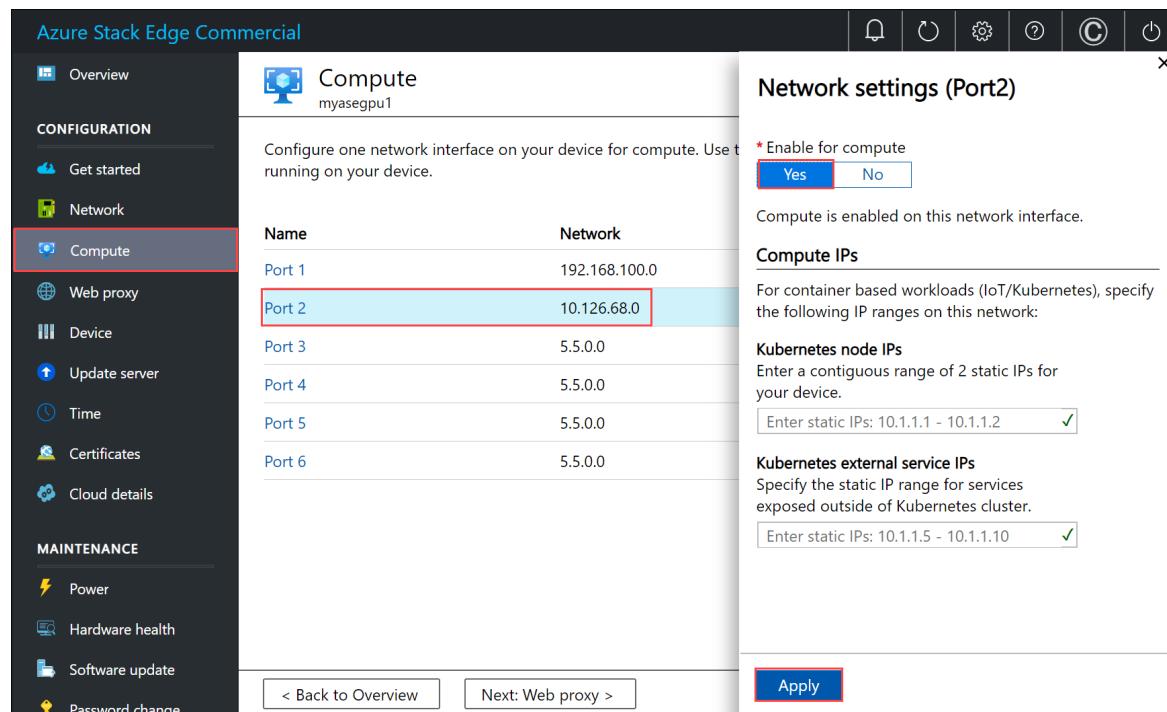
- [Az](#)

- AzureRM

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

To connect via Azure Resource Manager, provide the username *EdgeArmUser* and your password.

3. If you configured compute for Kubernetes, you can skip this step. Otherwise, ensure that you've enabled a network interface for compute by doing the following:
 - a. On your local user interface, go to **Compute** settings.
 - b. Select the network interface that you want to use to create a virtual switch. The VMs you create will be attached to a virtual switch that's attached to this port and the associated network. Be sure to choose a network that matches the IP address you'll use for the VM.



- c. Under **Enable for compute** on the network interface, select **Yes**. Azure Stack Edge will create and manage a virtual switch that corresponds to that network interface. Don't enter specific IPs for Kubernetes at this time. It can take several minutes to enable compute.

NOTE

If you're creating GPU VMs, select a network interface that's connected to the internet. Doing so enables you to install a GPU extension on your device.

Query for a built-in subscription on the device

For Azure Resource Manager, only a single fixed subscription that's user-visible is supported. This subscription is unique per device, and the subscription name and subscription ID can't be changed.

The subscription contains all the resources that are required for VM creation.

IMPORTANT

The subscription is created when you enable VMs from the Azure portal, and it lives locally on your device.

The subscription is used to deploy the VMs.

- [Az](#)
- [AzureRM](#)

1. To list the subscription, run the following command:

```
Get-AzSubscription
```

Here's some example output:

```
PS C:\WINDOWS\system32> Get-AzSubscription
```

Name	Id	TenantId
---	--	-----
Default Provider Subscription

```
PS C:\WINDOWS\system32>
```

2. Get a list of the registered resource providers that are running on the device. The list ordinarily includes compute, network, and storage.

```
Get-AzResourceProvider
```

NOTE

The resource providers are pre-registered, and they can't be modified or changed.

Here's some example output:

```
PS C:\WINDOWS\system32> Get-AzResourceProvider

ProviderNamespace : Microsoft.AzureBridge
RegistrationState : Registered
ResourceTypes     : {locations, operations, locations/ingestionJobs}
Locations        : {DBELocal}

ProviderNamespace : Microsoft.Compute
RegistrationState : Registered
ResourceTypes     : {virtualMachines, virtualMachines/extensions, locations, operations...}
Locations        : {DBELocal}

ProviderNamespace : Microsoft.Network
RegistrationState : Registered
ResourceTypes     : {operations, locations, locations/operations, locations/usages...}
Locations        : {DBELocal}

ProviderNamespace : Microsoft.Resources
RegistrationState : Registered
ResourceTypes     : {tenants, locations, providers, checkresourcename...}
Locations        : {DBELocal}

ProviderNamespace : Microsoft.Storage
RegistrationState : Registered
ResourceTypes     : {storageaccounts, storageAccounts/blobServices, storageAccounts/tableServices,
                    storageAccounts/queueServices...}
Locations        : {DBELocal}

PS C:\WINDOWS\system32>
```

Create a resource group

Start by creating a new Azure resource group and use this as a logical container for all the VM related resources, such as storage account, disk, network interface, and managed disk.

IMPORTANT

All the resources are created in the same location as that of the device, and the location is set to **DBELocal**.

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$ResourceGroupName = "<Resource group name>"
```

2. Create a resource group for the resources that you'll create for the VM.

```
New-AzResourceGroup -Name $ResourceGroupName -Location DBELocal
```

Here's some example output:

```
PS C:\WINDOWS\system32> New-AzResourceGroup -Name myaseazrg -Location DBELocal

ResourceGroupName : myaseazrg
Location         : dbelocal
ProvisioningState : Succeeded
Tags              :
ResourceId       : /subscriptions/.../resourceGroups/myaseazrg

PS C:\WINDOWS\system32>
```

Create a local storage account

Create a new local storage account by using an existing resource group. Use this local storage account to upload the virtual disk image when creating a VM.

Before you create a local storage account, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$StorageAccountName = "<Storage account name>"
```

2. Create a new local storage account on your device.

```
New-AzStorageAccount -Name $StorageAccountName -ResourceGroupName $ResourceGroupName -Location DBELocal -SkuName Standard_LRS
```

NOTE

By using Azure Resource Manager, you can create only local storage accounts, such as locally redundant storage (standard or premium). To create tiered storage accounts, see [Tutorial: Transfer data via storage accounts with Azure Stack Edge Pro with GPU](#).

Here's an example output:

```
PS C:\WINDOWS\system32> New-AzStorageAccount -Name myaseazsa -ResourceGroupName myaseazrg -Location DBELocal -SkuName Standard_LRS

StorageAccountName ResourceGroupName PrimaryLocation SkuName      Kind   AccessTier CreationTime
-----          -----          -----          -----      -----   -----   -----        -----
myaseazsa      myaseazrg     DBELocal      Standard_LRS Storage    6/10/2021
11:45...

PS C:\WINDOWS\system32>
```

To get the access keys for an existing local storage account that you have created, provide the associated resource group name and the local storage account name.

- [Az](#)
- [AzureRM](#)

```
Get-AzStorageAccountKey
```

Here's an example output:

```
PS C:\WINDOWS\system32> Get-AzStorageAccountKey

cmdlet Get-AzStorageAccountKey at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ResourceGroupName: myaseazrg
Name: myaseazsa

KeyName      Value
Permissions
-----      -----
-
key1        gv30F57tuPDyzBNc1M7fhil2UaiiwnhTT6zgiwE3T1F/CD217Cvw2YCPcrKF47joNKRvzp44leUe5HtVkJGx8RQ==      Full
key2        kmEynIs3xnpmpSxWbU41h5a7DZD7v4gGV3yXa2NbPbmhrPt10+QmE5Pk0xxypeSqbqzd9si+ArNvbsqIRuLH2Lw==      Full

PS C:\WINDOWS\system32>
```

Add the blob URI to the host file

You already added the blob URI in the hosts file for the client that you're using to connect to Azure Blob Storage in **Modify host file for endpoint name resolution** of [Connecting to Azure Resource Manager on your Azure Stack Edge device](#). This entry was used to add the blob URI:

```
<Device IP address> <storage name>.blob.<appliance name>.<dnsdomain>
```

Install certificates

If you're using HTTPS, you need to install the appropriate certificates on your device. Here, you install the blob endpoint certificate. For more information, see [Use certificates with your Azure Stack Edge Pro with GPU device](#).

Upload a VHD

Copy any disk images to be used into page blobs in the local storage account that you created earlier. You can use a tool such as [AzCopy](#) to upload the virtual hard disk (VHD) to the storage account.

- [Az](#)
- [AzureRM](#)

Use the following commands with AzCopy 10:

1. Set some parameters including the appropriate version of APIs for AzCopy. In this example, AzCopy 10 was used.

```
$Env:AZCOPY_DEFAULT_SERVICE_API_VERSION="2019-07-07"
$ContainerName = <Container name>
$ResourceGroupName = <Resource group name>
$StorageAccountName = <Storage account name>
$VHDPath = "Full VHD Path"
$VHDFile = <VHD file name>
```

2. Copy the VHD from the source (in this case, local system) to the storage account that you created on your device in the earlier step.

```
$StorageAccountKey = (Get-AzStorageAccountKey -ResourceGroupName $ResourceGroupName -Name
$StorageAccountName)[0].Value
$endPoint = (Get-AzStorageAccount -name $StorageAccountName -ResourceGroupName
$ResourceGroupName).PrimaryEndpoints.Blob
$StorageAccountContext = New-AzStorageContext -StorageAccountName $StorageAccountName -
StorageAccountKey $StorageAccountKey -Endpoint $endpoint
$StorageAccountSAS = New-AzStorageAccountSASToken -Service Blob -ResourceType
Container,Service,Object -Permission "acdlrw" -Context $StorageAccountContext -Protocol HttpsOnly
<Path to azcopy.exe> cp "$VHDPath\$VHDFile" "$endPoint$ContainerName$StorageAccountSAS"
```

Here's an example output:

```
PS C:\windows\system32> $ContainerName = "testcontainer1"
PS C:\windows\system32> $ResourceGroupName = "myaseazrg"
PS C:\windows\system32> $StorageAccountName = "myaseazsa"
PS C:\windows\system32> $VHDPath = "C:\Users\alkohli\Downloads\Ubuntu1604"
PS C:\windows\system32> $VHDFile = "ubuntu13.vhd"

PS C:\windows\system32> $StorageAccountKey = (Get-AzStorageAccountKey -ResourceGroupName
$ResourceGroupName -Name $StorageAccountName)[0].Value
PS C:\windows\system32> $endPoint = (Get-AzStorageAccount -name $StorageAccountName -
ResourceGroupName $ResourceGroupName).PrimaryEndpoints.Blob
PS C:\windows\system32> $StorageAccountContext = New-AzStorageContext -StorageAccountName
$StorageAccountName -StorageAccountKey $StorageAccountKey -Endpoint $endpoint
PS C:\windows\system32> $StorageAccountSAS = New-AzStorageAccountSASToken -Service Blob -ResourceType
Container,Service,Object -Permission "acdlrw" -Context $StorageAccountContext -Protocol HttpsOnly

PS C:\windows\system32> C:\azcopy\azcopy_windows_amd64_10.10.0\azcopy.exe cp "$VHDPath\$VHDFile"
"$endPoint$ContainerName$StorageAccountSAS"
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or destination doesn't have full
folder support

Job 72a5e3dd-9210-3e43-6691-6bebd4875760 has started
Log file is located at: C:\Users\alkohli\.azcopy\72a5e3dd-9210-3e43-6691-6bebd4875760.log

INFO: azcopy.exe: A newer version 10.11.0 is available to download
```

Create a managed disk from the VHD

You will now create a managed disk from the uploaded VHD.

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$DiskName = "<Managed disk name>"
```

2. Create a managed disk from uploaded VHD. To get the source URL for your VHD, go to the container in the storage account that contains the VHD in Storage Explorer. Select the VHD, and right-click and then select **Properties**. In the **Blob properties** dialog, select the **URI**.

```
$StorageAccountId = (Get-AzStorageAccount -ResourceGroupName $ResourceGroupName -Name
$StorageAccountName).Id
$DiskConfig = New-AzDiskConfig -Location DBELocal -StorageAccountId $StorageAccountId -CreateOption
Import -SourceUri "Source URL for your VHD"
New-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName -Disk $DiskConfig
```

Here's an example output..

```
PS C:\WINDOWS\system32> $DiskName = "myazmd"
PS C:\WINDOWS\system32> $StorageAccountId = (Get-AzStorageAccount -ResourceGroupName
$ResourceGroupName -Name $StorageAccountName).Id
PS C:\WINDOWS\system32> $DiskConfig = New-AzDiskConfig -Location DBELocal -StorageAccountId
$StorageAccountId -CreateOption Import -SourceUri
"https://myaseazsa.blob.myasegpu.wdshcsso.com/testcontainer1/ubuntu13.vhd"
PS C:\WINDOWS\system32> New-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName -Disk
$DiskConfig

ResourceGroupName      : myaseazrg
ManagedBy             :
Sku                  : Microsoft.Azure.Management.Compute.Models.DiskSku
Zones                :
TimeCreated          : 6/24/2021 12:19:56 PM
OsType               :
HyperVGeneration     :
CreationData          : Microsoft.Azure.Management.Compute.Models.CreationDat
                      a
DiskSizeGB            : 30
DiskSizeBytes         : 32212254720
UniqueId              : 53743801-cbf2-4d2f-acb4-971d037a9395
EncryptionSettingsCollection : 
ProvisioningState    : Succeeded
DiskIOPSReadWrite    : 500
DiskMBpsReadWrite   : 60
DiskState             : Unattached
Encryption           : Microsoft.Azure.Management.Compute.Models.Encryption
Id                   : /subscriptions/.../r
                      esourceGroups/myaseazrg/providers/Microsoft.Compute/d
                      isks/myazmd
Name                 : myazmd
Type                 : Microsoft.Compute/disks
Location             : DBELocal
Tags                : {}

PS C:\WINDOWS\system32>
```

Create a VM image from the managed disk

You'll now create a VM image from the managed disk.

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$DiskSize = "<Size greater than or equal to size of source managed disk>"
$OsType = "<linux or windows>"
$imageName = "<Image name>"
$hyperVGeneration = "<Generation of the image: V1 or V2>"
```

2. Create a VM image. The supported OS types are Linux and Windows.

```
$imageConfig = New-AzImageConfig -Location DBELocal -HyperVGeneration $hyperVGeneration
$ManagedDiskId = (Get-AzDisk -Name $DiskName -ResourceGroupName $ResourceGroupName).Id
Set-AzImageOsDisk -Image $imageConfig -OsType $OsType -OsState 'Generalized' -DiskSizeGB $DiskSize -
ManagedDiskId $ManagedDiskId
New-AzImage -Image $imageConfig -ImageName $ImageName -ResourceGroupName $ResourceGroupName
```

Here's an example output.

```
PS C:\WINDOWS\system32> $OsType = "linux"
PS C:\WINDOWS\system32> $ImageName = "myaseazlinuxvmimage"
PS C:\WINDOWS\system32> $DiskSize = 35
PS C:\WINDOWS\system32> $imageConfig = New-AzImageConfig -Location DBELocal
PS C:\WINDOWS\system32> $ManagedDiskId = (Get-AzDisk -Name $DiskName -ResourceGroupName
$ResourceGroupName).Id
PS C:\WINDOWS\system32> Set-AzImageOsDisk -Image $imageConfig -OsType $OsType -OsState 'Generalized'
-DiskSizeGB $DiskSize -ManagedDiskId $ManagedDiskId

ResourceGroupName      :
SourceVirtualMachine :
StorageProfile        : Microsoft.Azure.Management.Compute.Models.ImageStorageProfile
ProvisioningState     :
HyperVGeneration     : V1
Id                   :
Name                 :
Type                 :
Location             : DBELocal
Tags                :

PS C:\WINDOWS\system32> New-AzImage -Image $imageConfig -ImageName $ImageName -ResourceGroupName
$ResourceGroupName

ResourceGroupName      : myaseazrg
SourceVirtualMachine   :
StorageProfile        : Microsoft.Azure.Management.Compute.Models.ImageStorageProfile
ProvisioningState     : Succeeded
HyperVGeneration     : V1
Id                   : /subscriptions/.../resourceG
                           rups/myaseazrg/providers/Microsoft.Compute/images/myaseazlin
                           uxvmimage
Name                 : myaseazlinuxvmimage
Type                 : Microsoft.Compute/images
Location             : dbelocal
Tags                : {}

PS C:\WINDOWS\system32>
```

Create your VM with previously created resources

Before you create and deploy the VM, you must create one virtual network and associate a virtual network interface with it.

IMPORTANT

The following rules apply:

- You can create only one virtual network, even across resource groups. The virtual network must have exactly the same address space as the logical network.
- The virtual network can have only one subnet. The subnet must have exactly the same address space as the virtual network.
- When you create the virtual network interface card, you can use only the static allocation method. The user needs to provide a private IP address.

Query the automatically created virtual network

When you enable compute from the local UI of your device, a virtual network called `ASEVNET` is created automatically, under the `ASERG` resource group.

- [Az](#)
- [AzureRM](#)

Use the following command to query the existing virtual network:

```
$ArmVN = Get-AzVirtualNetwork -Name ASEVNET -ResourceGroupName ASERG
```

Create a virtual network interface card

You'll create a virtual network interface card by using the virtual network subnet ID.

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$IpConfigName = "<IP config name>"  
$NicName = "<Network interface name>"
```

2. Create a virtual network interface.

```
$ipConfig = New-AzNetworkInterfaceIpConfig -Name $IpConfigName -SubnetId $aRmVN.Subnets[0].Id  
$Nic = New-AzNetworkInterface -Name $NicName -ResourceGroupName $ResourceGroupName -Location DBELocal  
-IpConfiguration $IpConfig
```

By default, an IP is dynamically assigned to your network interface from the network enabled for compute. Use the `-PrivateIpAddress` parameter if you are allocating a static IP to your network interface.

Here's an example output:

```

PS C:\WINDOWS\system32> $IpConfigName = "myazipconfig1"
PS C:\WINDOWS\system32> $NicName = "myaznic1"
PS C:\WINDOWS\system32> $ipConfig = New-AzNetworkInterfaceIpConfig -Name $IpConfigName -SubnetId
$aRmVN.Subnets[0].Id
PS C:\WINDOWS\system32> $ipConfig = New-AzNetworkInterfaceIpConfig -Name $IpConfigName -SubnetId
$aRmVN.Subnets[0].Id
PS C:\WINDOWS\system32> $Nic = New-AzNetworkInterface -Name $NicName -ResourceGroupName
$ResourceGroupName -Location DBELocal -IpConfiguration $IpConfig
PS C:\WINDOWS\system32> $Nic

Name : myaznic1
ResourceGroupName : myaseazrg
Location : dbelocal
Id : /subscriptions/.../re
      sourceGroups/myaseazrg/providers/Microsoft.Network/networkInterfaces/myaznic1
Etag : W/"0b20057b-2102-4f34-958b-656327c0fb1d"
ResourceGuid : e7d4131f-6f01-4492-9d4c-a8ff1af7244f
ProvisioningState : Succeeded
Tags :
VirtualMachine : null
IpConfigurations : [
    {
        "Name": "myazipconfig1",
        "Etag":
        "W/"0b20057b-2102-4f34-958b-656327c0fb1d"",
        "Id":
        "/subscriptions/.../resourceGroups/myaseazrg/providers/Microsoft.
          Network/networkInterfaces/myaznic1/ipConfigurations/my
          azipconfig1",
        "PrivateIpAddress": "10.126.76.60",
        "PrivateIpAllocationMethod": "Dynamic",
        "Subnet": {
            "Delegations": [],
            "Id":
            "/subscriptions/.../resourceGroups/ASERG/providers/Microsoft.Ne
              twork/virtualNetworks/ASEVNET/subnets/ASEVNETsubNet",
            "ServiceAssociationLinks": []
        },
        "ProvisioningState": "Succeeded",
        "PrivateIpAddressVersion": "IPv4",
        "LoadBalancerBackendAddressPools": [],
        "LoadBalancerInboundNatRules": [],
        "Primary": true,
        "ApplicationGatewayBackendAddressPools": [],
        "ApplicationSecurityGroups": []
    }
]
DnsSettings : {
    "DnsServers": [],
    "AppliedDnsServers": [],
    "InternalDomainNameSuffix": "auwlfcx0dhxurjgisct43fc
      ywb.a--x.internal.cloudapp.net"
}
EnableIPForwarding : False
EnableAcceleratedNetworking : False
NetworkSecurityGroup : null
Primary :
MacAddress : 001DD84A58D1

```

```
PS C:\WINDOWS\system32>
```

Optionally, while you're creating a virtual network interface card for a VM, you can pass the public IP. In this instance, the public IP returns the private IP.

```
New-AzPublicIPAddress -Name <Public IP> -ResourceGroupName <ResourceGroupName> -AllocationMethod Static -  
Location DBELocal  
$publicIP = (Get-AzPublicIPAddress -Name <Public IP> -ResourceGroupName <Resource group name>).Id  
$ipConfig = New-AzNetworkInterfaceIpConfig -Name <ConfigName> -PublicIpAddressId $publicIP -SubnetId  
$subNetId
```

Create a VM

You can now use the VM image to create a VM and attach it to the virtual network that you created earlier.

- [Az](#)
- [AzureRM](#)

1. Set the username and password to sign in to the VM that you want to create.

```
$pass = ConvertTo-SecureString "<Password>" -AsPlainText -Force;  
$cred = New-Object System.Management.Automation.PSCredential("<Enter username>", $pass)
```

After you've created and powered up the VM, you'll use the preceding username and password to sign in to it.

2. Set the parameters.

```
$VmName = "<VM name>"  
$ComputerName = "<VM display name>"  
$OsDiskName = "<OS disk name>"
```

3. Create the VM.

```
$VirtualMachine = New-AzVMConfig -VmName $VmName -VMSize "Standard_D1_v2"  
  
$VirtualMachine = Set-AzVMOperatingSystem -VM $VirtualMachine -Linux -ComputerName $ComputerName -  
Credential $cred  
  
$VirtualMachine = Set-AzVmOsDisk -VM $VirtualMachine -Name $OsDiskName -Caching "ReadWrite" -  
CreateOption "FromImage" -Linux -StorageAccountType Standard_LRS  
  
$nicID = (Get-AzNetworkInterface -Name $NicName -ResourceGroupName $ResourceGroupName).Id  
  
$VirtualMachine = Add-AzVMNetworkInterface -Vm $VirtualMachine -Id $nicID  
  
$image = ( Get-AzImage -ResourceGroupName $ResourceGroupName -ImageName $ImageName).Id  
  
$VirtualMachine = Set-AzVMSourceImage -VM $VirtualMachine -Id $image  
  
New-AzVM -ResourceGroupName $ResourceGroupName -Location DBELocal -VM $VirtualMachine -Verbose
```

Here's an example output.

```

PS C:\WINDOWS\system32> $pass = ConvertTo-SecureString "Password1" -AsPlainText -Force;
PS C:\WINDOWS\system32> $cred = New-Object System.Management.Automation.PSCredential("myazuser",
$pass)
PS C:\WINDOWS\system32> $VmName = "myazvm"
>> $ComputerName = "myazvmfriendlyname"
>> $OsDiskName = "myazosdisk1"
PS C:\WINDOWS\system32> $VirtualMachine = New-AzVMConfig -VmName $VmName -VMSize "Standard_D1_v2"
PS C:\WINDOWS\system32> $VirtualMachine = Set-AzVMOperatingSystem -VM $VirtualMachine -Linux -
ComputerName $ComputerName -Credential $cred
PS C:\WINDOWS\system32> $VirtualMachine = Set-AzVmOsDisk -VM $VirtualMachine -Name $OsDiskName -
Caching "ReadWrite" -CreateOption "FromImage" -Linux -StorageAccountType Standard_LRS
PS C:\WINDOWS\system32> $nicID = (Get-AzNetworkInterface -Name $NicName -ResourceGroupName
$ResourceGroupName).Id
PS C:\WINDOWS\system32>
$nicID/subscriptions/.../resourceGroups/myaseazrg/providers/Microsoft.Network/networkInterfaces/myazn
ic1
PS C:\WINDOWS\system32> $VirtualMachine = Add-AzVMNetworkInterface -VM $VirtualMachine -Id $nicID
PS C:\WINDOWS\system32> $image = ( Get-AzImage -ResourceGroupName $ResourceGroupName -ImageName
$imageName).Id
PS C:\WINDOWS\system32> $VirtualMachine = Set-AzVMSourceImage -VM $VirtualMachine -Id $image
PS C:\WINDOWS\system32> New-AzVM -ResourceGroupName $ResourceGroupName -Location DBELocal -VM
$VirtualMachine -Verbose
WARNING: Since the VM is created using premium storage or managed disk, existing
standard storage account, myaseazsa, is used for boot diagnostics.
VERBOSE: Performing the operation "New" on target "myazvm".

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
----- -----
True          OK   OK

```

4. To figure out the IP assigned to the VM that you created, query the virtual network interface that you created. Locate the `PrivateIPAddress` and copy the IP for your VM. Here's an example output.

```

PS C:\WINDOWS\system32> $Nic

Name : myaznic1
ResourceGroupName : myaseazrg
Location : dbelocal
Id : /subscriptions/.../re
      sourceGroups/myaseazrg/providers/Microsoft.Network/net
      workInterfaces/myaznic1
Etag : W/"0b20057b-2102-4f34-958b-656327c0fb1d"
ResourceGuid : e7d4131f-6f01-4492-9d4c-a8ff1af7244f
ProvisioningState : Succeeded
Tags :
VirtualMachine : null
IpConfigurations : [
    {
        "Name": "myazipconfig1",
        "Etag":
        "W/"0b20057b-2102-4f34-958b-656327c0fb1d"",
        "Id":
        "/subscriptions/.../resourceGroups/myaseazrg/providers/Microsoft.
          Network/networkInterfaces/myaznic1/ipConfigurations/my
          azipconfig1",
        "PrivateIpAddress": "10.126.76.60",
        "PrivateIpAllocationMethod": "Dynamic",
        "Subnet": {
            "Delegations": [],
            "Id":
            "/subscriptions/.../resourceGroups/ASERG/providers/Microsoft.Ne
              twork/virtualNetworks/ASEVNET/subnets/ASEVNETsubNet",
            "ServiceAssociationLinks": []
        },
        "ProvisioningState": "Succeeded",
        "PrivateIpAddressVersion": "IPv4",
        "LoadBalancerBackendAddressPools": [],
        "LoadBalancerInboundNatRules": [],
        "Primary": true,
        "ApplicationGatewayBackendAddressPools": [],
        "ApplicationSecurityGroups": []
    }
]
DnsSettings : {
    "DnsServers": [],
    "AppliedDnsServers": [],
    "InternalDomainNameSuffix": "auwlfcx0dhxurjgisct43fc
ywb.--x.internal.cloudapp.net"
}
EnableIPForwarding : False
EnableAcceleratedNetworking : False
NetworkSecurityGroup : null
Primary :
MacAddress : 001DD84A58D1

PS C:\WINDOWS\system32>

```

Connect to the VM

Depending on whether you created a Windows VM or a Linux VM, the connection instructions can be different.

Connect to a Linux VM

To connect to a Linux VM, do the following:

Connect to the VM by using the private IP that you passed during the VM creation.

1. Open an SSH session to connect with the IP address.

```
ssh -l <username> <ip address>
```

2. At the prompt, provide the password that you used when you created the VM.

If you need to provide the SSH key, use this command.

```
ssh -i c:/users/Administrator/.ssh/id_rsa Administrator@5.5.41.236
```

Here's an example output when you connect to the VM:

```
PS C:\WINDOWS\system32> ssh -l myazuser "10.126.76.60"
The authenticity of host '10.126.76.60 (10.126.76.60)' can't be established.
ECDSA key fingerprint is SHA256:V649Zbo58zAYMKreeP7M6w7Na0Yf9QPg4SM7JZVV0E4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.126.76.60' (ECDSA) to the list of known hosts.
myazuser@10.126.76.60's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.18.0-1013-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information disabled due to load higher than 1.0

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

284 packages can be updated.
192 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

myazuser@myazvmfriendlyname:~$ client_loop: send disconnect: Connection reset
PS C:\WINDOWS\system32>
```

If you used a public IP address during the VM creation, you can use that IP to connect to the VM. To get the public IP, run the following command:

- [Az](#)
- [AzureRM](#)

```
$publicIp = Get-AzPublicIpAddress -Name $PublicIp -ResourceGroupName $ResourceGroupName
```

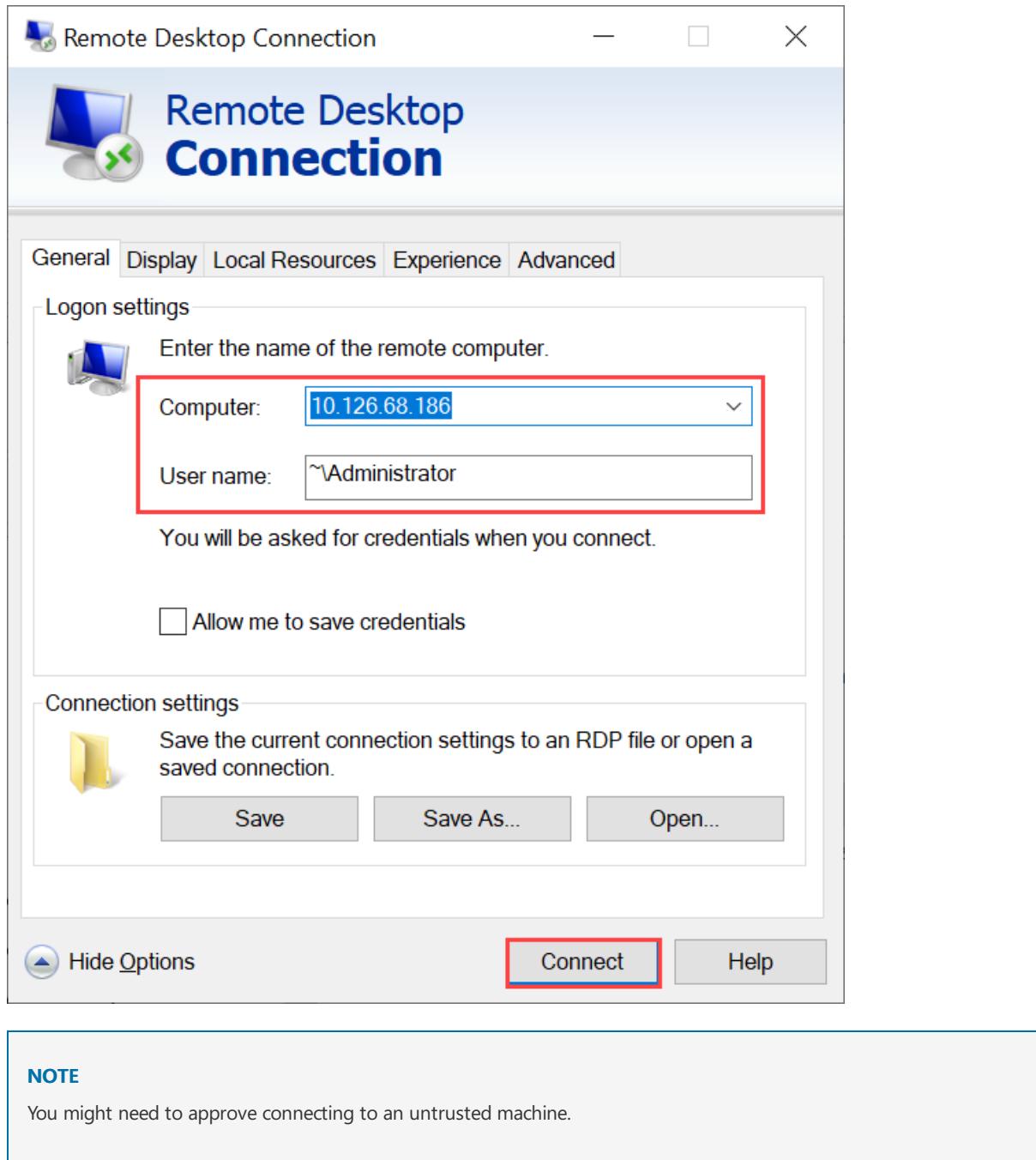
In this instance, the public IP is the same as the private IP that you passed during the creation of the virtual network interface.

Connect to a Windows VM

To connect to a Windows VM, do the following:

Connect to your Windows VM by using the Remote Desktop Protocol (RDP) via the IP that you passed during the VM creation.

1. On your client, open RDP.
2. Go to **Start**, and then enter **mstsc**.
3. On the **Remote Desktop Connection** pane, enter the IP address of the VM and the access credentials you used in the VM template parameters file. Then select **Connect**.



You're now signed in to your VM that runs on the appliance.

Manage the VM

The following sections describe some of the common operations that you can create on your Azure Stack Edge Pro device.

List VMs that are running on the device

To return a list of all the VMs that are running on your Azure Stack Edge device, run this command:

- [Az](#)
- [AzureRM](#)

```
Get-AzVM [-ResourceGroupName <String>] -Name <String>
```

For more information about this cmdlet, see [Get-AzVM](#).

Turn on the VM

To turn on a virtual machine that's running on your device, run the following cmdlet:

- [Az](#)
- [AzureRM](#)

```
Start-AzVM [-Name] <String> [-ResourceGroupName] <String>
```

For more information about this cmdlet, see [Start-AzVM](#).

Suspend or shut down the VM

To stop or shut down a virtual machine that's running on your device, run the following cmdlet:

- [Az](#)
- [AzureRM](#)

```
Stop-AzVM [-Name] <String> [-StayProvisioned] [-ResourceGroupName] <String>
```

For more information about this cmdlet, see [Stop-AzVM cmdlet](#).

Add a data disk

If the workload requirements on your VM increase, you might need to add a data disk. To do so, run the following command:

- [Az](#)
- [AzureRM](#)

```
Add-AzRmVMDataDisk -VM $VirtualMachine -Name "disk1" -VhdUri  
"https://contoso.blob.core.windows.net/vhds/diskstandard03.vhd" -LUN 0 -Caching ReadOnly -DiskSizeinGB 1 -  
CreateOption Empty  
  
Update-AzVM -ResourceGroupName "<Resource Group Name string>" -VM $VirtualMachine
```

Delete the VM

To remove a virtual machine from your device, run the following cmdlet:

- [Az](#)
- [AzureRM](#)

```
Remove-AzVM [-Name] <String> [-ResourceGroupName] <String>
```

For more information about this cmdlet, see [Remove-AzVm cmdlet](#).

Next steps

[Azure Resource Manager cmdlets](#)

Deploy VMs on your Azure Stack Edge Pro GPU device via Azure PowerShell script

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This tutorial describes how to create and manage a VM on your Azure Stack Edge Pro device using an Azure PowerShell script.

Prerequisites

Before you begin creating and managing a VM on your Azure Stack Edge Pro device using this script, you need to make sure you have completed the prerequisites listed in the following steps:

For Azure Stack Edge Pro device via the local web UI

Before you can deploy VMs on your Azure Stack Edge device, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

Make sure that you can use the following steps to access the device from your client. You've already done this configuration when you connected to Azure Resource Manager, and now you're verifying that the configuration was successful.

1. Verify that Azure Resource Manager communication is working by running the following command:

- [Az](#)
- [AzureRM](#)

```
Add-AzEnvironment -Name <Environment Name> -ARMEndpoint "https://management.<appliance name>. <DNSDomain>"
```

2. To call the local device APIs to authenticate, enter:

- [Az](#)
- [AzureRM](#)

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

To connect via Azure Resource Manager, provide the username *EdgeArmUser* and your password.

3. If you configured compute for Kubernetes, you can skip this step. Otherwise, ensure that you've enabled a network interface for compute by doing the following:
 - a. On your local user interface, go to **Compute** settings.
 - b. Select the network interface that you want to use to create a virtual switch. The VMs you create will be attached to a virtual switch that's attached to this port and the associated network. Be sure to choose a network that matches the IP address you'll use for the VM.

c. Under **Enable for compute** on the network interface, select Yes. Azure Stack Edge will create and manage a virtual switch that corresponds to that network interface. Don't enter specific IPs for Kubernetes at this time. It can take several minutes to enable compute.

NOTE

If you're creating GPU VMs, select a network interface that's connected to the internet. Doing so enables you to install a GPU extension on your device.

For your Windows client

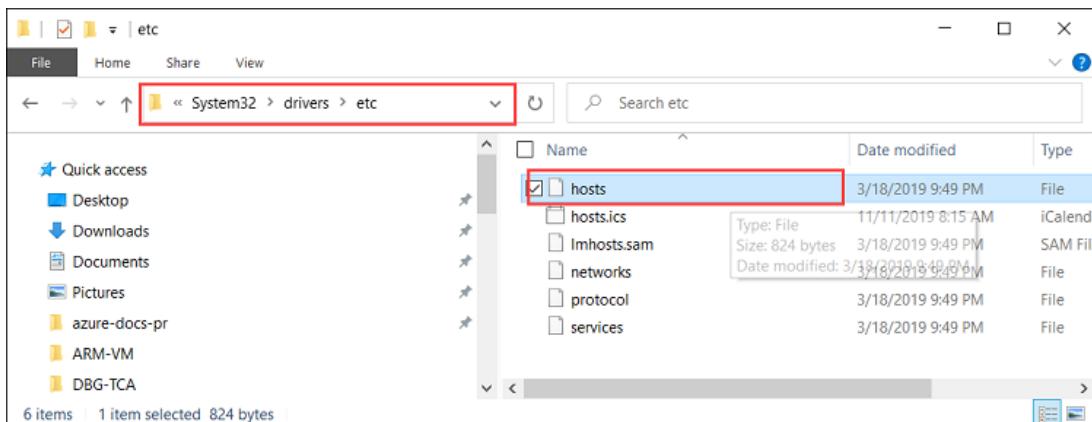
1. Make sure that you have modified:

- The host file on the client, OR,
- The DNS server configuration

IMPORTANT

We recommend that you modify the DNS server configuration for endpoint name resolution.

a. Start **Notepad** as an administrator (Administrator privileges is required to save the file), and then open the **hosts** file located at `C:\Windows\System32\Drivers\etc`.

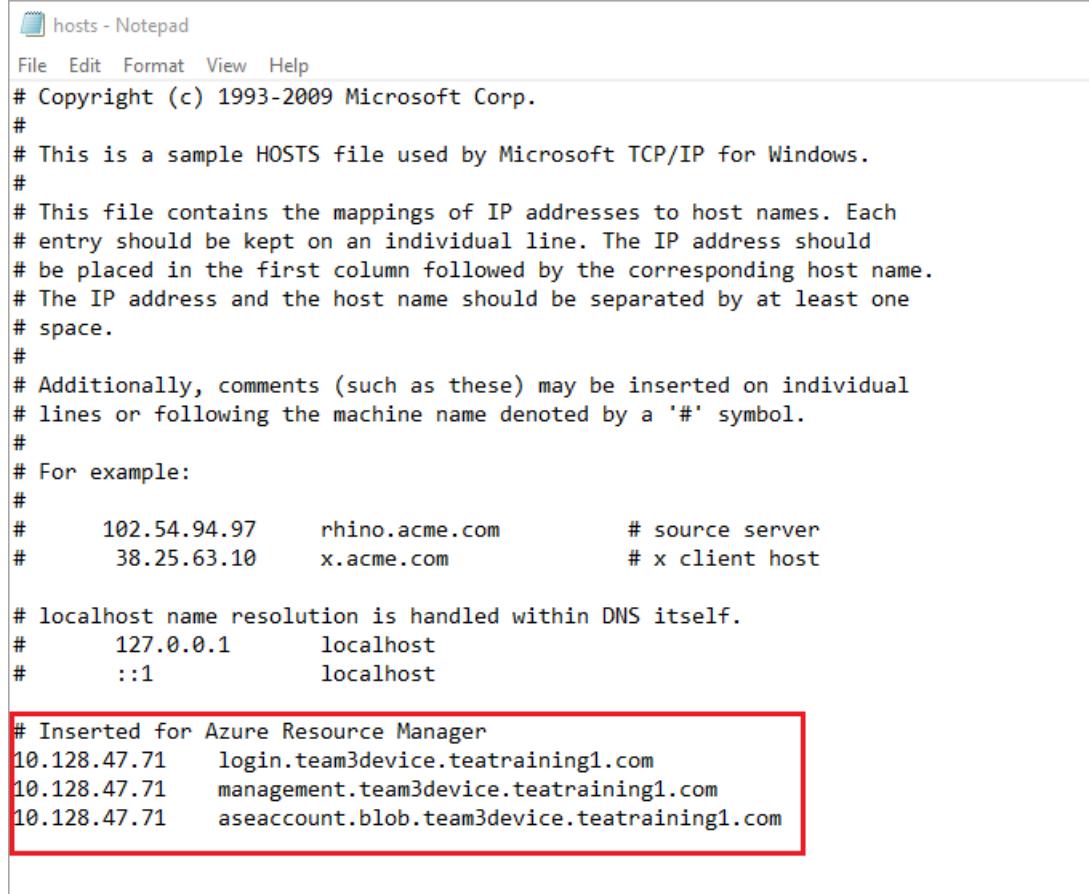


b. Add the following entries to your **hosts** file replacing with appropriate values for your device:

```
<device IP> login.<appliance name>.<DNS domain>
<device IP> management.<appliance name>.<DNS domain>
<device IP> <storage name>.blob.<appliance name>.<DNS domain>
```

For the storage account, you can provide a name that you want the script to use later to create a new storage account. The script does not check if that storage account is existing.

- c. Use the following image for reference. Save the **hosts** file.



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com        # source server
#      38.25.63.10      x.acme.com            # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost

# Inserted for Azure Resource Manager
10.128.47.71    login.team3device.teatraining1.com
10.128.47.71    management.team3device.teatraining1.com
10.128.47.71    aseaccount.blob.team3device.teatraining1.com
```

2. [Download the PowerShell script](#) used in this procedure.
3. Make sure that your Windows client is running PowerShell 5.0 or later.
4. Make sure that the [Azure.Storage Module version 4.5.0](#) is installed on your system. You can get this module from the [PowerShell Gallery](#). To install this module, type:

```
Install-Module -Name Azure.Storage -RequiredVersion 4.5.0
```

To verify the version of the installed module, type:

```
Get-InstalledModule -name Azure.Storage
```

To uninstall any other version modules, type:

```
Uninstall-Module -Name Azure.Storage
```

5. [Download AzCopy 10](#) to your Windows client. Make a note of this location as you will pass it as a parameter while running the script.
6. Make sure that your Windows client is running TLS 1.2 or later.

Create a VM

1. Run PowerShell as an administrator.
2. Go to the folder where you downloaded the script on your client.
3. Before you run the script, make sure you are still connected to the local Azure Resource Manager of the device and the connection has not expired.

```
PS C:\windows\system32> login-AzureRMAccount -EnvironmentName aztest1 -TenantId c0257de7-538f-415c-993a-1b87a031879d

Account          SubscriptionName      TenantId          Environment
-----          -----          -----
EdgeArmUser@localhost  Default Provider Subscription c0257de7-538f-415c-993a-1b87a031879d aztest1

PS C:\windows\system32> cd C:\Users\v2
PS C:\Users\v2>
```

4. Use the following command to run the script:

```
.\ArmPowershellClient.ps1 -NicPrivateIp <Private IP> -VHDPath <Path> -VHDFile <VHD File, with extension> -StorageAccountName <Name> -OS <Windows/Linux> -VMSize <Supported VM Size> -VMUserName <Username to be used to sign in to VM> -VMPassword <Password for the VM> --AzCopy10Path <Absolute Path>
```

If you want the IP to be dynamically allocated to the VM, omit the `-NicPrivateIp` parameter.

Here are the examples when the script is run to create a Windows VM and a Linux VM.

For a Windows VM:

Here is a sample output for a Windows VM that was created.

```
PS C:\Users\v2> .\ArmPowershellClient.ps1 -VHDPath \\asefs\Logs\vmvh -VHDFile
WindowsServer2016Datacenter.vhd -StorageAccountName myasesatest -OS Windows -VMSize Standard_D1_v2 -
VMUserName Administrator -VMPassword Password1 -AzCopy10Path C:\Users\AzCopy10\AzCopy.exe
New-AzureRmResourceGroup -Name rg201221071831 -Location DBELocal -Force
Successfully created Resource Group:rg201221071831
Successfully created Resource Group:StorAccRG
Get-AzureRmStorageAccount -Name myasesatest -ResourceGroupName StorAccRG -ErrorAction
SilentlyContinue
New-AzureRmStorageAccount -Name myasesatest -ResourceGroupName StorAccRG -SkuName Standard_LRS -
Location DBELocal

Created New Storage Account
Get-AzureRmStorageAccount -name myasesatest -resourcegroupname
StorageAccountName ResourceGroupName Location SkuName      Kind     AccessTier CreationTime
ProvisioningState EnableHttpsTrafficOnly
-----
myasesatest      StorAccRG        DBELocal  StandardLRS Storage           12/22/2020 3:18:38 AM
Succeeded        False           DBELocal  StandardLRS Storage           12/22/2020 3:18:38 AM
myasesatest      StorAccRG        DBELocal  StandardLRS Storage           12/22/2020 3:18:38 AM
Succeeded        False           DBELocal  StandardLRS Storage           12/22/2020 3:18:38 AM

Uploading Vhd to Storage Account

New-AzureStorageContext -StorageAccountName myasesatest -StorageAccountKey
hyibjhVlOR0gTlU1nQJlxrg94eGDhF+RIQ71Z7UVZIx0OPM1HP274NUhZtA1hMxBcpk2BVApiFasFPEhY/A== -Endpoint
https://myasesatest.blob.myasepuvm.wdshcsso.com/

New-AzureStorageAccountSASToken -Service Blob,File,Queue,Table -ResourceType Container,Service,Object
-Permission

SAS Token : ?sv=2017-07-29&sig=TXaGbium9tFFaJnu3SFmDus1JuqNiNQwvuHfpPJMYN0%3D&spr=https&se=2020-12-
22T04%3A18%3A43Z&srt=sco&ss=bfqt&sp=racwd1
```

```
C:\Users\AzCopy10\AzCopy.exe make https://myasesatest.blob.myasegpuvm.wdshcsso.com/vmimages?sv=2017-07-29&sig=TXaGbium9tFFaJnu3SFmDuslJuqNiNQwvuHfpPJMYN0%3D&spr=https&se=2020-12-22T04%3A18%3A43Z&srt=sco&ss=bfqt&sp=racwd1
```

Successfully created the resource.

```
AzCopy cp \\asefs\Logs\vmvhd\WindowsServer2016Datacenter.vhd  
https://myasesatest.blob.myasegpuvm.wdshcsso.com/vmimages?sv=2017-07-29&sig=TXaGbium9tFFaJnu3SFmDuslJuqNiNQwvuHfpPJMYN0%3D&spr=https&se=2020-12-22T04%3A18%3A43Z&srt=sco&ss=bfqt&sp=racwd1
```

INFO: Scanning...

```
Job b6f54665-93c4-2f47-4770-5f3b7b0de2dc has started  
Log file is located at: C:\Users\Administrator\.azcopy\b6f54665-93c4-2f47-4770-5f3b7b0de2dc.log
```

INFO: AzCopy.exe: A newer version 10.8.0 is available to download

99.9 %, 0 Done, 0 Failed, 1 Pending, 0 Skipped, 1 Total, (Disk may be limiting speed)

```
Job b6f54665-93c4-2f47-4770-5f3b7b0de2dc summary
```

Elapsed Time (Minutes): 12.7717

Total Number Of Transfers: 1

Number of Transfers Completed: 1

Number of Transfers Failed: 0

Number of Transfers Skipped: 0

TotalBytesTransferred: 13958644224

Final Job Status: Completed

VHD Upload Done

Creating a new managed disk

```
= New-AzureRmDiskConfig -Location DBELocal -CreateOption Import -SourceUri
```

```
Microsoft.Azure.Commands.Compute.Automation.Models.PSDisk
```

```
New-AzureRmDisk -ResourceGroupName rg201221071831 -DiskName ld201221071831 -Disk
```

```
ResourceGroupName : rg201221071831
ManagedBy        :
Sku              : Microsoft.Azure.Management.Compute.Models.DiskSku
Zones            :
TimeCreated      : 12/21/2020 7:31:35 PM
OsType           :
CreationData     : Microsoft.Azure.Management.Compute.Models.CreationData
DiskSizeGB       : 13
EncryptionSettings :
ProvisioningState : Succeeded
Id               : /subscriptions/947b3cfcd-7a1b-4a90-7cc5-e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Compute/disks/ld201221071831
Name             : ld201221071831
Type             : Microsoft.Compute/disks
Location         : DBELocal
Tags             : {}
```

Created a new managed disk

Creating a new Image out of managed disk

```
ResourceGroupName   :
SourceVirtualMachine :
StorageProfile       : Microsoft.Azure.Management.Compute.Models.ImageStorageProfile
ProvisioningState    :
Id                  :
Name                :
Type                :
Location            : DBELocal
Tags                :
```

```

New-AzureRmImage -Image Microsoft.Azure.Commands.Compute.Automation.Models.PSImage -ImageName ig201221071831 -ResourceGroupName rg201221071831 -HyperVGeneration V1

ResourceGroupName      : rg201221071831
SourceVirtualMachine   :
StorageProfile         : Microsoft.Azure.Management.Compute.Models.ImageStorageProfile
ProvisioningState      : Succeeded
Id                   : /subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Compute/images/ig201221071831
Name                 : ig201221071831
Type                  : Microsoft.Compute/images
Location              : dbelocal
Tags                  : {}

Created a new Image

Using Vnet /subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/ASERG/providers/Microsoft.Network/virtualNetworks/ASEVNET

Creating a new Network Interface
WARNING: The output object type of this cmdlet will be modified in a future release.

VirtualMachine          :
IpConfigurations        : {ip201221071831}
DnsSettings             : Microsoft.Azure.Commands.Network.Models.PSNetworkInterfaceDnsSettings
MacAddress               : 001DD87D7216
Primary                 :
EnableAcceleratedNetworking : False
EnableIPForwarding       : False
NetworkSecurityGroup     :
ProvisioningState        : Succeeded
VirtualMachineText       : null
IpConfigurationsText    : [
    {
        "Name": "ip201221071831",
        "Etag": "W/\"27785dd5-d12a-4d73-9495-ffad7847261a\"",
        "Id": "/subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Network/networkInterfaces/nic201221071
831/ipConfigurations/ip201221071831",
        "PrivateIpAddress": "10.57.51.61",
        "PrivateIpAllocationMethod": "Dynamic",
        "Subnet": {
            "Id": "/subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/ASERG/providers/Microsoft.Network/virtualNetworks/ASEVNET/subnets/ASEVNET
subNet",
            "ResourceNavigationLinks": [],
            "ServiceEndpoints": []
        },
        "ProvisioningState": "Succeeded",
        "PrivateIpAddressVersion": "IPv4",
        "LoadBalancerBackendAddressPools": [],
        "LoadBalancerInboundNatRules": [],
        "Primary": true,
        "ApplicationGatewayBackendAddressPools": [],
        "ApplicationSecurityGroups": []
    }
]
DnsSettingsText          : {
    "DnsServers": [],
    "AppliedDnsServers": [],
    "InternalDomainNameSuffix": "qgotb4hjdh4efnhn0vz5adtb3f.a--x.internal.cloudapp.net"
}
NetworkSecurityGroupText  : null
ResourceGroupName         : rg201221071831
Location                 : dbelocal
ResourceGuid              : e6327ab9-0855-4f04-9b36-17bbf31b5bd8
Type                     : Microsoft.Network/networkInterfaces

```

```

Type          : MICROSOFT.NETWORK/NETWORKINTERFACES
Tag          :
TagsTable   :
Name         : nic201221071831
Etag         : W/"27785dd5-d12a-4d73-9495-ffad7847261a"
Id          : /subscriptions/947b3cf7-a1b-4a90-7cc5-
e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Network/networkInterfaces/nic201221071
831

Created Network Interface

Creating a new VM

New-AzureRmVMConfig -VMName VM201221071831 -VMSize Standard_D1_v2

Set-AzureRmVMOperatingSystem -VM Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine -Windows -
ComputerName COM201221071831 -Credential System.Management.Automation.PSCredential

Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine = Set-AzureRmVMOSDisk -VM
Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine -Name osld201221071831 -Caching ReadWrite -
CreateOption FromImage -Windows -StorageAccountType StandardLRS

Add-AzureRmVMNetworkInterface -VM Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine -Id
/subscriptions/947b3cf7-a1b-4a90-7cc5-
e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Network/networkInterfaces/nic201221071
831.Id

Set-AzureRmVMSourceImage -VM Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine -Id
/subscriptions/947b3cf7-a1b-4a90-7cc5-
e52caf221332/resourceGroups/rg201221071831/providers/Microsoft.Compute/images/ig201221071831

New-AzureRmVM -ResourceGroupName rg201221071831 -Location DBELocal -VM
Microsoft.Azure.Commands.Compute.Models.PSVirtualMachine -Verbose
WARNING: Since the VM is created using premium storage or managed disk, existing standard storage
account, myasesa1, is used for boot
diagnostics.
VERBOSE: Performing the operation "New" on target "VM201221071831".

Ticks          : 1533424841
Days           : 0
Hours          : 0
Milliseconds   : 342
Minutes        : 2
Seconds        : 33
TotalDays      : 0.00177479726967593
TotalHours     : 0.0425951344722222
TotalMilliseconds : 153342.4841
TotalMinutes   : 2.55570806833333
TotalSeconds   : 153.3424841

RequestId      :
.IsSuccessStatusCode : True
StatusCode       : OK
ReasonPhrase    : OK

PS C:\Users\v2>

```

For a Linux VM:

Here is the sample of the command that was used to create a Linux VM.

```

.\ArmPowershellClient.ps1 -VHDPath \\asefs\Logs\vmvhds -VHDFile ubuntu13.vhd -StorageAccountName
myasesatest -OS Linux -VMSize Standard_D1_v2 -VMUserName Administrator -VMPassword Password1 -
AzCopy10Path C:\Users\AzCopy10\AzCopy.exe
New-AzureRmResourceGroup -Name rg201221075546 -Location DBELocal -Force

```

5. Once you have successfully created the VMs, these VMs should show up in the list of virtual machines in the Azure portal. To view the VMs, in the Azure Stack Edge resource for your device in Azure portal, go to **Edge services > Virtual machines**.

Name	Status	Size	Disk
VM201221071831	Running	Standard_D1_v2	1
VM201221075546	Running	Standard_D1_v2	1

To view the details of a VM, select the VM name. Note the dynamic allocation of IP for this VM.

Virtual machine	Size	Networking
Computer name: COM201221071831	VM Size: D1_v2	IP Address: 10.57.51.61
OS: Windows	Offering: Standard	IP allocation method: Dynamic
Status: Running	vCPUs: 1	Virtual network: ASEVNET/ASEVNETsubNet
	RAM: 3.58 GB	

Disk			
OS disk			
Disk name: osld201221071831			
Storage type: Standard			
Size: 13 GB			
Data disks			
Disk name	LUN	Storage type	Size
No results.			

6. To clean up the resources that the script created, use the following commands:

```
Get-AzureRmVM | Remove-AzureRmVM -Force
Get-AzureRmNetworkInterface | Remove-AzureRmNetworkInterface -Force
Get-AzureRmImage | Remove-AzureRmImage -Force
Get-AzureRmDisk | Remove-AzureRmDisk -Force
Get-AzureRmStorageAccount | Remove-AzureRmStorageAccount -Force
```

Next steps

[Deploy VMs using Azure PowerShell cmdlets](#)

Deploy VMs on your Azure Stack Edge Pro GPU device using Azure CLI and Python

9/21/2022 • 11 minutes to read • [Edit Online](#)

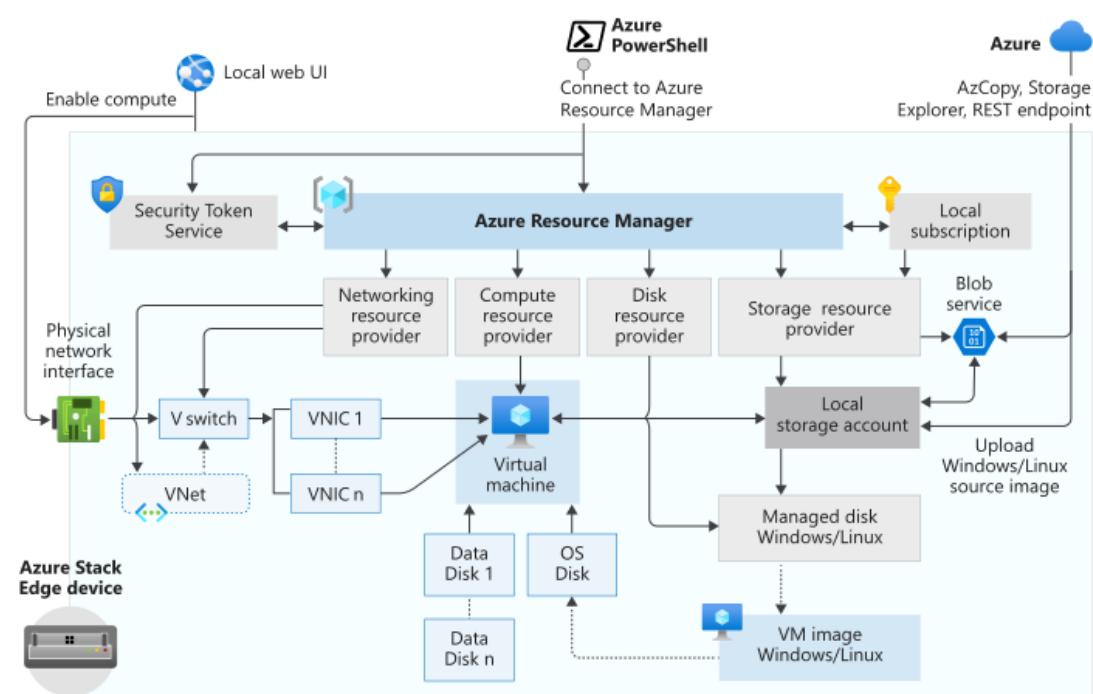
APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

You can create and manage virtual machines (VMs) on an Azure Stack Edge device using APIs. These APIs are standard Azure Resource Manager APIs called using the local Azure Stack Edge endpoint. The Azure Resource Manager APIs provide a consistent management layer that in this case enables you to create, update, and delete VMs in a local subscription that exists on the device. You can connect to the Azure Resource Manager running on Azure Stack Edge via Azure PowerShell cmdlets.

This tutorial describes how to create and manage a VM on your Azure Stack Edge Pro device using Python and the Azure API.

VM deployment workflow

The deployment workflow is illustrated in the following diagram.



The high-level summary of the deployment workflow is as follows:

1. Connect to Azure Resource Manager
2. Create a resource group
3. Create a storage account
4. Add blob URI to hosts file
5. Install certificates
6. Upload a VHD
7. Create managed disks from the VHD
8. Create a VM image from the image managed disk
9. Create VM with previously created resources
10. Create a VNet

11. Create a VNIC using the VNet subnet ID

For a detailed explanation of the workflow diagram, see [Deploy VMs on your Azure Stack Edge Pro device using Azure PowerShell](#). For information on how to connect to Azure Resource Manager, see [Connect to Azure Resource Manager using Azure PowerShell](#).

Prerequisites

Before you begin creating and managing a VM on your Azure Stack Edge Pro device using Azure CLI and Python, you need to make sure you have completed the prerequisites listed in the following steps:

1. You completed the network settings on your Azure Stack Edge Pro device as described in [Step 1: Configure Azure Stack Edge Pro device](#).
2. You enabled a network interface for compute. This network interface IP is used to create a virtual switch for the VM deployment. The following steps walk you through the process:
 - a. Go to **Compute**. Select the network interface that you will use to create a virtual switch.

IMPORTANT

You can only configure one port for compute.

- b. Enable compute on the network interface. Azure Stack Edge Pro creates and manages a virtual switch corresponding to that network interface.
3. You created and installed all the certificates on your Azure Stack Edge Pro device and in the trusted store of your client. Follow the procedure described in [Step 2: Create and install certificates](#).
4. You created a Base-64 encoded .cer certificate (PEM format) for your Azure Stack Edge Pro device. That certificate is already uploaded as signing chain on the device and installed in the trusted root store on your client. This certificate is also required in pem format for Python to work on this client.

Convert this certificate to `pem` format by using the `certutil` command. You must run this command in the directory that contains your certificate.

```
certutil.exe <SourceCertificateName.cer> <DestinationCertificateName.pem>
```

The following shows sample command usage:

```
PS C:\Certificates> certutil.exe -encode aze-root.cer aze-root.pem
Input Length = 2150
Output Length = 3014
CertUtil: -encode command completed successfully.
PS C:\Certificates>
```

You will also add this `pem` to the Python store later.

5. You assigned the device IP in your **Network** page in the local web UI of device. Add this IP to:

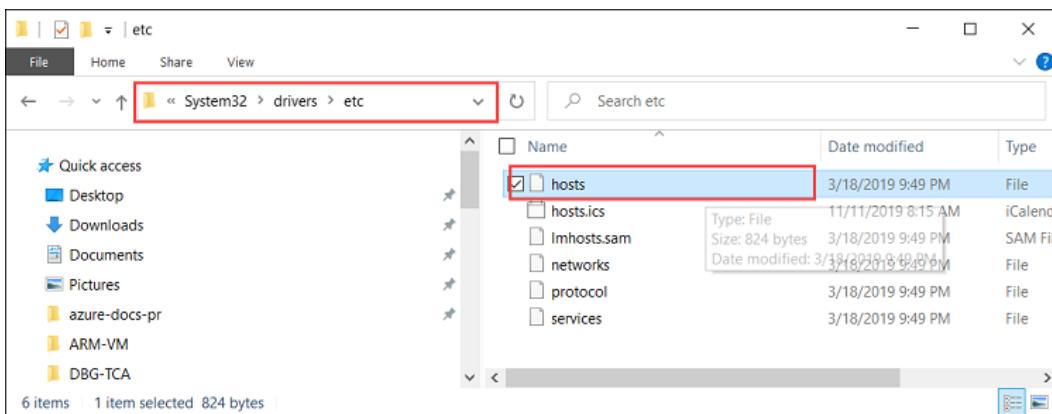
- The host file on the client, OR,
- The DNS server configuration

IMPORTANT

We recommend that you modify the DNS server configuration for endpoint name resolution.

- a. Start **Notepad** as an administrator (Administrator privileges is required to save the file), and then

open the hosts file located at `C:\Windows\System32\Drivers\etc`.



- b. Add the following entries to your hosts file replacing with appropriate values for your device:

```
<Device IP> login.<appliance name>.<DNS domain>
<Device IP> management.<appliance name>.<DNS domain>
<Device IP> <storage name>.blob.<appliance name>.<DNS domain>
```

- c. Use the following image for reference. Save the hosts file.

A screenshot of a Notepad window titled 'hosts - Notepad'. The window contains a sample HOSTS file with various comments and mappings. A red box highlights the last three lines, which are specific to Azure Resource Manager:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com          # source server
#      38.25.63.10      x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1            localhost
#
# Inserted for Azure Resource Manager
10.128.47.71      login.team3device.teatraining1.com
10.128.47.71      management.team3device.teatraining1.com
10.128.47.71      aseaccount.blob.team3device.teatraining1.com
```

6. Download the Python script used in this procedure.

7. Prepare your environment for the Azure CLI:

You can use either the Azure Cloud Shell or a local Azure CLI.

- [Azure Cloud Shell](#) with the Bash environment. Or launch the Cloud Shell here.

[Launch Cloud Shell](#)

- Local Azure CLI, see how to [install the Azure CLI](#). If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a](#)

Docker container.

- Sign in to the Azure CLI by using the [az login](#) command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
- When you first use Azure CLI, install the Azure CLI extension. For more information about extensions, see [Use extensions with the Azure CLI](#).
- Run [az version](#) to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#).

Step 1: Set up Azure CLI/Python on the client

Verify profile and install Azure CLI

1. Install Azure CLI on your client. In this example, Azure CLI 2.0.80 was installed. To verify the version of Azure CLI, run the [az --version](#) command.

The following is sample output from the above command:

```
PS C:\windows\system32> az --version
azure-cli          2.0.80

command-modules-nspkg    2.0.3
core                  2.0.80
nspkg                 3.0.4
telemetry              1.0.4
Extensions:
azure-cli-iot-ext      0.7.1

Python location 'C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2\python.exe'
Extensions directory 'C:\.azure\cliextensions'

Python (Windows) 3.6.6 (v3.6.6:4cf1f54eb7, Jun 27 2018, 02:47:15) [MSC v.1900 32 bit (Intel)]
Legal docs and information: aka.ms/AzureCliLegal

Your CLI is up-to-date.

Please let us know how we are doing: https://aka.ms/clihats
PS C:\windows\system32>
```

If you do not have Azure CLI, download and [Install Azure CLI on Windows](#). You can run Azure CLI using Windows command prompt or through Windows PowerShell.

2. Make a note of the CLI's Python location. You need the Python location to determine the location of the trusted root certificate store for Azure CLI.
3. To run the sample script used in this article, you will need the following Python library versions:

```
azure-common==1.1.23
azure-mgmt-resource==2.1.0
azure-mgmt-network==2.7.0
azure-mgmt-compute==5.0.0
azure-mgmt-storage==1.5.0
azure-storage-blob==1.2.0rc1
haikunator
msrestazure==0.6.2
```

To install the versions, run the following command:

```
.\python.exe -m pip install haikunator
```

The following sample output shows the installation of Haikunator:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> .\python.exe -m pip install haikunator

Collecting haikunator
  Downloading
    https://files.pythonhosted.org/packages/43/fa/130968f1a1bb1461c287b9ff35c630460801783243acda2cbf3a4c5
    964a5/haikunator-2.1.0-py2.py3-none-any.whl

Installing collected packages: haikunator
Successfully installed haikunator-2.1.0
You are using pip version 10.0.1, however version 20.0.1 is available.
You should consider upgrading using the 'python -m pip install --upgrade pip' command.

PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

The following sample output shows the installation of pip for `msrestazure`:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> .\python.exe -m pip install msrestazure==0.6.2
Requirement already satisfied: msrestazure==0.6.2 in c:\program files (x86)\microsoft
sdks\azure\cli2\lib\site-packages (0.6.2)
Requirement already satisfied: msrest<2.0.0,>=0.6.0 in c:\program files (x86)\microsoft
sdks\azure\cli2\lib\site-packages (from msrestazure==0.6.2) (0.6.10)
==== CUT ===== CUT =====
Requirement already satisfied: cffi!=1.11.3,>=1.8 in c:\program files (x86)\microsoft
sdks\azure\cli2\lib\site-packages (from cryptography>=1.1.0->adal<2.0.0,>=0.6.0->msrestazure==0.6.2)
(1.13.2)
Requirement already satisfied: pycparser in c:\program files (x86)\microsoft
sdks\azure\cli2\lib\site-packages (from cffi!=1.11.3,>=1.8->cryptography>=1.1.0->adal<2.0.0,>=0.6.0-
>msrestazure==0.6.2) (2.18)
You are using pip version 10.0.1, however version 20.0.1 is available.
You should consider upgrading using the 'python -m pip install --upgrade pip' command.
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

Trust the Azure Stack Edge Pro CA root certificate

- Find the certificate location on your machine. The location may vary depending on where you installed `az cli`. Run Windows PowerShell as administrator. Switch to the path where `az cli` installed Python:
`C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2\python.exe`.

To get the certificate location, type the following command:

```
.\python -c "import certifi; print(certifi.where())"
```

The cmdlet returns the certificate location, as seen below:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> .\python -c "import certifi;
print(certifi.where())"
C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2\lib\site-packages\certifi\cacert.pem
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

Make a note of this location as you will use it later -

```
C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2\lib\site-packages\certifi\cacert.pem
```

- Trust the Azure Stack Edge Pro CA root certificate by appending it to the existing Python certificate. You will provide the path to where you saved the PEM certificate earlier.

```
$pemFile = "<Path to the pem format certificate>"
```

An example path would be "C:\VM-scripts\rootteam3device.pem"

Then type the following series of commands into Windows PowerShell:

```
$root = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$root.Import($pemFile)

Write-Host "Extracting required information from the cert file"
$md5Hash    = (Get-FileHash -Path $pemFile -Algorithm MD5).Hash.ToLower()
$sha1Hash   = (Get-FileHash -Path $pemFile -Algorithm SHA1).Hash.ToLower()
$sha256Hash = (Get-FileHash -Path $pemFile -Algorithm SHA256).Hash.ToLower()

$issuerEntry  = [string]::Format("# Issuer: {0}", $root.Issuer)
$subjectEntry = [string]::Format("# Subject: {0}", $root.Subject)
$labelEntry   = [string]::Format("# Label: {0}", $root.Subject.Split('=')[-1])
$serialEntry  = [string]::Format("# Serial: {0}", $root.GetSerialNumberString().ToLower())
$md5Entry    = [string]::Format("# MD5 Fingerprint: {0}", $md5Hash)
$sha1Entry   = [string]::Format("# SHA1 Fingerprint: {0}", $sha1Hash)
$sha256Entry = [string]::Format("# SHA256 Fingerprint: {0}", $sha256Hash)
$certText = (Get-Content -Path $pemFile -Raw).ToString().Replace("`n",`n")

$rootCertEntry = "`n" + $issuerEntry + "`n" + $subjectEntry + "`n" + $labelEntry + "`n" +
$serialEntry + "`n" + $md5Entry + "`n" + $sha1Entry + "`n" + $sha256Entry + "`n" + $certText

Write-Host "Adding the certificate content to Python Cert store"
Add-Content "${env:ProgramFiles(x86)}\Microsoft SDKs\Azure\CLI2\Lib\site-packages\certifi\cacert.pem"
$rootCertEntry

Write-Host "Python Cert store was updated to allow the Azure Stack Edge Pro CA root certificate"
```

Connect to Azure Stack Edge Pro

1. Register your Azure Stack Edge Pro environment by running the [az cloud register](#) command.

In some scenarios, direct outbound internet connectivity is routed through a proxy or firewall, which enforces SSL interception. In these cases, the `az cloud register` command can fail with an error such as "Unable to get endpoints from the cloud." To work around this error, set the following environment variables in Windows PowerShell:

```
$ENV:AZURE_CLI_DISABLE_CONNECTION_VERIFICATION = 1
$ENV:ADAL_PYTHON_SSL_NO_VERIFY = 1
```

2. Set environment variables for the script for Azure Resource Manager endpoint, location where the resources are created and the path to where the source VHD is located. The location for the resources is fixed across all the Azure Stack Edge Pro devices and is set to `dbelocal`. You also need to specify the address prefixes and private IP address. All the following environment variables are values based on your values except for `AZURE_RESOURCE_LOCATION`, which should be hardcoded to `"dbelocal"`.

```
$ENV:ARM_ENDPOINT = "https://management.team3device.teatraining1.com"
$ENV:AZURE_RESOURCE_LOCATION = "dbelocal"
$ENV:VHD_FILE_PATH = "C:\Downloads\Ubuntu1604\Ubuntu13.vhd"
$ENV:ADDRESS_PREFIXES = "5.5.0.0/16"
$ENV:PRIVATE_IP_ADDRESS = "5.5.174.126"
```

3. Register your environment. Use the following parameters when running [az cloud register](#):

Value	Description	Example
Environment name	The name of the environment you are trying to connect to	Provide a name, for example, aze-environ
Resource Manager endpoint	This URL is <code>https://Management.<appliance name><dnsdomain></code> To get this URL, go to Devices page in the local web UI of your device.	For example, <code>https://management.team3device.teatraining1.co</code>

```
az cloud register -n <environmentname> --endpoint-resource-manager "https://management.<appliance name>.<DNS domain>"
```

The following shows sample usage of the above command:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> az cloud register -n az-new-env --endpoint-resource-manager "https://management.team3device.teatraining1.com"
```

4. Set the active environment by using the following command:

```
az cloud set -n <EnvironmentName>
```

The following shows sample usage of the above command:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> az cloud set -n az-new-env
Switched active cloud to 'az-new-env'.
Use 'az login' to log in to this cloud.
Use 'az account set' to set the active subscription.
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

5. Sign in to your Azure Stack Edge Pro environment by using the [az login](#) command. You can sign in to the Azure Stack Edge Pro environment either as a user or as a [service principal](#).

Follow these steps to sign in as a *user*:

You can either specify the username and password directly within the `az login` command, or authenticate by using a browser. You must do the latter if your account has multifactor authentication enabled.

The following shows sample usage of `az login`:

```
PS C:\Certificates> az login -u EdgeARMuser
```

After using the login command, you are prompted for a password. Provide the Azure Resource Manager password.

The following shows sample output for a successful sign-in after supplying the password:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> az login -u EdgeARMuser
Password:
[
  {
    "cloudName": "az-new-env",
    "id": "A4257FDE-B946-4E01-ADE7-674760B8D1A3",
    "isDefault": true,
    "name": "Default Provider Subscription",
    "state": "Enabled",
    "tenantId": "c0257de7-538f-415c-993a-1b87a031879d",
    "user": {
      "name": "EdgeArmUser@localhost",
      "type": "user"
    }
  }
]
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

Make a note of the `id` and `tenantId` values as these values correspond to your Azure Resource Manager Subscription ID and Azure Resource Manager Tenant ID respectively and will be used in the later step.

The following environment variables need to be set to work as *service principal*:

```
$ENV:ARM_TENANT_ID = "c0257de7-538f-415c-993a-1b87a031879d"
$ENV:ARM_CLIENT_ID = "cbd868c5-7207-431f-8d16-1cb144b50971"
$ENV:ARM_CLIENT_SECRET = "<Your Azure Resource Manager password>"
$ENV:ARM_SUBSCRIPTION_ID = "<Your subscription ID>"
```

Your Azure Resource Manager Client ID is hard-coded. Your Azure Resource Manager Tenant ID and Azure Resource Manager Subscription ID are both present in the output of the `az login` command you ran earlier. The Azure Resource Manager Client secret is the Azure Resource Manager password that you set.

For more information, see [Azure Resource Manager password](#).

6. Change the profile to version 2019-03-01-hybrid. To change the profile version, run the following command:

```
az cloud update --profile 2019-03-01-hybrid
```

The following shows sample usage of `az cloud update`:

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> az cloud update --profile 2019-03-01-hybrid
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

Step 2: Create a VM

A Python script is provided to you to create a VM. Depending on whether you are signed in as user or set as service principal, the script takes the input accordingly and creates a VM.

1. Run the Python script from the same directory where Python is installed.

```
.\python.exe example_dbe_arguments_name_https.py cli
```

2. When the script runs, uploading the VHD takes 20-30 minutes. To view the progress of the upload operation, you can use Azure Storage Explorer or AzCopy.

Here is a sample output of a successful run of the script. The script creates all the resources within a

resource group, uses those resources to create a VM, and finally deletes the resource group including all the resources it created.

```
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2> .\python.exe example_dbe_arguments_name_https.py
cli

Create Resource Group
Create a storage account
Uploading to Azure Stack Storage as blob:
    ubuntu13.vhd

Listing blobs...
    ubuntu13.vhd

VM image resource id:
    /subscriptions/.../resourceGroups/azure-sample-group-virtual-
machines118/providers/Microsoft.Compute/images/UbuntuImage

Create Vnet
Create Subnet
Create NIC
Creating Linux Virtual Machine
Tag Virtual Machine
Create (empty) managed Data Disk
Get Virtual Machine by Name
Attach Data Disk
Detach Data Disk
Deallocating the VM (to prepare for a disk resize)
Update OS disk size
Start VM
Restart VM
Stop VM

List VMs in subscription
    VM: VmName118

List VMs in resource group
    VM: VmName118

Delete VM
All example operations completed successfully!

Delete Resource Group
Deleted: azure-sample-group-virtual-machines118
PS C:\Program Files (x86)\Microsoft SDKs\Azure\CLI2>
```

Next steps

[Common Az CLI commands for Linux virtual machines](#)

Deploy Custom Script Extension on VMs running on your Azure Stack Edge Pro device

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

The Custom Script Extension downloads and runs scripts or commands on virtual machines running on your Azure Stack Edge Pro devices. This article details how to install and run the Custom Script Extension by using an Azure Resource Manager template.

About custom script extension

The Custom Script Extension is useful for post-deployment configuration, software installation, or any other configuration/management task. You can download scripts from Azure Storage or another accessible internet location, or you can provide scripts or commands to the extension runtime.

The Custom Script Extension integrates with Azure Resource Manager templates. You can also run it by using Azure CLI, PowerShell, or the Azure Virtual Machines REST API.

OS for Custom Script Extension

Supported OS for Custom Script Extension on Windows

The Custom Script Extension for Windows will run on the following OSs. Other versions may work but haven't been tested in-house on VMs running on Azure Stack Edge Pro devices.

DISTRIBUTION	VERSION
Windows Server 2019	Core
Windows Server 2016	Core

Supported OS for Custom Script Extension on Linux

The Custom Script Extension for Linux will run on the following OSs. Other versions may work but haven't been tested in-house on VMs running on Azure Stack Edge Pro devices.

DISTRIBUTION	VERSION
Linux: Ubuntu	18.04 LTS
Linux: Red Hat Enterprise Linux	7.4, 7.5, 7.7

Prerequisites

1. [Download the VM templates and parameters files](#) to your client machine. Unzip the download into a directory you'll use as a working directory.
2. You should have a VM created and deployed on your device. To create VMs, follow all the steps in [Deploy VM on your Azure Stack Edge Pro using templates](#).

If you need to download a script such as from GitHub or Azure Storage externally, while configuring compute network, enable the port that is connected to the Internet for compute. This allows you to download the script.

In the following example, Port 2 was connected to the internet and was used to enable the compute network. If you identified that Kubernetes isn't needed in the earlier step, you can skip the Kubernetes node IP and external service IP assignment.

Azure Stack Edge Pro (1 GPU)

Compute

myasegpuvm

Network settings (Port2)

Name Network

Port 1	192.168.100.0
Port 2	10.57.48.0
Port 3	192.168.0.0
Port 4	192.168.0.0
Port 5	192.168.0.0
Port 6	192.168.0.0

* Enable for compute
Yes No

Compute is enabled on this network interface.

Compute IPs
For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs
Enter a contiguous range of 2 static IPs for your device.
Enter static IPs: 10.1.1.1 - 10.1.1.2

Kubernetes external service IPs
Specify the static IP range for services exposed outside of Kubernetes cluster.
Enter static IPs: 10.1.1.5 - 10.1.1.10

< Back to Overview Next: Web proxy >

Apply

Install Custom Script Extension

Depending on the operating system for your VM, you could install Custom Script Extension for Windows or for Linux.

Custom Script Extension for Windows

To deploy Custom Script Extension for Windows for a VM running on your device, edit the

`addCSExtWindowsVM.parameters.json` parameters file and then deploy the template `addCSExtensiontoVM.json`.

Edit parameters file

The file `addCSExtWindowsVM.parameters.json` takes the following parameters:

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "value": "<Name of VM>"
        },
        "extensionName": {
            "value": "<Name of extension>"
        },
        "publisher": {
            "value": "Microsoft.Compute"
        },
        "type": {
            "value": "CustomScriptExtension"
        },
        "typeHandlerVersion": {
            "value": "1.10"
        },
        "settings": {
            "value": {
                "commandToExecute" : "<Command to execute>"
            }
        }
    }
}
```

Provide your VM name, name for the extension and the command that you want to execute.

Here's the sample parameter file that was used in this article.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "value": "VM5"
        },
        "extensionName": {
            "value": "CustomScriptExtension"
        },
        "publisher": {
            "value": "Microsoft.Compute"
        },
        "type": {
            "value": "CustomScriptExtension"
        },
        "typeHandlerVersion": {
            "value": "1.10"
        },
        "settings": {
            "value": {
                "commandToExecute" : "md C:\\\\Users\\\\Public\\\\Documents\\\\test"
            }
        }
    }
}
```

Deploy template

Deploy the template `addCSExtensiontoVM.json`. This template deploys extension to an existing VM. Run the following command:

```
$templateFile = "<Path to addCSExtensiontoVM.json file>"  
$templateParameterFile = "<Path to addCSExtWindowsVM.parameters.json file>"  
$RGName = "<Resource group name>"  
New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile $templateFile -  
TemplateParameterFile $templateParameterFile -Name "<Deployment name>"
```

NOTE

The extension deployment is a long running job and takes about 10 minutes to complete.

Here's a sample output:

```
PS C:\WINDOWS\system32> $templateFile = "C:\12-09-2020\ExtensionTemplates\addCSExtensiontoVM.json"  
PS C:\WINDOWS\system32> $templateParameterFile = "C:\12-09-  
2020\ExtensionTemplates\addCSExtWindowsVM.parameters.json"  
PS C:\WINDOWS\system32> $RGName = "myasegpuvm1"  
PS C:\WINDOWS\system32> New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile  
$templateFile -TemplateParameterFile $templateParameterFile -Name "deployment7"

DeploymentName      : deployment7
ResourceGroupName   : myasegpuvm1
ProvisioningState   : Succeeded
Timestamp          : 12/17/2020 10:07:44 PM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name          Type          Value
    ======      ======      =====
    vmName        String        VM5
    extensionName String        CustomScriptExtension
    publisher      String        Microsoft.Compute
    type          String        CustomScriptExtension
    typeHandlerVersion String        1.10
    settings      Object        {
        "commandToExecute": "md C:\\\\Users\\\\Public\\\\Documents\\\\test"
    }
Outputs            :
DeploymentLogLevel :
```

Track deployment

To check the deployment state of extensions for a given VM, run the following command:

```
Get-AzureRmVMExtension -ResourceGroupName <Name of resource group> -VMName <Name of VM> -Name <Name of the  
extension>
```

Here's a sample output:

```
PS C:\WINDOWS\system32> Get-AzureRmVMExtension -ResourceGroupName myasegpuvml -VMName VM5 -Name CustomScriptExtension

ResourceGroupName      : myasegpuvml
VMName                : VM5
Name                  : CustomScriptExtension
Location              : dbelocal
Etag                  : null
Publisher             : Microsoft.Compute
ExtensionType         : CustomScriptExtension
TypeHandlerVersion    : 1.10
Id                    : /subscriptions/947b3cf7-7a1b-4a90-7cc5-e52caf221332/resourceGroups/myasegpuvml/providers/Microsoft.Compute/virtualMachines/VM5/extensions/CustomScriptExtension
PublicSettings         :
  "commandToExecute": "md C:\\\\Users\\\\Public\\\\Documents\\\\test"
ProtectedSettings      :
ProvisioningState     : Creating
Statuses               :
SubStatuses            :
AutoUpgradeMinorVersion: True
ForceUpdateTag         :

PS C:\WINDOWS\system32>
```

NOTE

When the deployment is complete, the `ProvisioningState` changes to `Succeeded`.

Extension output is logged to files found under the following folder on the target virtual machine.

```
C:\WindowsAzure\Logs\Plugins\Microsoft.Compute.CustomScriptExtension
```

The specified files are downloaded into the following folder on the target virtual machine.

```
C:\Packages\Plugins\Microsoft.Compute.CustomScriptExtension\1.*\Downloads\<n>
```

where *n* is a decimal integer, which may change between executions of the extension. The 1.* value matches the actual, current `typeHandlerVersion` value of the extension. For example, the actual directory in this instance was `C:\Packages\Plugins\Microsoft.Compute.CustomScriptExtension\1.10.9\Downloads\0`.

In this instance, the command to execute for the custom extension was: `md C:\\\\Users\\\\Public\\\\Documents\\\\test`. When the extension is successfully installed, you can verify that the directory was created in the VM at the specified path in the command.

Custom Script Extension for Linux

To deploy Custom Script Extension for Windows for a VM running on your device, edit the `addCSExtLinuxVM.parameters.json` parameters file and then deploy the template `addCSExtensiontoVM.json`.

Edit parameters file

The file `addCSExtLinuxVM.parameters.json` takes the following parameters:

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "value": "<Name of your VM>"
        },
        "extensionName": {
            "value": "<Name of your extension>"
        },
        "publisher": {
            "value": "Microsoft.Azure.Extensions"
        },
        "type": {
            "value": "CustomScript"
        },
        "typeHandlerVersion": {
            "value": "2.0"
        },
        "settings": {
            "value": {
                "commandToExecute" : "<Command to execute>"
            }
        }
    }
}
```

Provide your VM name, name for the extension and the command that you want to execute.

Here's a sample parameter file that was used in this article:

```
$templateFile = "<Path to addCSExtensionToVM.json file>"
$templateParameterFile = "<Path to addCSExtLinuxVM.parameters.json file>"
$RGName = "<Resource group name>"
New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile $templateFile -
TemplateParameterFile $templateParameterFile -Name "<Deployment name>"
```

NOTE

The extension deployment is a long running job and takes about 10 minutes to complete.

Here's a sample output:

```

PS C:\WINDOWS\system32> $templateFile = "C:\12-09-2020\ExtensionTemplates\addCSExtensionToVM.json"
PS C:\WINDOWS\system32> $templateParameterFile = "C:\12-09-
2020\ExtensionTemplates\addCSExtLinuxVM.parameters.json"
PS C:\WINDOWS\system32> $RGName = "myasegpuvm1"
PS C:\WINDOWS\system32> New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile
$templateFile -TemplateParameterFile $templateParameterFile -Name "deployment99"

DeploymentName      : deployment99
ResourceGroupName   : myasegpuvm1
ProvisioningState   : Succeeded
Timestamp          : 12/18/2020 1:55:23 AM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name          Type          Value
    ======  ======  ======
    vmName        String        VM6
    extensionName String        LinuxCustomScriptExtension
    publisher      String        Microsoft.Azure.Extensions
    type          String        CustomScript
    typeHandlerVersion String        2.0
    settings      Object        {
        "commandToExecute": "sudo echo 'some text' >> /home/Administrator/file2.txt"
    }

Outputs            :
DeploymentLogLevel :

```

PS C:\WINDOWS\system32>

The `commandToExecute` was set to create a file `file2.txt` in the `/home/Administrator` directory and the contents of the file are `some text`. In this case, you can verify that the file was created in the specified path.

```

Administrator@VM6:~$ dir
file2.txt
Administrator@VM6:~$ cat file2.txt
some text
Administrator@VM6:

```

Track deployment status

Template deployment is a long running job. To check the deployment state of extensions for a given VM, open another PowerShell session (run as administrator). Run the following command:

```
Get-AzureRmVMExtension -ResourceGroupName myResourceGroup -VMName <VM Name> -Name <Extension Name>
```

Here's a sample output:

```
PS C:\WINDOWS\system32> Get-AzureRmVMExtension -ResourceGroupName myasegpuvml -VMName VM5 -Name CustomScriptExtension

ResourceGroupName      : myasegpuvml
VMName                : VM5
Name                  : CustomScriptExtension
Location              : dbelocal
Etag                  : null
Publisher             : Microsoft.Compute
ExtensionType         : CustomScriptExtension
TypeHandlerVersion    : 1.10
Id                   : /subscriptions/947b3cf8-7a1b-4a90-7cc5-e52caf221332/resourceGroups/myasegpuvml/providers/Microsoft.Compute/virtualMachines/VM5/extensions/CustomScriptExtension
PublicSettings        : {
                           "commandToExecute": "md C:\\\\Users\\\\Public\\\\Documents\\\\test"
                         }
ProtectedSettings     :
ProvisioningState     : Creating
Statuses              :
SubStatuses           :
AutoUpgradeMinorVersion : True
ForceUpdateTag        :

PS C:\WINDOWS\system32>
```

NOTE

When the deployment is complete, the `ProvisioningState` changes to `Succeeded`.

The extension execution output is logged to the following file: `/var/lib/waagent/custom-script/download/0/`.

Remove Custom Script Extension

To remove the Custom Script Extension, use the following command:

```
Remove-AzureRmVMExtension -ResourceGroupName <Resource group name> -VMName <VM name> -Name <Extension name>
```

Here's a sample output:

```
PS C:\WINDOWS\system32> Remove-AzureRmVMExtension -ResourceGroupName myasegpuvml -VMName VM6 -Name LinuxCustomScriptExtension
Virtual machine extension removal operation
This cmdlet will remove the specified virtual machine extension. Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Yes
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
----- -----
True          OK  OK
```

Next steps

[Azure Resource Manager cmdlets](#)

Install GPU extension on VMs for your Azure Stack Edge Pro GPU device

9/21/2022 • 10 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

This article describes how to install GPU driver extension to install appropriate Nvidia drivers on the GPU VMs running on your Azure Stack Edge device. The article covers installation steps for installing a GPU extension using Azure Resource Manager templates on both Windows and Linux VMs.

NOTE

- In the Azure portal, you can install a GPU extension during VM creation or after the VM is deployed. For steps and requirements, see [Deploy GPU virtual machines](#).
- If you're running a Windows 2016 VHD, you must enable TLS 1.2 inside the VM before you install the GPU extension on 2205 and higher. For detailed steps, see [Troubleshoot GPU extension issues for GPU VMs on Azure Stack Edge Pro GPU](#).

Prerequisites

Before you install GPU extension on the GPU VMs running on your device, make sure that:

- You have access to an Azure Stack Edge device on which you've deployed one or more GPU VMs. See how to [Deploy a GPU VM on your device](#).

- Make sure that the port enabled for compute network on your device is connected to Internet and has access. The GPU drivers are downloaded through the internet access.

Here's an example where Port 2 was connected to the internet and was used to enable the compute network. If Kubernetes isn't deployed on your environment, you can skip the Kubernetes node IP and external service IP assignment.

The screenshot shows the Azure Stack Edge Pro (1 GPU) interface. On the left, a sidebar lists various configuration options like Overview, Get started, Network, Compute (which is selected and highlighted with a red box), Web proxy, Device, Update server, Time, Certificates, and Cloud details. Below that is a Maintenance section with Power, Hardware health, Software update, Password change, and Device reset. At the bottom is a Troubleshooting section. The main content area is titled "Compute" and shows a table of network interfaces. The second row, "Port 2", is highlighted with a red box. To the right of the table is a "Network settings (Port2)" panel. It contains a section for "Compute" with a "Enable for compute" switch set to "Yes". Below it is a "Compute IPs" section with a table for "Kubernetes node IPs" and "Kubernetes external service IPs", both currently empty. A large "Apply" button is at the bottom of the panel.

2. Download the GPU extension templates and parameters files to your client machine. Unzip it into a directory you'll use as a working directory.
3. Verify that the client you'll use to access your device is still connected to the Azure Resource Manager over Azure PowerShell. The connection to Azure Resource Manager expires every 1.5 hours or if your Azure Stack Edge device restarts. If this happens, any cmdlets that you execute will return error messages to the effect that you aren't connected to Azure anymore. You'll need to sign in again. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

Edit parameters file

Depending on the operating system for your VM, you could install GPU extension for Windows or for Linux.

- [Windows](#)
- [Linux](#)

To deploy Nvidia GPU drivers for an existing VM, edit the `addGPUExtWindowsVM.parameters.json` parameters file and then deploy the template `addGPUextensiontoVM.json`.

Version 2205 and higher

The file `addGPUExtWindowsVM.parameters.json` takes the following parameters:

```
"parameters": {  
    "vmName": {  
        "value": "<name of the VM>"  
    },  
    "extensionName": {  
        "value": "<name for the extension. Example: windowsGpu>"  
    },  
    "publisher": {  
        "value": "Microsoft.HpcCompute"  
    },  
    "type": {  
        "value": "NvidiaGpuDriverWindows"  
    },  
    "typeHandlerVersion": {  
        "value": "1.5"  
    },  
    "settings": {  
        "value": {  
            "DriverURL" : "http://us.download.nvidia.com/tesla/511.65/511.65-data-center-tesla-desktop-winserver-2016-2019-2022-dch-international.exe",  
            "DriverCertificateUrl" : "https://go.microsoft.com/fwlink/?linkid=871664",  
            "DriverType": "CUDA"  
        }  
    }  
}
```

Versions lower than 2205

The file `addGPUExtWindowsVM.parameters.json` takes the following parameters:

```
"parameters": {
  "vmName": {
    "value": "<name of the VM>"
  },
  "extensionName": {
    "value": "<name for the extension. Example: windowsGpu>"
  },
  "publisher": {
    "value": "Microsoft.HpcCompute"
  },
  "type": {
    "value": "NvidiaGpuDriverWindows"
  },
  "typeHandlerVersion": {
    "value": "1.3"
  },
  "settings": {
    "value": {
      "DriverURL" : "http://us.download.nvidia.com/tesla/442.50/442.50-tesla-desktop-winserver-2019-2016-international.exe",
      "DriverCertificateUrl" : "https://go.microsoft.com/fwlink/?linkid=871664",
      "DriverType": "CUDA"
    }
  }
}
```

Deploy template

- [Windows](#)
- [Linux](#)

Deploy the template `addGPUextensiontoVM.json` to install the extension on an existing VM.

Run the following command:

```
$templateFile = "<Path to addGPUextensiontoVM.json>"
$templateParameterFile = "<Path to addGPUExtWindowsVM.parameters.json>"
RGName = "<Name of your resource group>"
New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile $templateFile -
TemplateParameterFile $templateParameterFile -Name "<Name for your deployment>"
```

NOTE

The extension deployment is a long running job and takes about 10 minutes to complete.

Here's a sample output:

```

PS C:\WINDOWS\system32> "C:\12-09-2020\ExtensionTemplates\addGPUextensiontoVM.json"
C:\12-09-2020\ExtensionTemplates\addGPUextensiontoVM.json
PS C:\WINDOWS\system32> $templateFile = "C:\12-09-2020\ExtensionTemplates\addGPUextensiontoVM.json"
PS C:\WINDOWS\system32> $templateParameterFile = "C:\12-09-
2020\ExtensionTemplates\addGPUExtWindowsVM.parameters.json"
PS C:\WINDOWS\system32> $RGName = "myasegpuvm1"
PS C:\WINDOWS\system32> New-AzureRmResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile
$templateFile -TemplateParameterFile $templateParameterFile -Name "deployment3"

DeploymentName      : deployment3
ResourceGroupName   : myasegpuvm1
ProvisioningState   : Succeeded
Timestamp          : 12/16/2020 12:18:50 AM
Mode                : Incremental
TemplateLink        :
Parameters          :
    Name          Type          Value
    ======      ======      =====
    vmName        String        VM2
    extensionName String        windowsgpuext
    publisher      String        Microsoft.HpcCompute
    type          String        NvidiaGpuDriverWindows
    typeHandlerVersion String        1.3
    settings      Object        {
        "DriverURL": "http://us.download.nvidia.com/tesla/442.50/442.50-tesla-desktop-
winserver-2019-2016-international.exe",
        "DriverCertificateUrl": "https://go.microsoft.com/fwlink/?linkid=871664",
        "DriverType": "CUDA"
    }
Outputs            :
DeploymentLogLevel :
PS C:\WINDOWS\system32>

```

Track deployment

- [Windows](#)
- [Linux](#)

To check the deployment state of extensions for a given VM, open another PowerShell session (run as administrator), and then run the following command:

```
Get-AzureRmVMExtension -ResourceGroupName <Name of resource group> -VMName <Name of VM> -Name <Name of the
extension>
```

Here's a sample output:

```

PS C:\WINDOWS\system32> Get-AzureRmVMExtension -ResourceGroupName myasegpuvm1 -VMName VM2 -Name
windowsgpuext

ResourceGroupName      : myasegpuvm1
VMName                : VM2
Name                  : windowsgpuext
Location              : dbelocal
Etag                  : null
Publisher             : Microsoft.HpcCompute
ExtensionType         : NvidiaGpuDriverWindows
TypeHandlerVersion    : 1.3
Id                   : /subscriptions/947b3cf8-7a1b-4a90-7cc5-
e52caf221332/resourceGroups/myasegpuvm1/providers/Microsoft.Compute/virtualMachines/VM2/extensions/windowsgp
uext
PublicSettings        :
  "DriverURL": "http://us.download.nvidia.com/tesla/442.50/442.50-tesla-desktop-
winserver-2019-2016-international.exe",
  "DriverCertificateUrl": "https://go.microsoft.com/fwlink/?linkid=871664",
  "DriverType": "CUDA"
ProtectedSettings      :
ProvisioningState     : Creating
Statuses              :
SubStatuses            :
AutoUpgradeMinorVersion : True
ForceUpdateTag         :

PS C:\WINDOWS\system32>

```

Extension execution output is logged to the following file. Refer to this file

`C:\Packages\Plugins\Microsoft.HpcCompute.NvidiaGpuDriverWindows\1.3.0.0>Status` to track the status of installation.

A successful install is indicated by a `message` as `Enable Extension` and `status` as `success`.

```

"status": {
    "formattedMessage": {
        "message": "Enable Extension",
        "lang": "en"
    },
    "name": "NvidiaGpuDriverWindows",
    "status": "success",
}

```

Verify driver installation

- [Windows](#)
- [Linux](#)

Sign in to the VM and run the `nvidia-smi` command-line utility installed with the driver.

Version 2205 and higher

The `nvidia-smi.exe` is located at `c:\Windows\System32\nvidia-smi.exe`. If you don't see the file, it's possible that the driver installation is still running in the background. Wait for 10 minutes and check again.

Versions lower than 2205

The `nvidia-smi.exe` is located at `c:\Program Files\NVIDIA Corporation\NVSMI\nvidia-smi.exe`. If you don't see the file, it's possible that the driver installation is still running in the background. Wait for 10 minutes and check again.

If the driver is installed, you see an output similar to the following sample:

```

PS C:\Users\Administrator> cd "C:\Program Files\NVIDIA Corporation\NVSMI"
PS C:\Program Files\NVIDIA Corporation\NVSMI> ls

    Directory: C:\Program Files\NVIDIA Corporation\NVSMI

Mode                LastWriteTime         Length Name
----                -----          -----
-a----        2/26/2020 12:00 PM      849640 MCU.exe
-a----        2/26/2020 12:00 PM     443104 nvdebugdump.exe
-a----        2/25/2020 2:06 AM      81823 nvidia-smi.1.pdf
-a----        2/26/2020 12:01 PM     566880 nvidia-smi.exe
-a----        2/26/2020 12:01 PM     991344 nvml.dll

PS C:\Program Files\NVIDIA Corporation\NVSMI> .\nvidia-smi.exe
Wed Dec 16 00:35:51 2020
+-----+
| NVIDIA-SMI 442.50      Driver Version: 442.50      CUDA Version: 10.2      |
|-----+-----+-----+
| GPU  Name        TCC/WDDM | Bus-Id      Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
|-----+-----+-----+-----+
|  0  Tesla T4        TCC | 0000503C:00:00.0 Off |          0 |
| N/A   35C   P8    11W /  70W |      8MiB / 15205MiB |      0%     Default |
+-----+-----+-----+
+-----+
| Processes:                               GPU Memory |
| GPU     PID  Type  Process name          Usage      |
|-----+-----+-----+-----|
| No running processes found               |
+-----+
PS C:\Program Files\NVIDIA Corporation\NVSMI>

```

For more information, see [Nvidia GPU driver extension for Windows](#).

NOTE

After you finish installing the GPU driver and GPU extension, you no longer need to use a port with Internet access for compute.

Remove GPU extension

To remove the GPU extension, use the following command:

```
Remove-AzureRmVMExtension -ResourceGroupName <Resource group name> -VMName <VM name> -Name <Extension name>
```

Here's a sample output:

```

PS C:\azure-stack-edge-deploy-vms> Remove-AzureRmVMExtension -ResourceGroupName rgl -VMName WindowsVM -Name
windowsgpuext
Virtual machine extension removal operation
This cmdlet will remove the specified virtual machine extension. Do you want to continue? [Y] Yes [N] No [S]
Suspend [?] Help (default is "Y"): y
RequestId IsSuccessStatusCode StatusCode ReasonPhrase
-----
True          OK          OK

```

Next steps

Learn how to:

- Troubleshoot GPU extension issues.
- Monitor VM activity on your device.
- Manage VM disks.
- Manage VM network interfaces.
- Manage VM sizes.

Install the password reset extension on VMs for your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article covers steps to install, verify, and remove the password reset extension using Azure Resource Manager templates on both Windows and Linux VMs.

Prerequisites

Before you install the password reset extension on the VMs running on your device:

1. Make sure to have access to an Azure Stack Edge device on which you've deployed one or more VMs. For more information, see [Deploy VMs on your Azure Stack Edge Pro GPU device via the Azure portal](#).

Here's an example where Port 2 was used to enable the compute network. If Kubernetes isn't deployed on your environment, you can skip the Kubernetes node IP and external service IP assignment.

The screenshot shows the Azure Stack Edge Pro (1 GPU) interface with the 'Advanced networking' section selected. On the left, there's a navigation menu with sections like Overview, Configuration (Get started, Network, Advanced networking), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting. The 'Advanced networking' section is expanded, showing a 'Virtual switch' table with one entry: Name 'vswitch1' and Network interface 'Port 2'. Below this is a 'Virtual network' table with one entry: Name 'Vnet1', Virtual switch 'vswitch1', VLAN ID '200', and Network 'Network IP address'. To the right, there's a 'Network settings (vswitch1)' panel. It has a dropdown for 'Intent' set to 'compute', which is highlighted with a red box. Below it, it says 'Compute is enabled on this network interface'. Under 'Compute IPs', there's a text input field containing '10.10.10.1-10.10.10.2'. Under 'Kubernetes external service IPs', there's a text input field containing '10.10.10.1-10.10.10.2'. At the bottom right of the panel is a blue 'Apply' button.

2. [Download the templates](#) to your client machine. Unzip the files into a directory you'll use as a working directory.
3. Verify that the client you'll use to access your device is connected to the local Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

The connection to Azure Resource Manager expires every 1.5 hours or if your Azure Stack Edge device restarts. If your connection expires, any cmdlets that you execute will return error messages to the effect that you aren't connected to Azure. In this case, sign in again.

Edit parameters file

Depending on the operating system for your VM, you can install the extension for Windows or for Linux. You'll find the parameter and template files in the *PasswordResetExtension* folder.

- [Windows](#)
- [Linux](#)

To change the password for an existing VM, edit the `addPasswordResetExtensionTemplate.parameters.json` parameters file and then deploy the template `addPasswordResetExtensionTemplate.json`.

The file `addPasswordResetExtensionTemplate.parameters.json` takes the following parameters:

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",  
    "contentVersion": "1.0.0.0",  
    "parameters": {  
        "vmName": {  
            "value": "<Name of the VM>"  
        },  
        "extensionType": {  
            "value": "<OS type of the VM, for example, Linux or Windows>"  
        },  
        "username": {  
            "value": "<Existing username for connecting to your VM>"  
        },  
        "Password": {  
            "value": "<New password for the user>"  
        }  
    }  
}
```

Deploy template

- [Windows](#)
- [Linux](#)

Set some parameters. Run the following command:

```
$templateFile = "<Path to addPasswordResetExtensionTemplate.json file>"  
$templateParameterFile = "<Path to addPasswordResetExtensionTemplate.parameters.json file>"  
$RGName = "<Name of resource group>"  
New-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile $templateFile -TemplateParameterFile  
$templateParameterFile -Name "<Deployment name>" -AsJob
```

The extension deployment is a long running job and takes about 10 minutes to complete.

Here's a sample output:

```

PS C:\WINDOWS\system32> $templateFile =
"C:\PasswordResetVmExtensionTemplates\addPasswordResetExtensionTemplate.json"
PS C:\WINDOWS\system32> $templateParameterFile =
"C:\PasswordResetVmExtensionTemplates\addPasswordResetExtensionTemplate.parameters.json"
PS C:\WINDOWS\system32> $RGName = "myasepro2rg"
PS C:\WINDOWS\system32> New-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile $templateFile
-TemplateParameterFile $templateParameterFile -Name "windowsvmdeploy" -AsJob
Id      Name          PSJobTypeName   State       HasMoreData  Location        Command
--      --           -----          ----       -----       -----          -----
9      Long Running... AzureLongRun... Running     True        localhost    New-
AzResourceGro...
PS C:\WINDOWS\system32>

```

Track deployment

- [Windows](#)
- [Linux](#)

To check the deployment status of extensions for a given VM, run the following command:

```
Get-AzVMExtension -ResourceGroupName <MyResourceGroup> -VMName <MyWindowsVM> -Name <Name of the extension>
```

Here's a sample output:

```

PS C:\WINDOWS\system32>
Get-AzVMExtension -ResourceGroupName myasepro2rg -VMName mywindowsvm -Name windowsVMAccessExt

ResourceGroupName      : myasepro2rg
VMName                : mywindowsvm
Name                  : windowsVMAccessExt
Location              : dbelocal
Etag                  : null
Publisher             : Microsoft.Compute
ExtensionType         : VMAccessAgent
TypeHandlerVersion    : 2.4
Id                   : /subscriptions/04a485ed-7a09-44ab-6671-
66db7f111122/resourceGroups/myasepro2rg/providers/Microsoft.Compute/virtualMachines/mywindowsvm/extensions/windowsVMAccessExt
PublicSettings         : {
                           "username": "azureuser"
                         }
ProtectedSettings      :
ProvisioningState     : Succeeded
Statuses              :
SubStatuses           :
AutoUpgradeMinorVersion : True
ForceUpdateTag        :

PS C:\WINDOWS\system32>

```

You can see below that the extension has been installed successfully.

Home > myasepro2single > Virtual machines >

mywindowsvm

Virtual machine

Start | Restart | Stop | Delete | Add extension | Refresh

Details Metrics

Virtual machine		Size	Installed extensions	
Computer name	mywindowsvm	Vm Size (Change) D1_v2	Name windowsVMAccessExt	Status Succeeded
Image name	windowsvhd	Offering Standard		
Operating system	Windows	vCPUs 1		
Status	Running	RAM 3.58 GB		

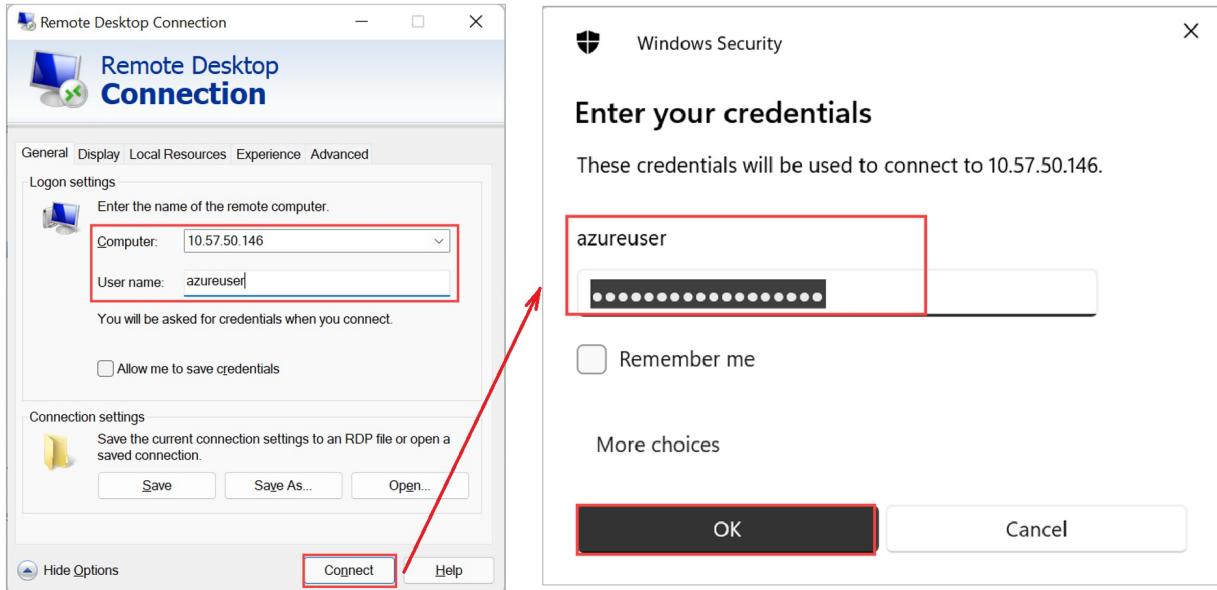
Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group
mywindowsvmnic (primary)	10.10.10.10	vswitch1	vswitch1subNet	Dynamic	MYASEPRO2RG

Verify the updated VM password

- Windows
- Linux

To verify the VM password update, connect to the VM using the new password. For detailed instructions, see [Connect to a Windows VM](#).



Remove the extension

- Windows
- Linux

To remove the password reset extension, run the following command:

```
Remove-AzVMExtension -ResourceGroupName <Resource group name> -VMName <VM name> -Name <Name of the extension>
```

Here's a sample output:

```
PS C:\WINDOWS\system32> Remove-AzVMExtension -ResourceGroupName myasepro2rg -VMName mywindowsvm5 -Name windowsVMAccessExt

Virtual machine extension removal operation
This cmdlet will remove the specified virtual machine extension. Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Yes

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
----- -----
True OK OK

PS C:\WINDOWS\system32>
```

Next steps

Learn how to:

- [Monitor VM activity on your device](#)
- [Manage VM disks](#)
- [Manage VM network interfaces](#)
- [Manage VM sizes](#)

Use the Azure portal to manage network interfaces on the VMs on your Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

You can create and manage virtual machines (VMs) on an Azure Stack Edge device using Azure portal, templates, Azure PowerShell cmdlets and via Azure CLI/Python scripts. This article describes how to manage the network interfaces on a VM running on your Azure Stack Edge device using the Azure portal.

When you create a VM, you specify one virtual network interface to be created. You may want to add one or more network interfaces to the virtual machine after it is created. You may also want to change the default network interface settings for an existing network interface.

This article explains how to add a network interface to an existing VM, change existing settings such as IP type (static vs. dynamic), and detach or delete an existing interface.

About network interfaces on VMs

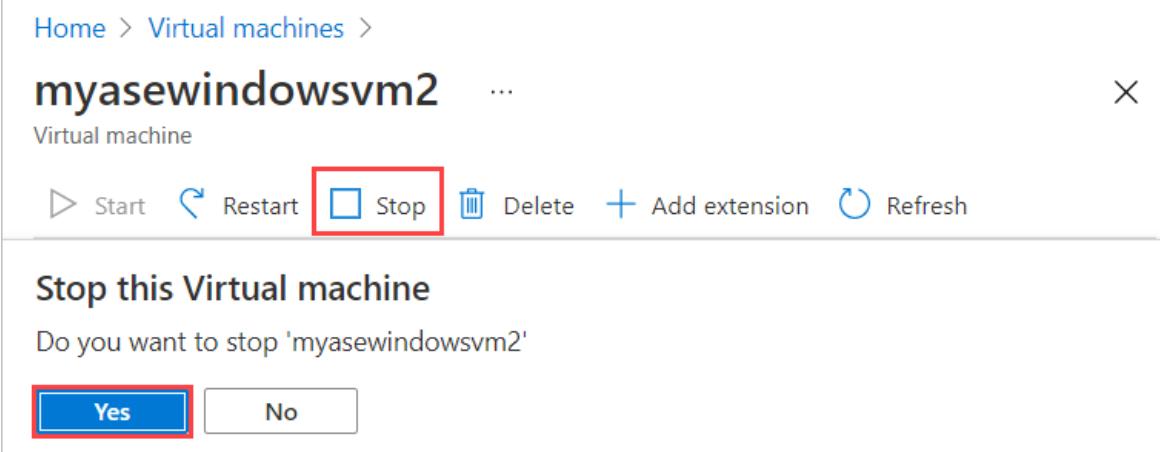
A network interface enables a virtual machine (VM) running on your Azure Stack Edge Pro device to communicate with Azure and on-premises resources. When you enable a port for compute network on your device, a virtual switch is created on that network interface. This virtual switch is then used to deploy compute workloads such as VMs or containerized applications on your device.

Multiple network interfaces can be associated with one virtual switch. Each network interface on your VM has a static or a dynamic IP address assigned to it. With IP addresses assigned to multiple network interfaces on your VM, certain capabilities are enabled on your VM. For example, your VM can host multiple websites or services with different IP addresses and SSL certificates on a single server. A VM on your device can serve as a network virtual appliance, such as a firewall or a load balancer.

Prerequisites

Before you begin to manage VMs on your device via the Azure portal, make sure that:

1. You've access to an activated Azure Stack Edge Pro GPU device. You have enabled a network interface for compute on your device. This action creates a virtual switch on that network interface on your VM.
 - a. In the local UI of your device, go to **Compute**. Select the network interface that you will use to create a virtual switch.
 - b. Enable compute on the network interface. Azure Stack Edge Pro GPU creates and manages a virtual switch corresponding to that network interface.
2. You have at least one VM deployed on your device. To create this VM, see the instructions in [Deploy VM on your Azure Stack Edge Pro via the Azure portal](#).
3. Your VM should be in **Stopped** state. To stop your VM, go to **Virtual machines** and select the VM you want to stop. In the VM Details page, select **Stop** and then select **Yes** when prompted for confirmation. Before you add, edit, or delete network interfaces, you must stop the VM.



Add a network interface

Follow these steps to add a network interface to a virtual machine deployed on your device.

1. Go to the virtual machine that you have stopped, and select **Networking**.

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group
guestnetwork	10.126.77.185	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG
myasewindowsvm2nic (primary)	10.126.76.208	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG

2. In the **Networking** blade, from the command bar, select **+ Add network interface**.

3. In the **Add network interface** blade, enter the following parameters:

FIELD	DESCRIPTION
Name	A unique name within the edge resource group. The name cannot be changed after the network interface is created. To manage multiple network interfaces easily, use the suggestions provided in the Naming conventions .
Select an edge resource group	Select the edge resource group to add the network interface to.

FIELD	DESCRIPTION
Virtual network	The virtual network associated with the virtual switch created on your device when you enabled compute on the network interface. There is only one virtual network associated with your device.
Subnet	A subnet within the selected virtual network. This field is automatically populated with the subnet associated with the network interface on which you enabled compute.
IP address assignment	A static or a dynamic IP for your network interface. The static IP should be an available, free IP from the specified subnet range. Choose dynamic if a DHCP server exists in the environment.

Add network interface

Create and attach a network interface to a virtual machine (VM). A network interface lets a VM communicate with the internet, Azure, and on-premises resources.

[Learn more about network interface](#)

Name *

Select an edge resource group * ⓘ

Virtual network * ⓘ

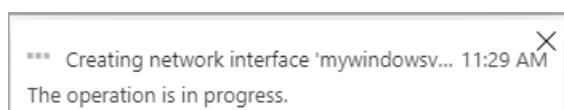
Subnet * ⓘ

IP address assignment * ⓘ

Dynamic
 Static

Add
Close

4. You'll see a notification that the network interface creation is in progress.



5. After the network interface is successfully created, the list of network interfaces refreshes to display the newly created interface.

Networking						X
Add network interface		Refresh				
Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource gro...	
guestnetwork	10.126.77.185	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG	
myasewindowsvm2nic (primary)	10.126.76.208	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG	

Edit a network interface

Follow these steps to edit a network interface associated with a virtual machine deployed on your device.

1. Go to the virtual machine that you have stopped, and select **Networking** in the virtual machine **Details**.
2. In the list of network interfaces, select the interface that you wish to edit. In the far right of the network interface selected, select the edit icon (pencil).

Networking						X
Add network interface		Refresh				
Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource gro...	
guestnetwork	10.126.77.185	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG	
myasewindowsvm2nic (primary)	10.126.76.208	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG	

3. In the **Edit network interface** blade, you can only change the IP assignment of the network interface. The name, edge resource group, virtual network, and subnet associated with the network interface can't be changed once it is created. Change the **IP assignment** to static, and save the changes.

Edit network interface

X

Create and attach a network interface to a virtual machine (VM). A network interface lets a VM communicate with the internet, Azure, and on-premises resources.

[Learn more about network interface](#)

Name

guestnetwork

Select an edge resource group ⓘ

myaserg

Virtual network ⓘ

ASEVNET

Subnet ⓘ

ASEVNETsubNet (10.126.72.0/21)

IP address assignment * ⓘ

- Dynamic
 Static

Specify IP address

example: 172.21.1.11

Save

Close

4. The list of network interface refreshes to display the updated network interface.

Detach a network interface

Follow these steps to detach or remove a network interface associated with a virtual machine deployed on your device.

1. Go to the virtual machine that you have stopped, and select **Networking** in the virtual machine **Details**.
2. In the list of network interfaces, select the interface that you wish to edit. In the far right of the network interface selected, select the detach icon (unplug).

Networking					
Add network interface		Select an edge resource group			
Network interface	IP Address	Virtual network	Subnet	IP allocation method	
guestnetwork	10.126.77.185	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG
myasewindowsvm2nic (primary)	10.126.76.208	ASEVNET	ASEVNETsubNet	Dynamic	MYASERG

3. You'll see a message asking you to confirm that you want to detach the network interface. Select **Yes**.

Detach the network interface

Are you sure you want to detach the network interface?

Yes

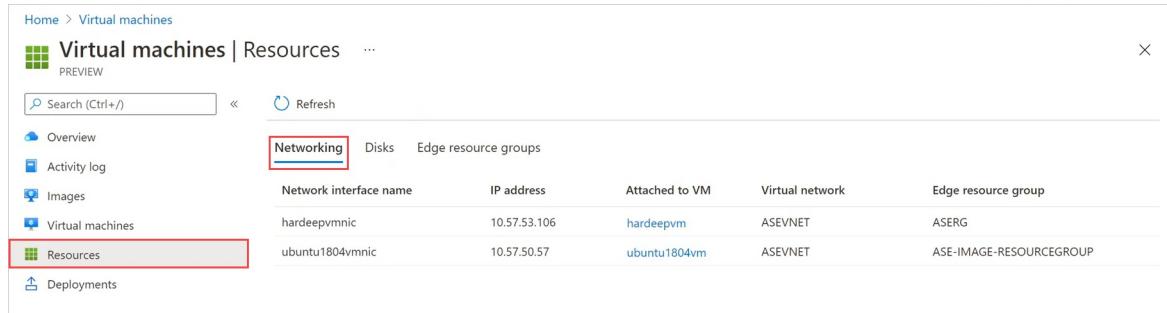
No

After the interface is completely detached, the list of network interfaces is refreshed to display the remaining interfaces.

Delete a network interface

Follow these steps to delete a network interface that isn't attached to a virtual machine.

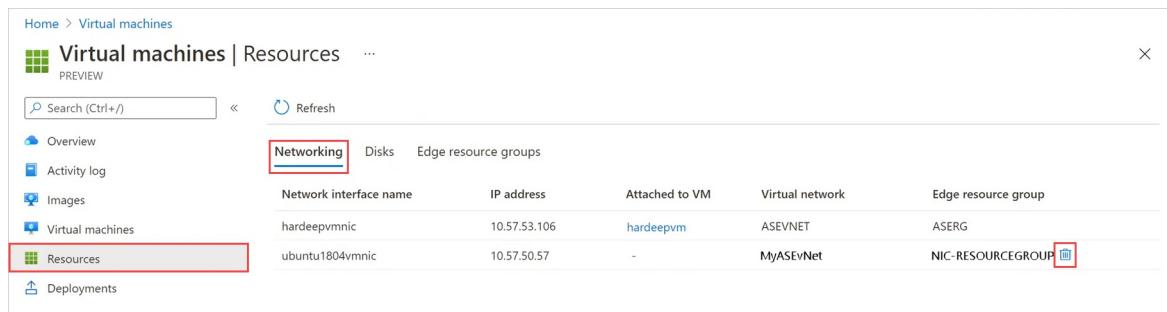
1. Go to **Virtual machines**, and then to the **Resources** page. Select **Networking**.



The screenshot shows the Azure portal's "Virtual machines | Resources" page. The "Networking" tab is active. In the left sidebar, the "Resources" link is highlighted with a red box. The main table lists two network interfaces:

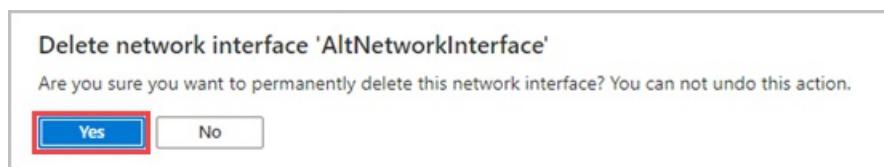
Network interface name	IP address	Attached to VM	Virtual network	Edge resource group
hardeepvmnic	10.57.53.106	hardeepvpm	ASEVNET	ASERG
ubuntu1804vmnic	10.57.50.57	ubuntu1804vm	ASEVNET	ASE-IMAGE-RESOURCEGROUP

2. On the **Networking** blade, select the delete icon (trashcan) by the network interface you want to delete. The delete icon is only displayed for network interfaces that aren't attached to a VM.



The screenshot shows the same "Virtual machines | Resources" page as before, but now the delete icon (trashcan) next to the second network interface, "ubuntu1804vmnic", is highlighted with a red box.

3. You'll see a message asking you to confirm that you want to delete the network interface. The operation can't be reversed. Select **Yes**.



The screenshot shows a confirmation dialog box with the title "Delete network interface 'AltNetworkInterface'". The message inside reads: "Are you sure you want to permanently delete this network interface? You can not undo this action." There are "Yes" and "No" buttons at the bottom.

After deletion of the network interface completes, the network interface is removed from the list.

Next steps

To learn how to deploy virtual machines on your Azure Stack Edge Pro device, see [Deploy virtual machines via the Azure portal](#).

Use the Azure portal to manage disks on the VMs on your Azure Stack Edge Pro GPU

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

You can provision disks on the virtual machines (VMs) deployed on your Azure Stack Edge Pro device using the Azure portal. The disks are provisioned on the device via the local Azure Resource Manager and consume the device capacity. The operations such as adding, detaching, and deleting a disk can be done via the Azure portal, which in turn makes calls to the local Azure Resource Manager to provision the storage.

This article explains how to add, detach or remove, and delete data disks from an existing VM, and resize the VM itself via, the Azure portal.

About disks on VMs

Your VM can have an OS disk and a data disk. Every virtual machine deployed on your device has one attached operating system disk. This OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume.

NOTE

You cannot change the OS disk size for a VM deployed on your device. The OS disk size is determined by the VM size that you selected.

A data disk on the other hand, is a managed disk attached to the VM running on your device. A data disk is used to store application data. Data disks are typically SCSI drives. The size of the VM determines how many data disks you can attach to a VM. By default, premium storage is used to host the disks.

A VM deployed on your device may sometimes contain a temporary disk. The temporary disk provides short-term storage for applications and processes, and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event or when you redeploy a VM. During a successful standard reboot of the VM, data on the temporary disk will persist.

Prerequisites

Before you begin to manage disks on the VMs running on your device via the Azure portal, make sure that:

1. You've access to an activated Azure Stack Edge Pro GPU device. You have also enabled a network interface for compute on your device. This action creates a virtual switch on that network interface on your VM.
 - a. In the local UI of your device, go to **Compute**. Select the network interface that you will use to create a virtual switch.

IMPORTANT

You can only configure one port for compute.

- b. Enable compute on the network interface. Azure Stack Edge Pro GPU creates and manages a

virtual switch corresponding to that network interface.

2. You have at least one VM deployed on your device. To create this VM, see the instructions in [Deploy VM on your Azure Stack Edge Pro via the Azure portal](#).

Add a data disk

Follow these steps to add a disk to a virtual machine deployed on your device.

1. Go to the virtual machine to which you want to add a data disk, and select **Disks** in the virtual machine **Details**.

The screenshot shows the 'Disks' blade for a virtual machine named 'testdeployment'. A red box highlights the 'Disks' button in the top left. Below it, the 'OS disk' section displays the disk name as 'testdeployment_disk1_efd06d0ec1274610a30bba4c1473d1ad' and storage type as 'Standard'. The 'Data disks' section shows a table with columns: Disk name, LUN, Storage type, and Size. The table is currently empty, displaying 'No results.'

2. In the Disks blade, under **Data Disks**, select **Create and attach a new disk**.

The screenshot shows the 'Create and attach a new disk' blade. At the top, there's a breadcrumb navigation: Home > Virtual machines > Overview > Disks. The main area has a 'Data disks' button highlighted with a red box. Below it, there are two options: 'Create and attach a new disk' (highlighted with a red box) and 'Attach an existing disk'. At the bottom, there are 'Save' and 'Discard' buttons.

3. In the **Create a new disk** blade, enter the following parameters:

FIELD	DESCRIPTION
Name	A unique name within the resource group. The name cannot be changed after the data disk is created.

FIELD	DESCRIPTION
Edge resource group	Enter the Edge resource group in which to store the new disk.
Size	The size of your data disk in GiB. The maximum size of a data disk is determined by the VM size that you have selected. When provisioning a disk, you should also consider the actual space on your device and other VM workloads that are running that consume capacity.

Create new disk

Virtual machine: myasewindowsvm2

Input the name and the size in order to create and attach new disk. [Learn more about data disks](#)

Name *

Edge resource group * ⓘ

Size (GiB) * ⓘ

OK

Select OK and proceed.

- In the Disks display, you'll see an entry corresponding to the new disk. Accept the default or assign a valid Logical Unit Number (LUN) to the disk, and select Save. A LUN is a unique identifier for a SCSI disk. For more information, see [What is a LUN?](#).

Home > Virtual machines > myasewindowsvm2 >

Disks

...
myasewindowsvm2

⟳ Refresh

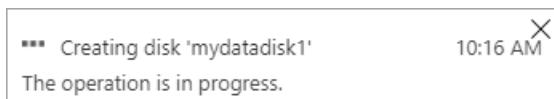
OS disk			
Name	Storage type	Size(GiB)	
myasewindowsvm2_disk1_2a066432056446669...	Standard_LRS	30	

LUN	Name	Size (GiB)	Edge resource group	
0	myvmdisk2	10	MYASERG	🔗 X
1	myazdisk1	10	MYASERG	🔗 X
2	mydatadisk3	10	MYASERG	🔗

[Create and attach a new disk](#) [Attach an existing disk](#)

Save **Discard**

5. You'll see a notification that disk creation is in progress. After the disk is successfully created, the virtual machine is updated.



6. Navigate back to the virtual machine **Details** page. The list of disks updates to display the newly created data disk.

A screenshot of the Azure portal's virtual machine details page for "myasewindowsvm2". The "Details" tab is selected. In the "Disks" section, a new disk named "mydatadisk3" is listed with LUN 2, Standard storage type, and 10 GB size. The entire "Disks" table row for "mydatadisk3" is highlighted with a red border.

Disk name	LUN	Storage type	Size
myvmdisk2	0	Standard	10 GB
myazdisk1	1	Standard	10 GB
mydatadisk3	2	Standard	10 GB

Change a data disk

Follow these steps to change a disk associated with a virtual machine deployed on your device.

1. Go to the virtual machine that has the data disk to change, and select **Disks** in the virtual machine **Details**.
2. In the list of data disks, select the disk that you wish to change. In the far right of the disk selected, select the edit icon (pencil).

Home > Virtual machines > myazvm >

Disks ... ×

myazvm

↻ Refresh

OS disk

Name	Storage type	Size(GiB)
myazosdisk1	Standard_LRS	35

Data disks

LUN	Name	Size (GiB)	Edge resource group
0	datadisk02	10	MYASEAZRG ☒
1	datadisk01	10	MYASEAZRG ☒

[Create and attach a new disk](#) [Attach an existing disk](#)

Save Discard

3. In the **Change disk** blade, you can only change the size of the disk. You can't change the name of a disk once it's created. Change the **Size** of the disk, and save the change.

Change Disk

Virtual machine: myazvm

To change the disk size, provide the data size for your workload. [Learn more about data disks](#)

Name
datadisk01

Edge resource group ⓘ
myaseazrg

Size (GiB) * ⓘ
 ✓

OK

NOTE

You can only expand a data disk. You can't shrink the disk.

4. In the **Disks** display, the list of disks refreshes to display the updated disk.

Attach an existing disk

Follow these steps to attach an existing disk to the virtual machine deployed on your device.

1. Go to the virtual machine to which you wish to attach the existing disk, and select **Disks** in the virtual machine **Details**.

2. In the Disks blade, under Data Disks, select Attach an existing disk.

The screenshot shows the 'Disks' blade for a virtual machine named 'myazvms'. The 'OS disk' section lists 'myazosdisk1' with a size of 35 GiB. The 'Data disks' section shows a table with columns: LUN, Name, Size (GiB), and Edge resource group. It contains one row for 'datadisk01' (LUN 1, 10 GiB, MYASEAZRG). Below the table are two buttons: 'Create and attach a new disk' and 'Attach an existing disk', with the latter being highlighted by a red box. At the bottom are 'Save' and 'Discard' buttons.

3. Accept default LUN or assign a valid LUN. Choose an existing data disk from the dropdown list. Select Save.

The screenshot shows the 'Disks' blade for the same virtual machine. The 'Data disks' section shows a table with LUN 1 assigned to 'datadisk01'. A new row is being added with LUN 2, and the 'Name' field contains 'datadisk02' with a dropdown arrow, which is also highlighted by a red box. The 'Create and attach a new disk' and 'Attach an existing disk' buttons are visible below. At the bottom are 'Save' and 'Discard' buttons, with the 'Save' button being highlighted by a red box.

Select **Save** and proceed.

4. You'll see a notification that the virtual machine is updated. After the VM is updated, navigate back to the virtual machine **Details** page. Refresh the page to view the newly attached disk in the list of data disks.

Disks			
OS disk			
Disk name	testdeployment_disk1_efd06d0ec127 4610a30bba4c1473d1ad		
Storage type	Standard		
Size	30 GB		
Data disks			
Disk name	LUN	Storage type	Size
mydatadisk1	1	Standard	10 GB

Detach a data disk

Follow these steps to detach or remove a data disk associated with a virtual machine deployed on your device.

NOTE

- You can remove a data disk while the VM is running. Make sure that nothing is actively using the disk before detaching it from the VM.
- If you detach a disk, it is not automatically deleted. Follow the steps in [Delete a disk](#), below.

1. Go to the virtual machine from which you wish to detach a data disk, and select **Disks** in the virtual machine **Details**.

Disks			
OS disk			
Disk name	testdeployment_disk1_efd06d0ec127 4610a30bba4c1473d1ad		
Storage type	Standard		
Size	30 GB		
Data disks			
Disk name	LUN	Storage type	Size
mydatadisk1	1	Standard	10 GB
mydatadisk2	2	Standard	10 GB

2. In the list of disks, select the disk that you wish to detach. In the far right of the disk selected, select the detach icon ("X"). The selected disk will be detached. Select **Save**.

Disks

testdeployment



OS disk

Name	Storage type	Size(GiB)
testdeployment_disk1_efd06d0ec1274610a30bba4c1473d1ad	Standard_LRS	30

Data disks

LUN	Name	Size (GiB)	
1	mydatadisk1	10	

[Create and attach a new disk](#)[Attach an existing disk](#)[Save](#)[Discard](#)

3. After the disk is detached, the virtual machine is updated. Refresh the page to view the updated list of data disks.

Disks

OS disk

Disk name	testdeployment_disk1_efd06d0ec1274610a30bba4c1473d1ad
Storage type	Standard
Size	30 GB

Data disks

Disk name	LUN	Storage type	Size
mydatadisk1	1	Standard	10 GB

Delete a data disk

Follow these steps to delete a data disk that's not attached to a VM deployed on your device.

NOTE

Before deleting a data disk, you must [detach the data disk from the VM](#) if the disk is in use.

1. Go to **Virtual machines** on your device, and go to the **Resources** pane. Select **Disks**.

Virtual machines | Resources

Networking Disks Edge resource groups

Name	Size (GiB)	Attached VM	Edge resource group
myasewindowsvm2_disk1	30	myasewindowsvm2	MYASERG
myazdisk1	10	myasewindowsvm2	MYASERG
myazmd	30	-	MYASEAZRG
myazosdisk1	35	myazvm	MYASEAZRG
myvmdisk2	10	myasewindowsvm2	MYASERG

2. In the list of disks, select the disk that you wish to delete. In the far right of the disk selected, select the delete icon (trashcan).

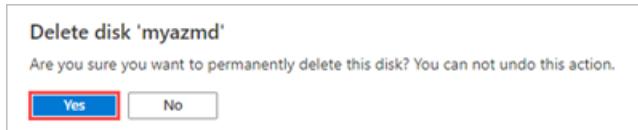
Virtual machines | Resources

Networking Disks Edge resource groups

Name	Size (GiB)	Attached VM	Edge resource group
myasewindowsvm2_disk1_2a0664320564466693...	30	myasewindowsvm2	MYASERG
myazdisk1	10	myasewindowsvm2	MYASERG
myazmd	30	-	MYASEAZRG
myazosdisk1	35	myazvm	MYASEAZRG
myvmdisk2	10	myasewindowsvm2	MYASERG

If you don't see the delete icon, you can select the VM name in the **Attached VM** column and [detach the disk from the VM](#).

3. You'll see a message asking you to confirm that you want to delete the disk. The operation can't be reversed. Select **Yes**.



When deletion is complete, the disk is removed from the list.

Next steps

To learn how to deploy virtual machines on your Azure Stack Edge Pro device, see [Deploy virtual machines via the Azure portal](#).

Manage Edge resource groups on Azure Stack Edge Pro GPU devices

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

Edge resource groups contain resources that are created on the device via the local Azure Resource Manager during virtual machine creation and deployment. These local resources can include virtual machines, VM images, disks, network interfaces, and other resource types such as Edge storage accounts.

This article describes how to view and delete Edge resource groups on an Azure Stack Edge Pro GPU device.

View Edge resource groups

Follow these steps to view the Edge resource groups for the current subscription.

1. Go to **Virtual machines** on your device, and go to the **Resources** pane. Select **Edge resource groups**.

Name	Virtual machines	Managed images	Disks	Network interfaces	Other resources
ase-image-resourcegroup	1	-	4	1	1
ASERG	1	2	2	1	1
atda-RG	-	-	-	-	-

NOTE

You can get the same listing by using `Get-AzResource` in Azure PowerShell after you set up the Azure Resource Manager environment on your device. For more information, see [Connect to Azure Resource Manager](#).

Delete an Edge resource group

Follow these steps to delete an Edge resource group that's no longer in use.

NOTE

- A resource group must be empty to be deleted.
- You can't delete the ASERG resource group. That resource group stores the ASEVNET virtual network, which is created automatically when you enable compute on your device.

1. Go to **Virtual machines** on your device, and go to the **Resources** pane. Select **Edge resource groups**.

Name	Virtual machines	Managed images	Disks	Network interfaces	Other resources
ase-image-resourcegroup	1	-	4	1	1
ASERG	1	2	2	1	1
atda-RG	-	-	-	-	-

2. Select the resource group that you want to delete. In the far right of the resource group, select the delete icon (trashcan).

The delete icon is only displayed when a resource group doesn't contain any resources.

Name	Virtual machines	Managed images	Disks	Network interfaces	Other resources
ase-image-resourcegroup	1	-	2	1	1
ASERG	-	1	-	-	1
asevmresources	-	1	-	-	-
asevmresources	-	-	-	-	-
myaseazrg1	-	-	-	-	1
myaseazrg2	-	-	-	-	1

3. You'll see a message asking you to confirm that you want to delete the Edge resource group. The operation can't be reversed. Select Yes.



When deletion is complete, the resource group is removed from the list.

Next steps

- To learn how to administer your Azure Stack Edge Pro GPU device, see [Use local web UI to administer an Azure Stack Edge Pro GPU](#).
- Set up the Azure Resource Manager environment on your device.

Use the Azure portal to resize the VMs on your Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article explains how to resize the virtual machines (VMs) deployed on your Azure Stack Edge Pro GPU device.

About VM sizing

The VM size determines the amount of compute resources (like CPU, GPU, and memory) that are made available to the VM. You should create virtual machines by using a VM size appropriate for your application workload.

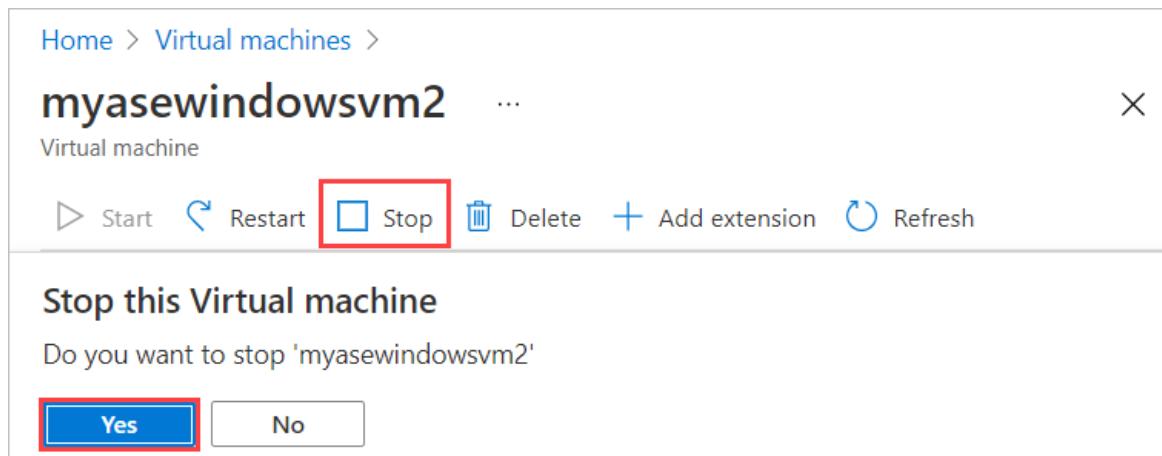
Even though all the machines will be running on the same hardware, machine sizes have different limits for disk access. This can help you manage overall disk access across your VMs. If a workload increases, you can also resize an existing virtual machine.

For more information, see [Supported VM sizes for your device](#).

Prerequisites

Before you resize a VM running on your device via the Azure portal, make sure that:

1. You have at least one VM deployed on your device. To create this VM, see the instructions in [Deploy VM on your Azure Stack Edge Pro via the Azure portal](#).
2. Your VM should be in **Stopped** state. To stop your VM, go to **Virtual machines > Overview** and select the VM you want to stop. In the Overview page, select **Stop** and then select **Yes** when prompted for confirmation. Before you resize your VM, you must stop the VM.



Resize a VM

Follow these steps to resize a virtual machine deployed on your device.

1. Go to the virtual machine that you have stopped, and select **VM size (change)** in the virtual machine **Details**.

Home > Virtual machines >

myazvms

Virtual machine

Start Restart Stop Delete Add extension Refresh

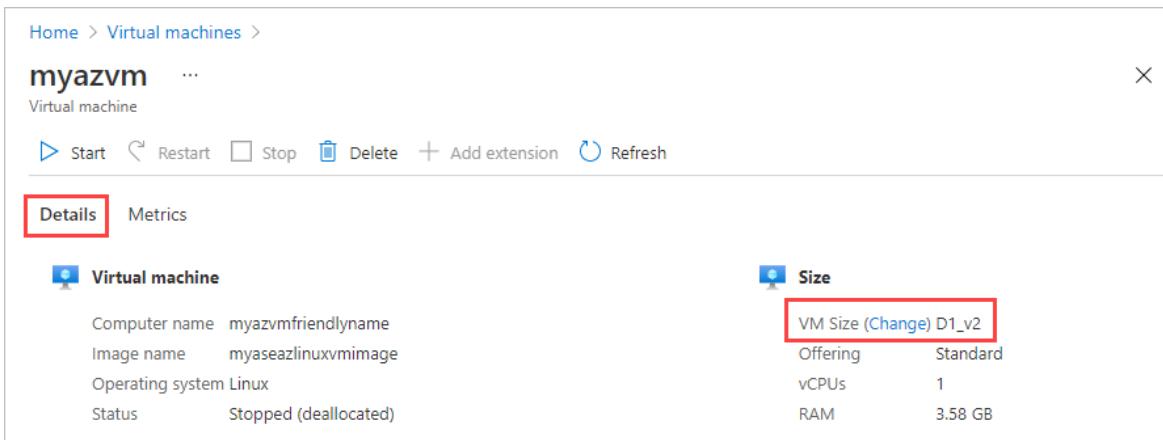
Details Metrics

Virtual machine

Computer name	myazvmsfriendlyname
Image name	myaseazlinuxvmimage
Operating system	Linux
Status	Stopped (deallocated)

Size

VM Size (Change)	D1_v2
Offering	Standard
vCPUs	1
RAM	3.58 GB



2. In the Change VM size blade, from the command bar, select the VM size and then select Change.

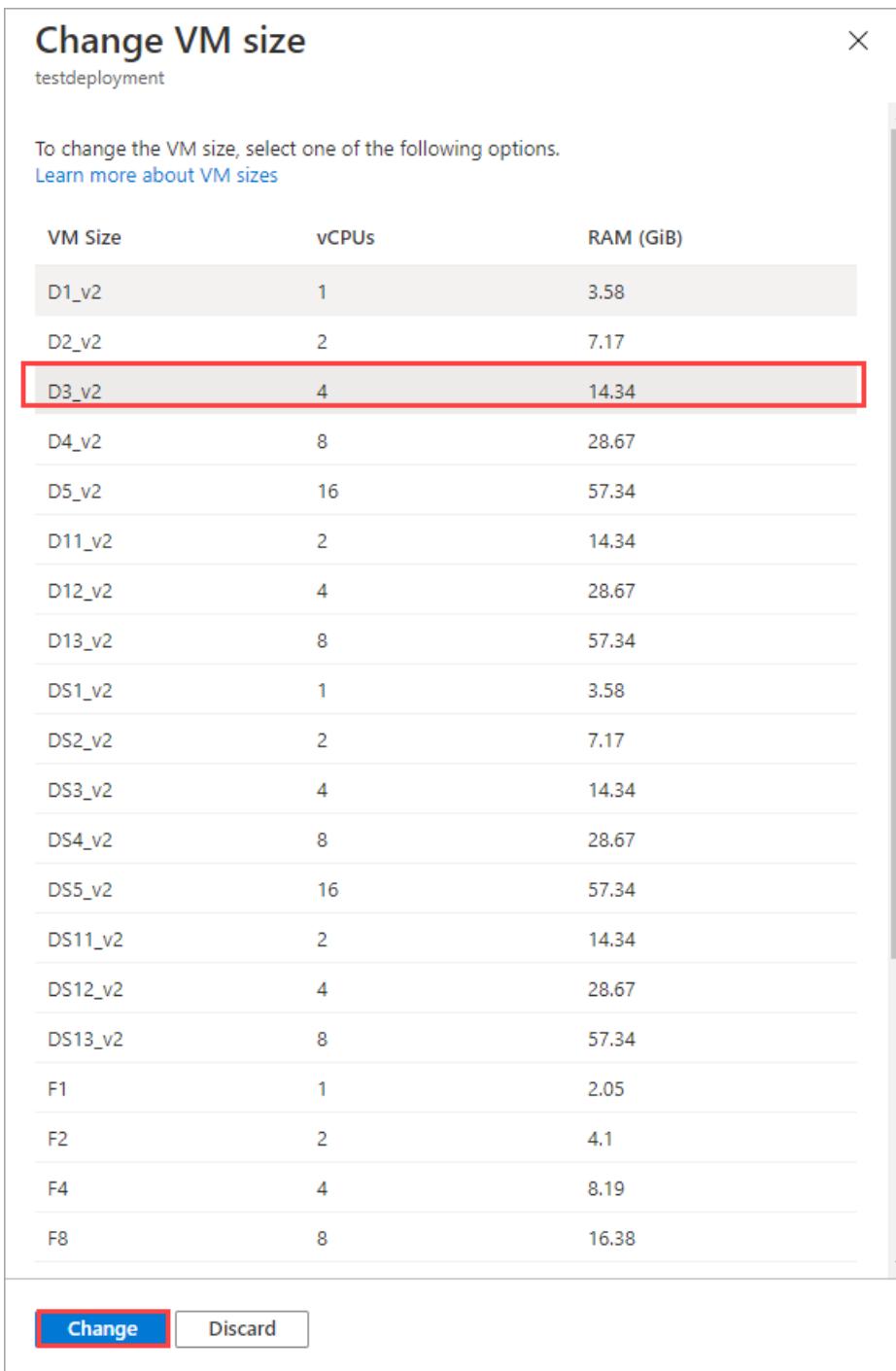
Change VM size

testdeployment

To change the VM size, select one of the following options.
[Learn more about VM sizes](#)

VM Size	vCPUs	RAM (GiB)
D1_v2	1	3.58
D2_v2	2	7.17
D3_v2	4	14.34
D4_v2	8	28.67
D5_v2	16	57.34
D11_v2	2	14.34
D12_v2	4	28.67
D13_v2	8	57.34
DS1_v2	1	3.58
DS2_v2	2	7.17
DS3_v2	4	14.34
DS4_v2	8	28.67
DS5_v2	16	57.34
DS11_v2	2	14.34
DS12_v2	4	28.67
DS13_v2	8	57.34
F1	1	2.05
F2	2	4.1
F4	4	8.19
F8	8	16.38

Change Discard



3. You'll see a notification that the virtual machine is being updated. After the virtual machine is successfully updated, the Overview page refreshes to display the resized VM.

Overview



Start Restart Stop Delete Refresh

Virtual machine

Computer name testdeployment

OS Linux

Status Stopped

Size

VM Size ([Change](#))

D3_v2

Offering

Standard

vCPUs

4

RAM

14.34 GB

Next steps

To learn how to deploy virtual machines on your Azure Stack Edge Pro device, see [Deploy virtual machines via the Azure portal](#).

Create a new virtual switch in Azure Stack Edge Pro GPU via PowerShell

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to create a new virtual switch on your Azure Stack Edge Pro GPU device. For example, you would create a new virtual switch if you want your virtual machines to connect through a different physical network port.

VM deployment workflow

1. Connect to the PowerShell interface on your device.
2. Query available physical network interfaces.
3. Create a virtual switch.
4. Verify the virtual network and subnet that are automatically created.

Prerequisites

Before you begin, make sure that:

- You've access to a client machine that can access the PowerShell interface of your device. See [Connect to the PowerShell interface](#).

The client machine should be running a [Supported OS](#).

- Use the local UI to enable compute on one of the physical network interfaces on your device as per the instructions in [Enable compute network](#) on your device.

Connect to the PowerShell interface

[Connect to the PowerShell interface of your device](#).

Query available network interfaces

1. Use the following command to display a list of physical network interfaces on which you can create a new virtual switch. You will select one of these network interfaces.

```
Get-NetAdapter -Physical
```

Here is an example output:

```
[10.100.10.10]: PS>Get-NetAdapter -Physical
```

Name LinkSpeed	InterfaceDescription	ifIndex	Status	MacAddress
Port2	QLogic 2x1GE+2x25GE QL41234HMCU NIC ...	12	Up	34-80-0D-
05-26-EA ...ps	Ethernet Remote NDIS Compatible Device	11	Up	F4-02-70-
CD-41-39 ...ps	Port1 QLogic 2x1GE+2x25GE QL41234HMCU NI...#3	9	Up	34-80-0D-
05-26-EB ...ps	Port5 Mellanox ConnectX-4 Lx Ethernet Ad...#2	8	Up	0C-42-A1-
C0-E3-99 ...ps	Port3 QLogic 2x1GE+2x25GE QL41234HMCU NI...#4	7	Up	34-80-0D-
05-26-E9 ...ps	Port6 Mellanox ConnectX-4 Lx Ethernet Adapter	6	Up	0C-42-A1-
C0-E3-98 ...ps	Port4 QLogic 2x1GE+2x25GE QL41234HMCU NI...#2	4	Up	34-80-0D-
05-26-E8 ...ps				

```
[10.100.10.10]: PS>
```

2. Choose a network interface that is:

- In the **Up** status.
- Not used by any existing virtual switches. Currently, only one virtual switch can be configured per network interface.

To check the existing virtual switch and network interface association, run the

```
Get-HcsExternalVirtualSwitch
```

Here is an example output.

```
[10.100.10.10]: PS>Get-HcsExternalVirtualSwitch
```

Name	:	vSwitch1
InterfaceAlias	:	{Port2}
EnableIov	:	True
MacAddressPools	:	
IPAddressPools	:	{}
ConfigurationSource	:	Dsc
EnabledForCompute	:	True
SupportsAcceleratedNetworking	:	False
DbeDhcpHostVnicName	:	f4a92de8-26ed-4597-a141-cb233c2ba0aa
Type	:	External

```
[10.100.10.10]: PS>
```

In this instance, Port 2 is associated with an existing virtual switch and shouldn't be used.

Create a virtual switch

Use the following cmdlet to create a new virtual switch on your specified network interface. After this operation is complete, your compute instances can use the new virtual network.

```
Add-HcsExternalVirtualSwitch -InterfaceAlias <Network interface name> -WaitForSwitchCreation $true
```

Use the `Get-HcsExternalVirtualSwitch` command to identify the newly created switch. The new switch that is created is named as `vswitch-<InterfaceAlias>`.

Here is an example output:

```
[10.100.10.10]: PS> Add-HcsExternalVirtualSwitch -InterfaceAlias Port5 -WaitForSwitchCreation $true
[10.100.10.10]: PS>Get-HcsExternalVirtualSwitch

Name          : vSwitch1
InterfaceAlias : {Port2}
EnableIov     : True
MacAddressPools :
IPAddressPools :
ConfigurationSource : Dsc
EnabledForCompute : True
SupportsAcceleratedNetworking : False
DbeDhcpHostVnicName : f4a92de8-26ed-4597-a141-cb233c2ba0aa
Type          : External

Name          : vswitch-Port5
InterfaceAlias : {Port5}
EnableIov     : True
MacAddressPools :
IPAddressPools :
ConfigurationSource : Dsc
EnabledForCompute : False
SupportsAcceleratedNetworking : False
DbeDhcpHostVnicName : 9b301c40-3daa-49bf-a20b-9f7889820129
Type          : External

[10.100.10.10]: PS>
```

Verify network, subnet for switch

After you have created the new virtual switch, Azure Stack Edge Pro GPU automatically creates a virtual network and subnet that corresponds to it. You can use this virtual network when creating VMs.

To identify the virtual network and the subnet associated with the new switch that you created, use the `Get-HcsVirtualNetwork` cmdlet.

Create virtual LANs

To add a virtual local area network (LAN) configuration on a virtual switch, use the following cmdlet.

```
Add-HcsVirtualNetwork-VirtualSwitchName <Virtual Switch name> -VnetName <Virtual Network Name> -VlanId <Vlan Id> -AddressSpace <Address Space> -GatewayIPAddress <Gateway IP>-DnsServers <Dns Servers List> -DnsSuffix <Dns Suffix name>
```

The following parameters can be used with the `Add-HcsVirtualNetwork-VirtualSwitchName` cmdlet.

PARAMETERS	DESCRIPTION
VNetName	Name for the virtual LAN network
VirtualSwitchName	Virtual switch name where you want to add virtual LAN config
AddressSpace	Subnet address space for the virtual LAN network
GatewayIPAddress	Gateway for the virtual network

PARAMETERS	DESCRIPTION
DnsServers	List of Dns Server IP addresses
DnsSuffix	Dns name without the host part for the virtual LAN network subnet

Here is an example output.

```
[10.100.10.10]: PS> Add-HcsVirtualNetwork -VirtualSwitchName vSwitch1 -VnetName vlanNetwork100 -VlanId 100 -AddressSpace 5.5.0.0/16 -GatewayIPAddress 5.5.0.1 -DnsServers "5.5.50.50","5.5.50.100" -DnsSuffix "name.domain.com"

[10.100.10.10]: PS> Get-HcsVirtualNetwork

Name          : vnet2015
AddressSpace   : 10.128.48.0/22
SwitchName     : vSwitch1
GatewayIPAddress : 10.128.48.1
DnsServers    : {}
DnsSuffix      :
VlanId        : 2015

Name          : vnet3011
AddressSpace   : 10.126.64.0/22
SwitchName     : vSwitch1
GatewayIPAddress : 10.126.64.1
DnsServers    : {}
DnsSuffix      :
VlanId        : 3011
```

NOTE

- You can configure multiple virtual LANs on the same virtual switch.
- The gateway IP address must in the same subnet as the parameter passed in as address space.
- You can't remove a virtual switch if there are virtual LANs configured. To delete this virtual switch, you first need to delete the virtual LAN and then delete the virtual switch.

Verify network, subnet for virtual LAN

After you've created the virtual LAN, a virtual network and a corresponding subnet are automatically created. You can use this virtual network when creating VMs.

To identify the virtual network and the subnet associated with the new switch that you created, use the `Get-HcsVirtualNetwork` cmdlet.

Next steps

- [Deploy VMs on your Azure Stack Edge Pro GPU device via Azure PowerShell](#)
- [Deploy VMs on your Azure Stack Edge Pro GPU device via the Azure portal](#)

Tag VMs on Azure Stack Edge via Azure PowerShell

9/21/2022 • 7 minutes to read • [Edit Online](#)

This article describes how to tag virtual machines (VMs) running on your Azure Stack Edge Pro GPU devices using Azure PowerShell.

About tags

Tags are user-defined key-value pairs that can be assigned to a resource or a resource group. You can apply tags to VMs running on your device to logically organize them into a taxonomy. You can place tags on a resource at the time of creation or add it to an existing resource. For example, you can apply the name `Organization` and the value `Engineering` to all VMs that are used by the Engineering department in your organization.

For more information on tags, see how to [Manage tags via AzureRM PowerShell](#).

Prerequisites

Before you can deploy a VM on your device via PowerShell, make sure that:

- You have access to a client that you'll use to connect to your device.
 - Your client runs a [Supported OS](#).
 - Your client is configured to connect to the local Azure Resource Manager of your device as per the instructions in [Connect to Azure Resource Manager for your device](#).

Verify connection to local Azure Resource Manager

Make sure that the following steps can be used to access the device from your client.

Verify that your client can connect to the local Azure Resource Manager.

1. Call local device APIs to authenticate:

- [Az](#)
- [AzureRM](#)

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

2. Provide the username `EdgeArmUser` and the password to connect via Azure Resource Manager. If you do not recall the password, [Reset the password for Azure Resource Manager](#) and use this password to sign in.

Add a tag to a VM

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$VMName = <VM Name>
$VMRG = <VM Resource Group>
$TagName = <Tag Name>
$TagValue = <Tag Value>
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VMName = "myazvm"
PS C:\WINDOWS\system32> $VMRG = "myaseazrg"
PS C:\WINDOWS\system32> $TagName = "Organization"
PS C:\WINDOWS\system32> $TagValue = "Sales"
```

2. Get the VM object and its tags.

```
$VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
$tags = $VirtualMachine.Tags
```

3. Add the tag and update the VM. Updating the VM may take a few minutes.

You can use the optional **-Force** flag to run the command without user confirmation.

```
$tags.Add($TagName, $TagValue)
Set-AzResource -ResourceId $VirtualMachine.Id -Tag $tags -Force
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
PS C:\WINDOWS\system32> $tags = $VirtualMachine.Tags
PS C:\WINDOWS\system32> $tags.Add($TagName, $TagValue)
PS C:\WINDOWS\system32> Set-AzResource -ResourceId $VirtualMachine.ID -Tag $tags -Force

Name          : myazvm
ResourceId    : /subscriptions/d64617ad-6266-4b19-45af-81112d213322/resourceGroups/myaseazrg/providers/Microsoft.Compute/virtualMachines/myazvm
ResourceName   : myazvm
ResourceType   : Microsoft.Compute/virtualMachines
ResourceGroupName : myaseazrg
Location       : dbelocal
SubscriptionId : d64617ad-6266-4b19-45af-81112d213322
Tags          : {Organization}
Properties     : @{vmId=568a264f-c5d3-477f-a16c-4c5549eafa8c; hardwareProfile=;
                  storageProfile=; osProfile=; networkProfile=; diagnosticsProfile=;
                  provisioningState=Succeeded}
```

View tags of a VM

- [Az](#)
- [AzureRM](#)

You can view the tags applied to a specific virtual machine running on your device.

1. Define the parameters associated with the VM whose tags you want to view.

```
$VMName = <VM Name>
$VMRG = <VM Resource Group>
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VMName = "myazvm"
PS C:\WINDOWS\system32> $VMRG = "myaseazrg"
```

2. Get the VM object and view its tags.

```
$VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
$VirtualMachine.Tags
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
PS C:\WINDOWS\system32> $VirtualMachine.Tags

Key          Value
---          -----
Organization  Sales

PS C:\WINDOWS\system32>
```

View tags for all resources

- [Az](#)
- [AzureRM](#)

To view the current list of tags for all the resources in the local Azure Resource Manager subscription (different from your Azure subscription) of your device, use the `Get-AzTag` command.

Here is an example output when multiple VMs are running on your device and you want to view all the tags on all the VMs.

```
PS C:\WINDOWS\system32> Get-AzTag

Name      Count
----      -----
Organization 2

PS C:\WINDOWS\system32>
```

The preceding output indicates that there are two `Organization` tags on the VMs running on your device.

To view further details, use the `-Detailed` parameter.

```
PS C:\WINDOWS\system32> Get-AzTag -Detailed |f1

Name      : Organization
ValuesTable :
    Name      Count
    ======  ====
    Sales     1
    Engineering 1
Count      : 2
Values     : {Sales, Engineering}

PS C:\WINDOWS\system32>
```

The preceding output indicates that out of the two tags, 1 VM is tagged as `Engineering` and the other one is tagged as belonging to `Sales`.

Remove a tag from a VM

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$VMName = <VM Name>
$VMRG = <VM Resource Group>
$TagName = <Tag Name>
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VMName = "myaselinuxvm1"
PS C:\WINDOWS\system32> $VMRG = "myaserg1"
PS C:\WINDOWS\system32> $TagName = "Organization"
```

2. Get the VM object.

```
$VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
$VirtualMachine
```

Here is an example output:

```
PS C:\WINDOWS\system32> $VirtualMachine = Get-AzVM -ResourceGroupName $VMRG -Name $VMName
PS C:\WINDOWS\system32> $VirtualMachine

ResourceGroupName  : myaseazrg
Id               : /subscriptions/d64617ad-6266-4b19-45af-81112d21332/resourceGroups/myaseazrg/providers/Microsoft.Compute/virtualMachines/myazvm
VmId             : 568a264f-c5d3-477f-a16c-4c5549eafa8c
Name              : myazvm
Type              : Microsoft.Compute/virtualMachines
Location          : dbelocal
Tags              : {"Organization":"Sales"}
DiagnosticsProfile : {BootDiagnostics}
HardwareProfile   : {VmSize}
NetworkProfile    : {NetworkInterfaces}
OSProfile         : {ComputerName, AdminUsername, LinuxConfiguration, Secrets, AllowExtensionOperations, RequireGuestProvisionSignal}
ProvisioningState  : Succeeded
StorageProfile    : {ImageReference, OsDisk, DataDisks}

PS C:\WINDOWS\system32>
```

3. Remove the tag and update the VM. Use the optional `-Force` flag to run the command without user confirmation.

```
$tags = $VirtualMachine.Tags
$tags.Remove($TagName)
Set-AzResource -ResourceId $VirtualMachine.Id -Tag $tags -Force
```

Here is an example output:

```
PS C:\WINDOWS\system32> $tags = $VirtualMachine.Tags
PS C:\WINDOWS\system32> $tags.Remove($TagName)
True
PS C:\WINDOWS\system32> Set-AzResource -ResourceId $VirtualMachine.Id -Tag $tags -Force

Name          : myazvm
ResourceId    : /subscriptions/d64617ad-6266-4b19-45af-81112d213322/resourceGroups/myaseazrg/providers/Microsoft.Compute/virtualMachines/myazvm
ResourceName   : myazvm
ResourceType   : Microsoft.Compute/virtualMachines
ResourceGroupName : myaseazrg
Location       : dbelocal
SubscriptionId : d64617ad-6266-4b19-45af-81112d213322
Tags          : {}
Properties     : @{vmId=568a264f-c5d3-477f-a16c-4c5549eafa8c; hardwareProfile=;
                  storageProfile=; osProfile=; networkProfile=; diagnosticsProfile=;
                  provisioningState=Succeeded}

PS C:\WINDOWS\system32>
```

Next steps

- Learn how to [How to tag a virtual machine in Azure using az cmdlets in PowerShell](#).
- Learn how to [Manage tags via AzureRM cmdlets in PowerShell](#).

Reset VM password for your Azure Stack Edge Pro GPU device via the Azure portal

9/21/2022 • 2 minutes to read • [Edit Online](#)

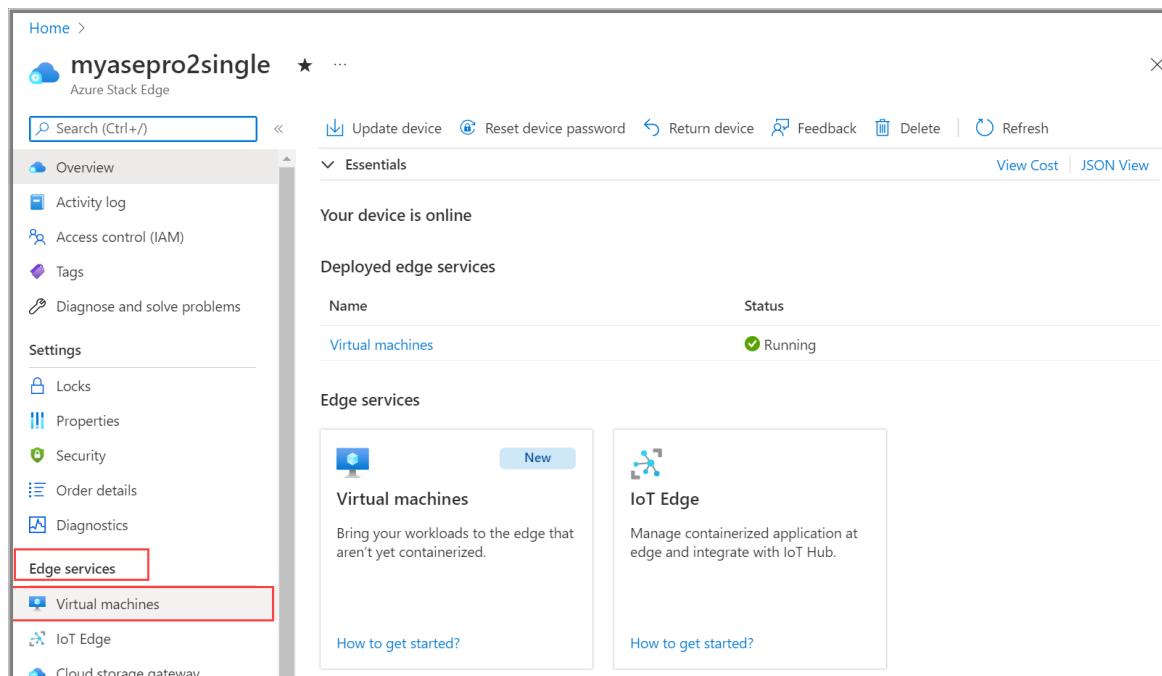
APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article covers steps to reset the password on both Windows and Linux VMs using the Azure portal. To reset a password using PowerShell and local Azure Resource Manager templates, see [Install the VM password reset extension](#).

Reset Windows VM password

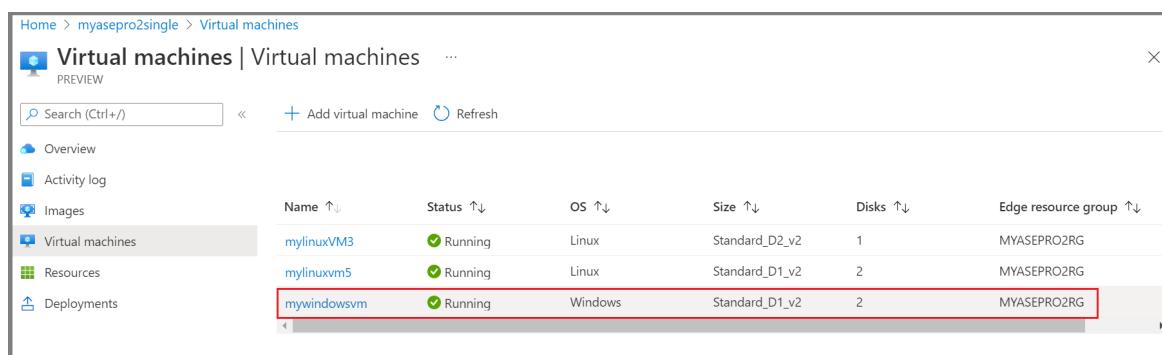
Use the following steps to reset the VM password for your Azure Stack Edge Pro GPU device:

1. In the Azure portal, go to the Azure Stack Edge resource for your device, then go to **Edge services > Virtual machines**.



The screenshot shows the Azure Stack Edge resource page for 'myasepro2single'. The left sidebar has a 'Edge services' section with 'Virtual machines' highlighted. The main area shows 'Your device is online' and 'Deployed edge services' with a table for 'Virtual machines' (Status: Running). It also shows 'Edge services' like 'Virtual machines' and 'IoT Edge'.

2. From the Azure portal VM list view, select the VM name with the password you would like to reset.



The screenshot shows the 'Virtual machines' list view for 'myasepro2single'. The 'Virtual machines' item in the sidebar is selected. The main table lists three VMs: 'mylinuxVM3' (Linux, Standard_D2_v2, 1 disk, Edge resource group MYASEPRO2RG), 'mylinuxvm5' (Linux, Standard_D1_v2, 2 disks, Edge resource group MYASEPRO2RG), and 'mywindowsvm' (Windows, Standard_D1_v2, 2 disks, Edge resource group MYASEPRO2RG). The row for 'mywindowsvm' is highlighted with a red border.

3. Select **Reset password**.

Virtual machine

Size

Installed extensions

Computer name	mywindowsvm	VM Size (Change)	D1_v2	Name	Status
Image name	windowsvhd	Offering	Standard	windowsVMAccessExt	Succeeded
Operating system	Windows	vCPUs	1		
Status	Running	RAM	3.58 GB		

Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group...
mywindowsvmnic (primary)	10.57.50.146	vswitch1	vswitch1subNet	Dynamic	MYASEPRO2RG

Disk

OS disk	LUN	Storage type	Size
mywindowsvm_disk1_52cbdf3ca9634ee6bec4d	0	Standard	10 GB

4. Specify the username and the new password. Confirm the new password, and then select **Save**.

For more information about Windows VM password requirements, see [Password requirements for a Windows VM](#).

Virtual machine

Size

Reset password

This uses the VMAccess extension to reset the built-in administrator account and reset the Remote Desktop service configuration. Once you have logged in to the VM, you should reset the password for that user. [Learn more](#)

Computer name	mywindowsvm	VM Size (Change)	D1_v2
Image name	windowsvhd	Offering	Standard
Operating system	Windows	vCPUs	1
Status	Running	RAM	3.58 GB

Networking

Network interface	IP Address	Virtual network	Subnet
mywindowsvmnic (primary)	10.57.50.146	vswitch1	vswitch1subNet

Disk

OS disk	LUN	Storage type	Size
mywindowsvm_disk1_52cbdf3ca9634ee6bec4d	0	Standard	10 GB

5. While the operation is in progress, you can view the notification that shows the status of the operation. Select **Refresh** to update status of the operation.

Virtual machine

Size

Installed extensions

Computer name	mywindowsvm	VM Size (Change)	D1_v2	Name	Status
Image name	windowsvhd	Offering	Standard	windowsVMAccessExt	Succeeded
Operating system	Windows	vCPUs	1		
Status	Running	RAM	3.58 GB		

Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group
mywindowsvmnic (primary)	10.57.50.146	vswitch1	vswitch1subNet	Dynamic	MYASEPRO2RG

6. When the operation is complete, you can see that the *windowsVMAccessExt* extension is installed for the VM.

Name	Status
windowsVMAccessExt	Succeeded

7. Connect to the VM with the new password.

Reset Linux VM password

Use the following steps to reset the VM password for your Azure Stack Edge Pro GPU device:

- In the Azure portal, go to the Azure Stack Edge resource for your device, then go to **Edge services > Virtual machines**.

- From the Azure portal VM list view, select the VM name with the password you would like to reset.

Name	Status	OS	Size	Disks	Edge resource group
mylinuxVM3	Running	Linux	Standard_D2_v2	1	MYASEPRO2RG
mylinuxvm5	Running	Linux	Standard_D1_v2	2	MYASEPRO2RG
mywindowsvm	Running	Windows	Standard_D1_v2	2	MYASEPRO2RG

- Select **Reset password**.

The screenshot shows the Azure portal interface for a virtual machine named 'mylinuxvm5'. The top navigation bar includes 'Start', 'Restart', 'Stop', 'Delete', 'Add extension', 'Reset password' (which is highlighted with a red box), and 'Refresh'. Below the navigation is a 'Details' tab selected, showing the following information:

Virtual machine		Size		Installed extensions	
Computer name	mylinuxvm5	VM Size (Change)	D1_v2	Name	Status
Image name	Newlinuximg	Offering	Standard	No results.	
Operating system	Linux	vCPUs	1		
Status	Running	RAM	3.58 GB		

Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource...
mylinuxvm5nic (primary)	10.57.51.13	vswitch1	vswitch1subNet	Dynamic	MYASEPRO2RG

Disks

OS disk		Data disks	
Disk name	LUN	Storage type	Size
mydisk5	1	Standard	10 GB

4. Specify the username and the new password. Confirm the new password, and then select **Save**.

For more information about Linux VM password requirements, see [Password requirements for a Linux VM](#).

The screenshot shows the Azure portal interface for a virtual machine named 'mylinuxvm5'. The 'Reset password' button is highlighted with a red box. A modal dialog titled 'Reset password' is open, showing the following fields:

Authentication type *	
<input checked="" type="radio"/> Password	<input type="radio"/> SSH public key

Username *: azureuser

Password *: (redacted)

Confirm password *: (redacted)

At the bottom right of the dialog are 'Save' and 'Discard' buttons, with 'Save' highlighted with a red box.

5. While the operation is in progress, you can view the notification that shows the status of the operation.

Select **Refresh** to update status of the operation.

Home > myasepro2single > Virtual machines >
mylinuxvm5 ...
Virtual machine
Start Restart Stop Delete Add extension Reset password Refresh

Details Metrics

Virtual machine

Computer name	mylinuxvm5
Image name	Newlinuximg
Operating system	Linux
Status	Running

Size

VM Size (Change)	D1_v2
Offering	Standard
vCPUs	1
RAM	3.58 GB

Installed extensions

Name	Status
linuxVMAccessExt	Succeeded

Networking

Network interface	IP Address	Virtual network	Subnet	IP allocation method	Select an edge resource group
mylinuxvm5nic (primary)	10.57.51.13	vswitch1	vswitch1subNet	Dynamic	MYASEPRO2RG

6. When the operation is complete, you can see that the */linuxVMAccessExt* extension is installed for the VM.

Home > myasepro2single > Virtual machines >
mylinuxvm5 ...
Virtual machine
Start Restart Stop Delete Add extension Reset password Refresh

Details Metrics

Virtual machine

Computer name	mylinuxvm5
Image name	Newlinuximg
Operating system	Linux
Status	Running

Size

VM Size (Change)	D1_v2
Offering	Standard
vCPUs	1
RAM	3.58 GB

Installed extensions

Name	Status
linuxVMAccessExt	Succeeded

7. Connect to the VM with the new password.

Next steps

- Learn about [Deploy VMs on your Azure Stack Edge Pro GPU device via the Azure portal](#).
- Learn about [Install the password reset extension on VMs for your Azure Stack Edge Pro GPU device](#).

Back up VM disks on Azure Stack Edge Pro GPU via Azure PowerShell

9/21/2022 • 10 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to create backups of virtual machine disks on Azure Stack Edge Pro GPU device using Azure PowerShell.

IMPORTANT

This procedure is meant to be used for VMs that are stopped. To back up running VMs, we recommend that you use a third-party backup tool.

Workflow

The following steps summarize the high-level workflow to back up a VM disk on your device:

1. Stop the VM.
2. Take a snapshot of the VM disk.
3. Copy the snapshot to a local storage account as a VHD.
4. Upload the VHD to an external target.

Prerequisites

Before you back up VMs, make sure that:

- You've access to a client that you'll use to connect to your device.
 - Your client runs a [Supported OS](#).
 - Your client is configured to connect to the local Azure Resource Manager of your device as per the instructions in [Connect to Azure Resource Manager for your device](#).

Verify connection to local Azure Resource Manager

Make sure that the following steps can be used to access the device from your client.

Verify that your client can connect to the local Azure Resource Manager.

1. Call local device APIs to authenticate:

- [Az](#)
- [AzureRM](#)

```
login-AzAccount -EnvironmentName <Environment Name> -TenantId c0257de7-538f-415c-993a-1b87a031879d
```

2. Provide the username `EdgeArmUser` and the password to connect via Azure Resource Manager. If you do not recall the password, [Reset the password for Azure Resource Manager](#) and use this password to sign in.

Back up a VM Disk

- [Az](#)
- [AzureRM](#)

1. Get a list of the VMs running on your device. Identify the VM that you want to stop and the corresponding resource group.

```
Get-AzVM
```

Here is an example output:

```
PS C:\Users\user> Get-AzVM

ResourceGroupName          Name  Location        VmSize OsType      NIC
-----      -----      -----      -----
MYASEAZRG                 myazvm dbelocal Standard_D1_v2 Linux      myaznic1
MYASERG                   myasewindowsvm2 dbelocal Standard_D1_v2 Linux myasewindowsvm2nic

PS C:\Users\user>
```

2. Set some parameters.

```
$ResourceGroupName = "<Resource group name>"  
$VmName = "<VM name>"
```

3. Stop the VM.

```
Stop-AzVM -ResourceGroupName $ResourceGroupName -Name $VmName
```

Here is an example output:

```
PS C:\Users\user> Stop-AzVM -ResourceGroupName myaserg -Name myasewindowsvm2  
Virtual machine stopping operation  
This cmdlet will stop the specified virtual machine. Do you want to continue?  
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y  
  
OperationId : 8a2fa7ea-99d0-4f9f-b8ca-e37389cd8413  
Status       : Succeeded  
StartTime    : 6/28/2021 11:51:33 AM  
EndTime      : 6/28/2021 11:51:50 AM  
Error        :  
  
PS C:\Users\user>
```

You can also stop the VM from the Azure portal.

4. Take a snapshot of the VM disk and save the snapshot to a local resource group. You can use this procedure for both OS and data disks.

- a. Get the list of disks on your device, or in a specific resource group. Make a note of the name of the disk to back up.

```
$Disk = Get-AzDisk -ResourceGroupName $ResourceGroupName  
$Disk.Name
```

Here is an example output:

```
PS C:\Users\user> $Disk = Get-AzDisk -ResourceGroupName myaserg
PS C:\Users\user> $Disk.Name
myasewindowsvm2_disk1_2a066432056446669368969835d5e3b3
myazdisk1
myvmdisk2
PS C:\Users\user>
```

- b. Create a local resource group to serve as the destination for the VM snapshot. Location is set as `dbelocal`.

```
New-AzResourceGroup -ResourceGroupName <Resource group name> -Location dbelocal
```

```
PS C:\Users\user> New-AzResourceGroup -ResourceGroupName myaseazrg1 -Location dbelocal

ResourceGroupName : myaseazrg1
Location        : dbelocal
ProvisioningState : Succeeded
Tags            :
ResourceId      : /subscriptions/.../resourceGroups/myaseazrg1

PS C:\Users\user>
```

- c. Set some parameters.

```
$DiskResourceGroup = <Disk resource group>
$DiskName = <Disk name>
$SnapshotName = <Snapshot name>
$DestinationRG = <Snapshot destination resource group>
```

- d. Set the snapshot configuration and take the snapshot.

```
$Disk = Get-AzDisk -ResourceGroupName $DiskResourceGroup -DiskName $DiskName
$SnapshotConfig = New-AzSnapshotConfig -SourceUri $Disk.Id -CreateOption Copy -Location
'dbelocal'
$Snapshot = New-AzSnapshot -Snapshot $SnapshotConfig -SnapshotName $SnapshotName -
ResourceGroupName $DestinationRG
```

Verify that the snapshot is created in the destination resource group.

```
Get-AzSnapshot -ResourceGroupName $DestinationRG
```

Here is an example output:

```

PS C:\Users\user> $DiskResourceGroup = "myaserg"
PS C:\Users\user> $DiskName = "myazdisk1"
PS C:\Users\user> $SnapshotName = "myasdisk1ss"
PS C:\Users\user> $DestinationRG = "myaseazrg1"
PS C:\Users\user> $Disk = Get-AzDisk -ResourceGroupName $DiskResourceGroup -DiskName $DiskName
PS C:\Users\user> $SnapshotConfig = New-AzSnapshotConfig -SourceUri $Disk.Id -CreateOption
Copy -Location 'dbelocal'
PS C:\Users\user> $Snapshot=New-AzSnapshot -Snapshot $SnapshotConfig -SnapshotName
$SnapshotName -ResourceGroupName $DestinationRG
PS C:\Users\user> Get-AzSnapshot -ResourceGroupName $DestinationRG

ResourceGroupName      : myaseazrg1
ManagedBy              :
Sku                   : Microsoft.Azure.Management.Compute.Models.SnapshotSku
TimeCreated            : 6/28/2021 6:57:40 PM
OsType                :
HyperVGeneration      :
CreationData           : Microsoft.Azure.Management.Compute.Models.CreationDat
                        a
DiskSizeGB             : 10
DiskSizeBytes          : 10737418240
UniqueId               : fbc1cfac-8bbb-44d8-8aa4-9e8811950fcc
EncryptionSettingsCollection :
ProvisioningState       : Succeeded
Incremental             : False
Encryption              : Microsoft.Azure.Management.Compute.Models.Encryption
Id                     : /subscriptions/.../r
                        esourceGroups/myaseazrg1/providers/Microsoft.Compute/
                        snapshots/myasdisk1ss
Name                  : myasdisk1ss
Type                  : Microsoft.Compute/snapshots
Location              : DBELocal
Tags                  : {}

PS C:\Users\user>

```

Copy the snapshot into a local storage account

Copy the snapshots to a local storage account on your device.

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```

$StorageAccountRG = <Local storage account resource group>
$StorageAccountName = <Storage account name>
$StorageEndpointSuffix = <Connection string in format: DeviceName.DnsDomain.com>
$DestStorageContainer = <Destination storage container>
$DestFileName = <Blob file name>

```

2. Create a local storage account on your device.

```

New-AzStorageAccount -Name $StorageAccountName -ResourceGroupName $StorageAccountRG -Location
DBELocal -SkuName Standard_LRS

```

Here is an example output:

```
PS C:\Users\user> New-AzStorageAccount -Name $StorageAccountName -ResourceGroupName  
$StorageAccountRG -Location DBELocal -SkuName Standard_LRS  
  
StorageAccountName ResourceGroupName PrimaryLocation SkuName      Kind     AccessTier  
----- ----- ----- -----  
myaseazsa1      myaseazrg2      DBELocal      Standard_LRS Storage  
PS C:\Users\user>
```

3. Create a container in the local storage account that you created.

```
$keys = Get-AzStorageAccountKey -ResourceGroupName $StorageAccountRG -Name $StorageAccountName  
$keyValue = $keys[0].Value  
$storageContext = New-AzStorageContext -StorageAccountName $StorageAccountName -StorageAccountKey  
$keyValue -Protocol Http -Endpoint $StorageEndpointSuffix;  
$container = New-AzStorageContainer -Name $DestStorageContainer -Context $storageContext -Permission  
Container -ErrorAction Ignore;
```

Here is an example output:

```

PS C:\Users\user> $StorageAccountRG = "myaseazrg2"
PS C:\Users\user> $StorageAccountName = "myaseazsa1"
PS C:\Users\user> $StorageEndpointSuffix = "myasegpu.wdshcsso.com"
PS C:\Users\user> $DestStorageContainer = "testcont1"
PS C:\Users\user> $DestFileName = "testfile1"

PS C:\Users\user> $keys = Get-AzStorageAccountKey -ResourceGroupName $StorageAccountRG -Name
$StorageAccountName
PS C:\Users\user> $keyValue = $keys[0].Value
PS C:\Users\user> $storageContext = New-AzStorageContext -StorageAccountName $StorageAccountName -
StorageAccountKey $keyValue -Protocol Http -Endpoint $StorageEndpointSuffix;
PS C:\Users\user> $storagecontext

StorageAccountName : myaseazsa1
BlobEndPoint : http://myaseazsa1.blob.myasegpu.wdshcsso.com/
TableEndPoint : http://myaseazsa1.table.myasegpu.wdshcsso.com/
QueueEndPoint : http://myaseazsa1.queue.myasegpu.wdshcsso.com/
FileEndPoint : http://myaseazsa1.file.myasegpu.wdshcsso.com/
Context : Microsoft.WindowsAzure.Commands.Storage.AzureStorageContext
Name :
StorageAccount : BlobEndpoint=http://myaseazsa1.blob.myasegpu.wdshcsso.com/;Que
ueEndpoint=http://myaseazsa1.queue.myasegpu.wdshcsso.com/;Tabl
eEndpoint=http://myaseazsa1.table.myasegpu.wdshcsso.com/;FileE
ndpoint=http://myaseazsa1.file.myasegpu.wdshcsso.com/;AccountN
ame=myaseazsa1;AccountKey=[key hidden]
TableStorageAccount : BlobEndpoint=http://myaseazsa1.blob.myasegpu.wdshcsso.com/;Que
ueEndpoint=http://myaseazsa1.queue.myasegpu.wdshcsso.com/;Tabl
eEndpoint=http://myaseazsa1.table.myasegpu.wdshcsso.com/;FileE
ndpoint=http://myaseazsa1.file.myasegpu.wdshcsso.com/;DefaultE
ndpointsProtocol=https;AccountName=myaseazsa1;AccountKey=[key
hidden]
Track20authToken :
EndPointSuffix : myasegpu.wdshcsso.com/
ConnectionString : BlobEndpoint=http://myaseazsa1.blob.myasegpu.wdshcsso.com/;Que
ueEndpoint=http://myaseazsa1.queue.myasegpu.wdshcsso.com/;Tabl
eEndpoint=http://myaseazsa1.table.myasegpu.wdshcsso.com/;FileE
ndpoint=http://myaseazsa1.file.myasegpu.wdshcsso.com/;AccountN
ame=myaseazsa1;AccountKey=itOn5Awjh3hnoGKL7EDQ681zhIKG/szCt05Z
IWAxP/T22gwExb5l0sKjI833Hqpc0MsBiSH2rM6NuwnJyEO1Q==
ExtendedProperties : {}

```

```

PS C:\Users\user> $container = New-AzStorageContainer -Name $DestStorageContainer -Context
$storageContext -Permission Container -ErrorAction Ignore;
PS C:\Users\user> $container
Blob End Point: http://myaseazsa1.blob.myasegpu.wdshcsso.com/

```

Name	PublicAccess	LastModified
---	-----	-----
testcont1	Container	6/28/2021 2:46:03 PM +00:00

```
PS C:\Users\user>
```

You can also use Azure Storage Explorer to [Create a local storage account](#) and then [Create a container in the local storage account](#) on your device.

4. Download the snapshot into the local storage account.

```
$sassnapshot = Grant-AzSnapshotAccess -ResourceGroupName $DestinationRG -SnapshotName $SnapshotName -  
Access 'Read' -DurationInSecond 3600  
$destContext = New-AzStorageContext -StorageAccountName $StorageAccountName -StorageAccountKey  
$keyValue  
Start-AzStorageBlobCopy -AbsoluteUri $sassnapshot.AccessSAS -DestContainer $DestStorageContainer -  
DestContext $destContext -DestBlob $DestFileName
```

Here is an example output:

```
PS C:\Users\user> $sassnapshot  
  
AccessSAS : https://md-2.blob.myasegpu.wdshcsso.com/22615edc48654bb8b77e383d3a7649ac  
/abcd.vhd?sv=2017-04-17&sr=b&si=43ca8395-6942-496b-92d7-f0d6dc68ab63&sk=system-1&sig  
=K%2Bc34uq7%2BLcTetG%2Bj9lo0H440e03vDkD24Ug0Gf%2Bex8%3D  
  
PS C:\Users\user> $destContext = New-AzStorageContext -StorageAccountName $StorageAccountName -  
StorageAccountKey $keyValue  
PS C:\Users\user> $destContext  
  
StorageAccountName : myaseazsa1  
BlobEndPoint : https://myaseazsa1.blob.myasegpu.wdshcsso.com/  
TableEndPoint : https://myaseazsa1.table.myasegpu.wdshcsso.com/  
QueueEndPoint : https://myaseazsa1.queue.myasegpu.wdshcsso.com/  
FileEndPoint : https://myaseazsa1.file.myasegpu.wdshcsso.com/  
Context : Microsoft.WindowsAzure.Commands.Storage.AzureStorageContext  
Name :  
StorageAccount : BlobEndpoint=https://myaseazsa1.blob.myasegpu.wdshcsso.com/;Qu  
eueEndpoint=https://myaseazsa1.queue.myasegpu.wdshcsso.com/;Ta  
bleEndpoint=https://myaseazsa1.table.myasegpu.wdshcsso.com/;Fi  
leEndpoint=https://myaseazsa1.file.myasegpu.wdshcsso.com/;Acco  
untName=myaseazsa1;AccountKey=[key hidden]  
TableStorageAccount : BlobEndpoint=https://myaseazsa1.blob.myasegpu.wdshcsso.com/;Qu  
eueEndpoint=https://myaseazsa1.queue.myasegpu.wdshcsso.com/;Ta  
bleEndpoint=https://myaseazsa1.table.myasegpu.wdshcsso.com/;Fi  
leEndpoint=https://myaseazsa1.file.myasegpu.wdshcsso.com/;Defa  
ultEndpointsProtocol=https;AccountName=myaseazsa1;AccountKey=[  
key hidden]  
Track20authToken :  
EndPointSuffix : myasegpu.wdshcsso.com/  
ConnectionString : BlobEndpoint=https://myaseazsa1.blob.myasegpu.wdshcsso.com/;Qu  
eueEndpoint=https://myaseazsa1.queue.myasegpu.wdshcsso.com/;Ta  
bleEndpoint=https://myaseazsa1.table.myasegpu.wdshcsso.com/;Fi  
leEndpoint=https://myaseazsa1.file.myasegpu.wdshcsso.com/;Acco  
untName=myaseazsa1;AccountKey=itOn5Awjh3hnoGKL7EDQ681zhIKG/szC  
t05ZIWAXp/T22gwExb5l0sKjI833Hqpc0MsBiSH2rM6NuwnJyE01Q==  
ExtendedProperties : {}  
  
PS C:\Users\user> Start-AzStorageBlobCopy -AbsoluteUri $sassnapshot.AccessSAS -DestContainer  
$DestStorageContainer -DestContext $destContext -DestBlob $DestFileName  
  
AccountName: myaseazsa1, ContainerName: testcont1  
  
Name BlobType Length ContentType LastMo  
----- ----- -----  
testfile1 BlockBlob -1 dified  
-----  
202...  
  
PS C:\Users\user>
```

You can also use Storage Explorer to verify that the snapshot was copied correctly to the storage account.

The screenshot shows the Azure Storage Explorer interface. On the left, the 'EXPLORER' sidebar lists 'Storage Accounts' and 'Local & Attached' sections. Under 'Storage Accounts', there are several entries like '(Attached Containers)', '(Emulator - Default Ports) (Key)', 'aseaccount (Key)', etc. A specific container named 'testcont1' is selected and highlighted with a red box. Inside 'testcont1', there are 'File Shares', 'Queues', 'Tables', and a 'Blob Containers' section. Under 'Blob Containers', a file named 'testfile1' is listed in a table. The table columns are 'Name', 'Access Tier', 'Access Tier Last Modified', 'Last Modified', 'Blob Type', 'Content Type', 'Size', and 'Status'. The 'testfile1' row is also highlighted with a red box. The top navigation bar includes 'Upload' (which is highlighted), 'Download', 'Open', 'New Folder', 'Copy URL', 'Select All', 'Copy', 'Paste', 'Rename', 'Delete', 'Undelete', and 'More'.

Download VHD to external target

To move your backups to an external location, you can use Azure Storage Explorer or AzCopy.

- Use the following AzCopy command to download VHD to an external target.

```
azcopy copy "https://<local storage account name>.blob.<device name>.<DNS domain>/<container name>/<filename><SAS query string>" <destination target>
```

- To set up and use Azure Storage Explorer with Azure Stack Edge, see the instructions in [Use Storage Explorer for upload](#).

Next steps

[Deploy virtual machines on your Azure Stack Edge Pro GPU device using templates.](#)

Monitor VM metrics for CPU, memory on Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to monitor CPU and memory metrics for a virtual machine on your Azure Stack Edge Pro GPU device.

About VM metrics

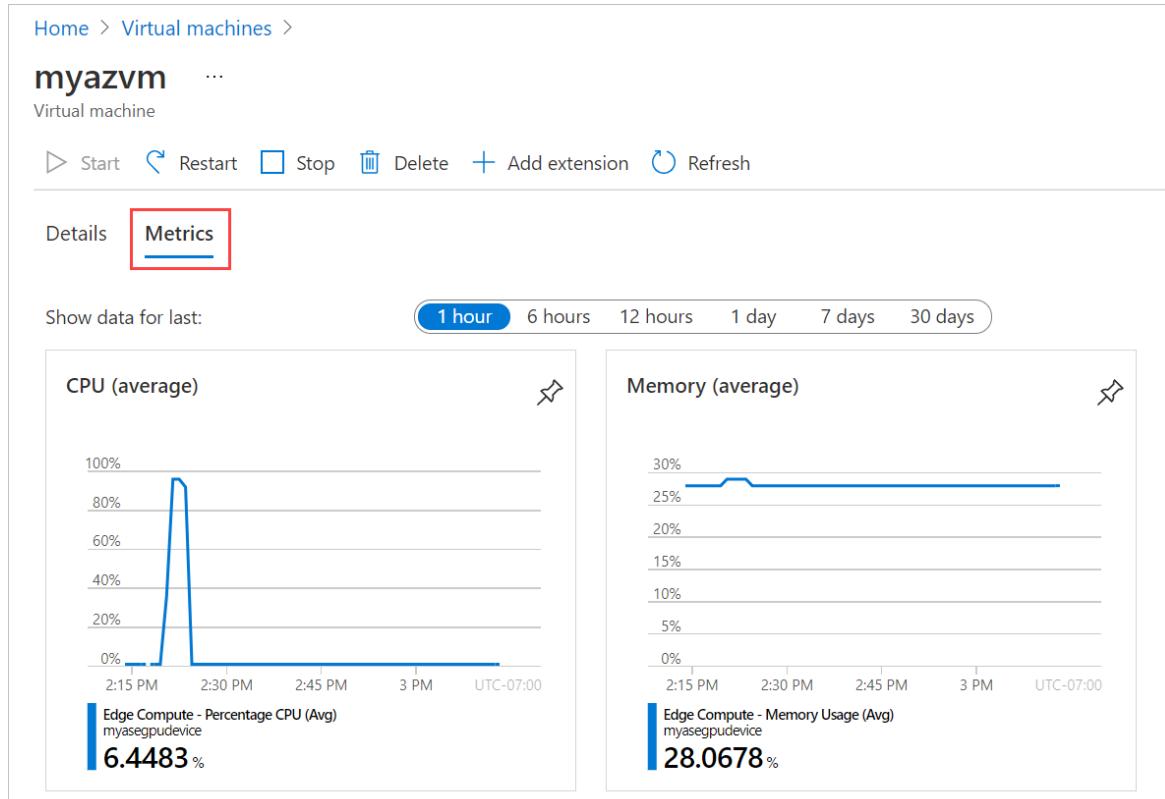
The **Metrics** tab for a virtual machine lets you view CPU and memory metrics, adjusting the time period and zooming in on periods of interest.

The VM metrics are based on CPU and memory usage data collected from the VM's guest operating system. Resource usage is sampled once per minute.

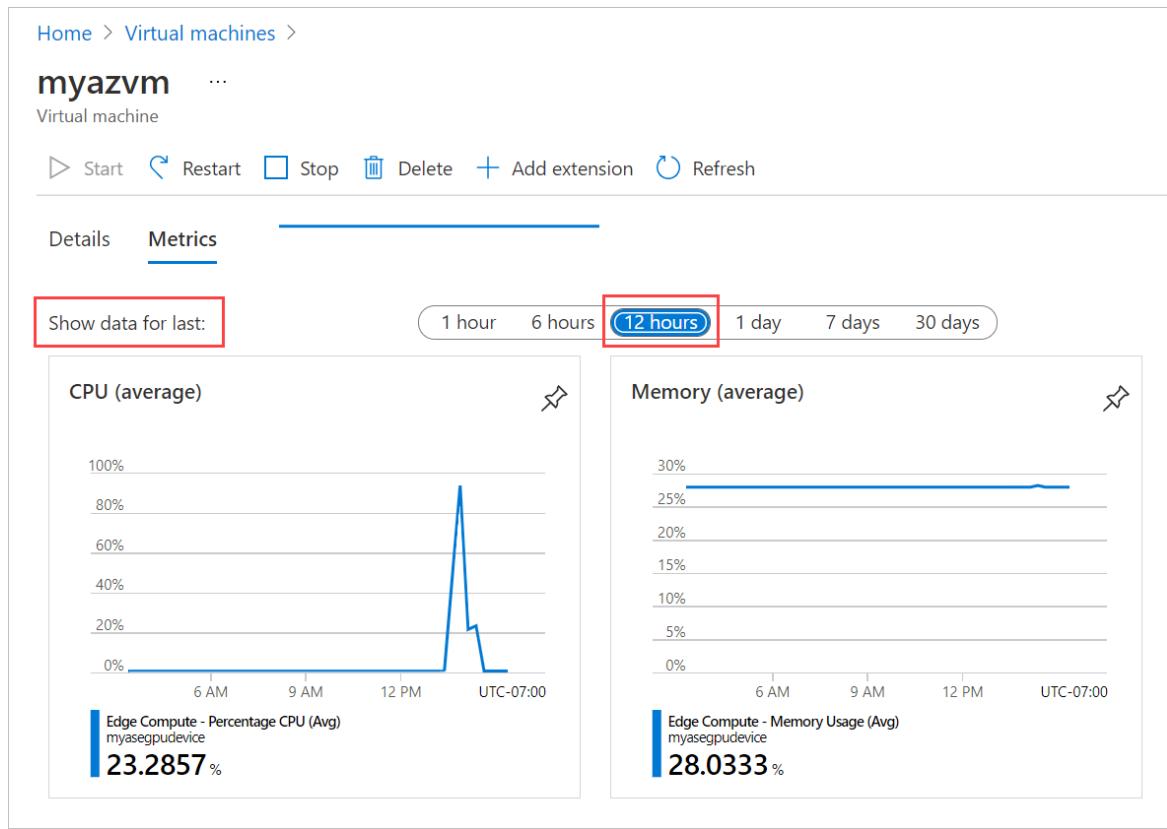
If a device is disconnected, metrics are cached on the device. When the device is reconnected, the metrics are pushed from the cache, and the VM **Metrics** are updated.

Monitor CPU and memory metrics

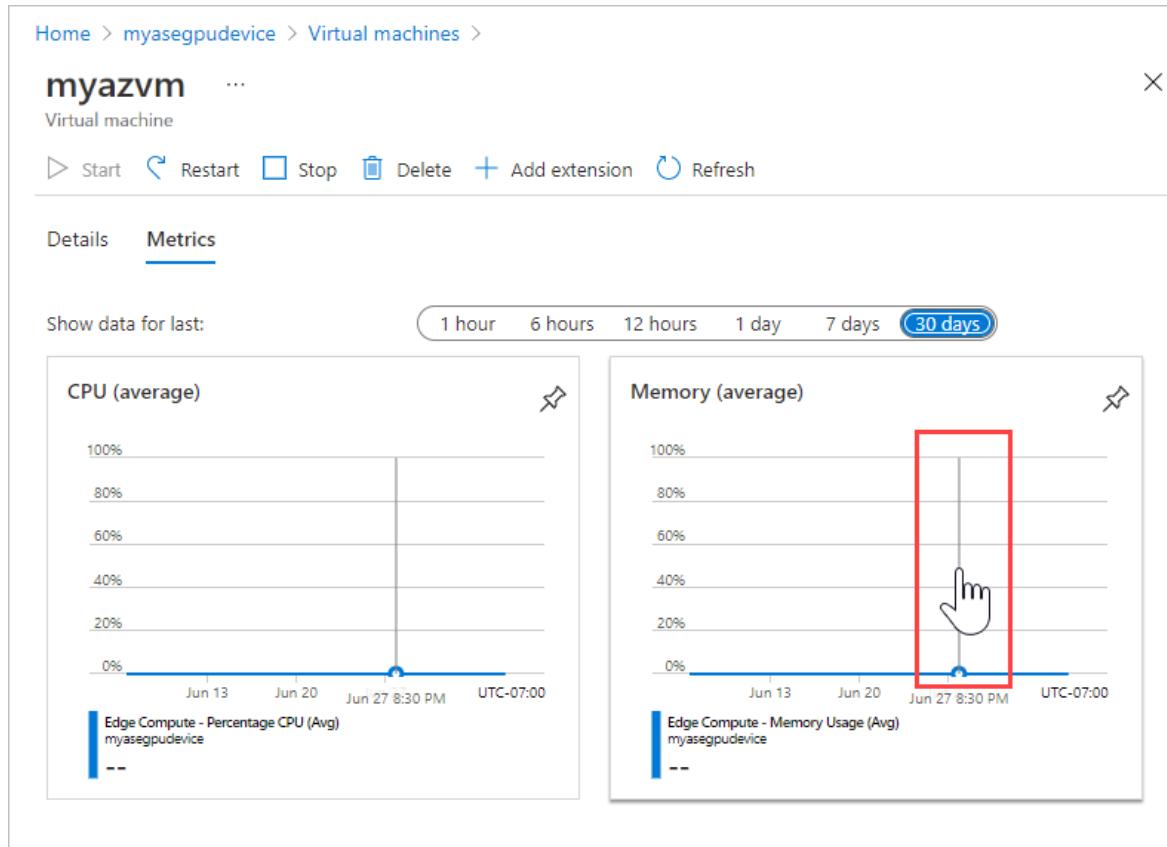
1. Open the device in the Azure portal, and go to **Virtual Machines**. Select the virtual machine, and select **Metrics**.



2. By default, the graphs show average CPU and memory usage for the previous hour. To see data for a different time period, select a different option beside **Show data for last**.



- Point anywhere in either chart with your mouse to display a vertical line with a hand that you can move left or right to view an earlier or later data sample. Click to open a detail view for that time period.



Next steps

- Monitor VM activity on your device.
- Collect VM guest logs in a Support package.

Monitor VM activity on your Azure Stack Edge Pro GPU device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to view activity logs in the Azure portal for virtual machines on your Azure Stack Edge Pro GPU device.

NOTE

You can zoom in on a VM's CPU and memory usage during periods of activity on the **Metrics** tab for the virtual machine. For more information, see [Monitor VM metrics](#).

View activity logs

To view activity logs for the virtual machines on your Azure Stack Edge Pro GPU device, do these steps:

1. Go to the device and then to **Virtual Machines**. Select **Activity log**.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> Write Deployments	Succeeded	10 minutes ...	Thu May 27...	Edge Gateway Test	hardsing@microsoft.com
> Delete Deployments	Succeeded	19 minutes ...	Thu May 27...	Edge Gateway Test	gyanb@microsoft.com
> Delete VirtualMachines	Failed	19 minutes ...	Thu May 27...	Edge Gateway Test	gyanb@microsoft.com
> Delete VirtualMachines	Failed	21 minutes ...	Thu May 27...	Edge Gateway Test	gyanb@microsoft.com
> Write VirtualMachines	Failed	7 hours ago	Thu May 27...	Edge Gateway Test	hardsing@microsoft.com
> Write VirtualMachines	Failed	7 hours ago	Thu May 27...	Edge Gateway Test	hardsing@microsoft.com
> Write Disks	Succeeded	7 hours ago	Thu May 27...	Edge Gateway Test	hardsing@microsoft.com
> Write Disks	Succeeded	7 hours ago	Thu May 27...	Edge Gateway Test	hardsing@microsoft.com

You'll see the VM guest logs for virtual machines on the device.

2. Use filters above the list to target the activity you need to see.

Timespan

Last 1 hour

Last 6 hours

Last 24 hours

Last week

Last 2 weeks

Last month

Custom

Apply **Cancel**

3. Click the down arrow by an operation name to view the associated activity.

Home > PortalPhysicalDevice5 > Virtual machines

Virtual machines | Activity log PREVIEW

Activity Overview Diagnostics settings Download as CSV Logs Pin current filters Reset filters

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Write Deployments	Succeeded	10 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Write Deployments	Started	16 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Write Deployments	Started	16 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Delete Deployments	Succeeded	19 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Delete VirtualMachines	Failed	19 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Delete VirtualMachines	Started	19 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Delete VirtualMachines	Accepted	19 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com
Delete VirtualMachines	Accepted	19 minutes ...	Thu May 27...	mySubscription	gusp@contoso.com

Activity log Images Virtual machines Resources Deployments

The screenshot shows the Azure portal's Activity log for a specific resource group. The left sidebar has 'Virtual machines' selected. The main area displays activity logs for operations like 'Write Deployments' and 'Delete VirtualMachines'. A red box highlights the 'Delete VirtualMachines' section, showing five entries. The first entry failed, while the others were accepted.

On any **Activity log** pane in Azure, you can filter and sort activities, select columns to display, drill down to details for a specific activity, and get **Quick Insights** into errors, failed deployments, alerts, service health, and security changes over the last 24 hours. For more information about the logs and the filtering options, see [View activity logs](#).

Next steps

- [Troubleshoot VM deployment](#).
- [Collect VM guest logs in a Support package](#).

Connect to a virtual machine console on an Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Azure Stack Edge Pro GPU solution runs non-containerized workloads via the virtual machines. This article describes how to connect to the console of a virtual machine deployed on your device.

The virtual machine console allows you to access your VMs with keyboard, mouse, and screen features using the commonly available remote desktop tools. You can access the console and troubleshoot any issues experienced when deploying a virtual machine on your device. You can connect to the virtual machine console even if your VM has failed to provision.

Workflow

The high-level workflow has the following steps:

1. Connect to the PowerShell interface on your device.
2. Enable console access to the VM.
3. Connect to the VM using remote desktop protocol (RDP).
4. Revoke console access to the VM.

Prerequisites

Before you begin, make sure that you have completed the following prerequisites:

For your device

You should have access to an Azure Stack Edge Pro GPU device that is activated. The device must have one or more VMs deployed on it. You can deploy VMs via Azure PowerShell, via the templates, or via the Azure portal.

For client accessing the device

Make sure that you have access to a client system that:

- Can access the PowerShell interface of the device. The client is running a [Supported operating system](#).
- The client is running PowerShell 7.0 or later. This version of PowerShell works for Windows, Mac, and Linux clients. See instructions to [install PowerShell 7](#).
- Has remote desktop capabilities. Depending on whether you are using Windows, macOS, or Linux, you should install one of these [Remote desktop clients](#). This article provides instructions with [Windows Remote Desktop](#) and [FreeRDP](#).

Connect to VM console

Follow these steps to connect to the virtual machine console on your device.

Connect to the PowerShell interface on your device

The first step is to [Connect to the PowerShell interface](#) of your device.

Enable console access to the VM

1. In the PowerShell interface, run the following command to enable access to the VM console.

```
Grant-HcsVMConnectAccess -ResourceGroupName <VM resource group> -VirtualMachineName <VM name>
```

2. In the sample output, make a note of the virtual machine ID. You'll need this for a later step.

```
[10.100.10.10]: PS>Grant-HcsVMConnectAccess -ResourceGroupName mywindowsvm1rg -VirtualMachineName mywindowsvm1  
VirtualMachineId      : 81462e0a-decb-4cd4-96e9-057094040063  
VirtualMachineHostName : 3V78B03  
ResourceGroupName      : mywindowsvm1rg  
VirtualMachineName     : mywindowsvm1  
Id                   : 81462e0a-decb-4cd4-96e9-057094040063  
[10.100.10.10]: PS>
```

Connect to the VM

You can now use a Remote Desktop client to connect to the virtual machine console.

Use Windows Remote Desktop

1. Create a new text file and input the following text.

```
pcb:s:<VM ID from PowerShell>;EnhancedMode=0  
full address:s:<IP address of the device>  
server port:i:2179  
username:s:EdgeARMUser  
negotiate security layer:i:0
```

2. Save the file as *.rdp on your client system. You'll use this profile to connect to the VM.

3. Double-click the profile to connect to the VM. Provide the following credentials:

- **Username:** Sign in as EdgeARMUser.
- **Password:** Provide the local Azure Resource Manager password for your device. If you have forgotten the password, [Reset Azure Resource Manager password via the Azure portal](#).

Use FreeRDP

If using FreeRDP on your Linux client, run the following command:

```
./wfreerdp /u:EdgeARMUser /vmconnect:<VM ID from PowerShell> /v:<IP address of the device>
```

Revoke VM console access

To revoke access to the VM console, return to the PowerShell interface of your device. Run the following command:

```
Revoke-HcsVMConnectAccess -ResourceGroupName <VM resource group> -VirtualMachineName <VM name>
```

Here is an example output:

```
[10.100.10.10]: PS>Revoke-HcsVMConnectAccess -ResourceGroupName mywindowsvm1rg -VirtualMachineName mywindowsvm1

VirtualMachineId      : 81462e0a-decb-4cd4-96e9-057094040063
VirtualMachineHostName : 3V78B03
ResourceGroupName      : mywindowsvm1rg
VirtualMachineName     : mywindowsvm1
Id                     : 81462e0a-decb-4cd4-96e9-057094040063

[10.100.10.10]: PS>
```

NOTE

We recommend that after you are done using the VM console, you either revoke the access or close the PowerShell window to exit the session.

Next steps

- Troubleshoot [VM deployments](#) in Azure portal.

Collect VM guest logs on an Azure Stack Edge Pro GPU device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

To diagnose any VM provisioning failure on your Azure Stack Edge Pro GPU device, you'll review guest logs for the failed virtual machine. This article describes how to collect guest logs for the VMs in a Support package.

NOTE

You can also monitor activity logs for virtual machines in the Azure portal. For more information, see [Monitor VM activity on your device](#).

Collect VM guest logs in Support package

To collect guest logs for failed virtual machines on an Azure Stack Edge Pro GPU device, do these steps:

1. [Connect to the PowerShell interface of your device](#).
2. Collect in-guest logs for failed VMs, and include these logs in a support package, by running the following commands:

```
Get-VMInGuestLogs -FailedVM  
Get-HcsNodeSupportPackage -Path "\\\<network path>" -Include InGuestVMLogFiles -Credential  
"domain_name\user"
```

You'll find the logs in the `hcslogs\VmGuestLogs` folder.

3. To get VM provisioning history details, review the following logs:

Linux VMs:

- `/var/log/cloud-init-output.log`
- `/var/log/cloud-init.log`
- `/var/log/waagent.log`

Windows VMs:

- `C:\Windows\Azure\Panther\WaSetup.xml`

Next steps

- [Monitor the VM activity log](#).
- [Troubleshoot VM provisioning on Azure Stack Edge Pro GPU](#).

Troubleshoot virtual machine image uploads in Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot issues that occur when downloading and managing virtual machine (VM) images on an Azure Stack Edge Pro GPU device.

Unable to add VM image to blob container

Error Description: In the Azure portal, when trying to upload a VM image to a blob container, the **Add** button isn't available, and the image can't be uploaded. The **Add** button isn't available when you don't have the required contributor role permissions to the resource group or subscription for the device.

Suggested solution: Make sure you have the required contributor permissions to add files to the resource group or storage account. For more information, see [Prerequisites for the Azure Stack Edge resource](#).

Invalid blob type for the source blob URI

Error Description: A VHD stored as a block blob cannot be downloaded. To be downloaded, a VHD must be stored as a page blob.

Suggested solution: Upload the VHD to the Azure Storage account as a page blob. Then download the blob. For upload instructions, see [Use Storage Explorer for upload](#).

Only blobs formatted as VHDs can be imported

Error Description: The VHD can't be imported because it doesn't meet formatting requirements. To be imported, a virtual hard disk must be a fixed-size, Generation 1 VHD.

Suggested solutions:

- Follow the steps in [Prepare generalized image from Windows VHD to deploy VMs on Azure Stack Edge Pro GPU](#) to create a fixed-size VHD for a Generation 1 virtual machine from your source VHD or VHDX.
- If you prefer to use PowerShell:
 - You can use [Convert-VHD](#) in the Windows PowerShell module for Hyper-V. You can't use Convert-VHD to convert a VM image from a Generation 2 VM to Generation 1; instead, use the portal procedures in [Prepare generalized image from Windows VHD to deploy VMs on Azure Stack Edge Pro GPU](#).
 - If you need to find out the current VHD type, use [Get-VHD](#).

The condition specified using HTTP conditional header(s) is not met

Error Description: If any changes are being made to a VHD when you try to download it from Azure, the download will fail because the VHD in Azure won't match the VHD being downloaded. This error also occurs when a download is attempted before the upload of the VHD to Azure has completed.

Suggested solution: Wait until the upload of the VHD has completed and no changes are being made to the VHD. Then try downloading the VHD again.

Next steps

- Learn how to [Deploy VMs via the Azure portal](#).
- Learn how to [Deploy VMs via Azure PowerShell](#).

Troubleshoot VM deployment in Azure Stack Edge Pro GPU

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot common errors when deploying virtual machines on an Azure Stack Edge Pro GPU device. The article provides guidance for investigating the most common issues that cause VM provisioning timeouts and issues during network interface and VM creation.

To diagnose any VM provisioning failure, you'll review guest logs for the failed virtual machine. For steps to collect VM guest logs and include them in a Support package, see [Collect guest logs for VMs on Azure Stack Edge Pro](#).

For guidance on issues that prevent successful upload of a VM image before your VM deployment, see [Troubleshoot virtual machine image uploads in Azure Stack Edge Pro GPU](#).

VM provisioning timeout

This section provides troubleshooting for most common causes of a VM provisioning timeout.

When VM provisioning times out, you see the following error:

X Creation of virtual machine failed.

Possible Causes

- DeploymentFailed : At least one resource deployment operation failed. Please list deployment operations for details. Please see <https://aka.ms/DeployOperations> for usage details.
- Conflict : {
"status": "Failed",
"error": {
"code": "ResourceDeploymentFailure",
"message": "The resource operation completed with terminal provisioning state 'Failed'.",
"details": [
{
"code": "VmProvisioningTimeout",
"message": "VM 'WindowsVM1' failed to provision with timeout. ."
}
]
}
}

The following issues are the top causes of VM provisioning timeouts:

- The IP address that you assigned to the VM is already in use. [Learn more](#)
 - The VM image that you used to deploy the VM wasn't prepared correctly. [Learn more](#)
 - The default gateway and DNS server couldn't be reached from the guest VM. [Learn more](#)
 - During a `cloud init` installation, `cloud init` either didn't run or there were issues while it was running. (Linux VMs only) [Learn more](#)
 - For a Linux VM deployed using a custom VM image, the Provisioning flags in the `/etc/waagent.conf` file are not correct. (Linux VMs only) [Learn more](#)

IP assigned to the VM is already in use

Error description: The VM was assigned a static IP address that is already in use, and VM provisioning failed. This error happens when the IP address is in use in the subnet on which the VM is deployed. When you deploy a VM via the Azure portal, the process checks for an existing IP address within your device but can't check IP addresses of other services or virtual machines that might also be on your subnet.

Suggested solution: Use a static IP address that is not in use, or use a dynamic IP address provided by the

DHCP server.

To check for a duplicate IP address:

- Run the following `ping` and `Test-NetConnection` (`tnc`) commands from any appliance on the same network:

```
ping <IP address>
tnc <IP address>
tnc <IP address> -CommonTCPPort "RDP"
```

If you get a response, the IP address that you assigned to the new VM is already in use.

VM image not prepared correctly

Error description: To prepare a VM image for use on an Azure Stack Edge Pro GPU device, you must follow a specific workflow. You must create a gen1 virtual machine in Azure, customize the VM, generalize the VHD, and then download the OS VHD for that virtual machine. The prepared image must be a gen1 VHD with the "vhd" filename extension and the fixed type.

For an overview of requirements, see [Create custom VM images for an Azure Stack Edge Pro GPU device](#). For guidance on resolving VM image issues, see [Troubleshoot virtual machine image uploads in Azure Stack Edge Pro GPU](#).

Suggested solution: Complete the workflow for preparing your VM image. For guidance, see one of the following articles:

- [Custom VM image workflows for Windows and Linux VMs](#)
- [Prepare a generalized image from a Windows VHD](#)
- [Prepare a generalized image using an ISO](#)
- [Use a specialized image to deploy VMs](#)

Gateway, DNS server couldn't be reached from guest VM

Error description: If the default gateway and DNS server can't be reached during VM deployment, VM provisioning will time out, and the VM deployment will fail.

Suggested solution: Verify that the default gateway and DNS server can be reached from the VM. Then repeat VM deployment.

To verify that the default gateway and DNS server can be reached from the VM, do the following steps:

- [Connect to the VM](#).
- Run the following commands:

```
ping <default gateway IP address>
ping <DNS server IP address>
```

To find out the IP addresses for the default gateway and DNS servers, go to the local UI for your device. Select the port you're interested in, and view the network settings.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. On the left, there's a sidebar with options like Overview, Configuration, Get started, Network (which is selected), Compute, Web proxy, Device, Update server, Time, Certificates, Cloud details, Maintenance, and Power. The main area has tabs for Network and Compute. Under Network, it shows 'Network interfaces' with a table for Port 1 through Port 6. Port 1 is set to 192.168.100.10 with subnet mask 255.255.255.0. Port 2 is set to 10.57.53.204 with subnet mask 255.255.248.0. Port 3 is set to 192.168.4.222 with subnet mask 255.255.0.0. Port 4 is set to 192.168.4.133 with subnet mask 255.255.0.0. Port 5 is set to 192.168.2.25 with subnet mask 255.255.0.0. Port 6 is set to 192.168.4.217 with subnet mask 255.255.0.0. To the right, a modal window titled 'Network settings (Port 2)' is open, showing 'IP settings' with 'Static' selected. It includes fields for Subnet mask (255.255.248.0), Gateway (10.57.48.1), Primary DNS (10.50.50.50), and Secondary DNS (10.50.10.50). At the bottom of the modal are buttons for Serial, IP address, MAC address, and Apply.

`cloud init` issues (Linux VMs)

Error description: `cloud init` did not run, or there were issues while `cloud init` was running. `cloud-init` is used to customize a Linux VM when the VM boots for the first time. For more information, see [cloud-init support for virtual machines in Azure](#).

Suggested solutions: To find issues that occurred when `cloud init` was run:

1. [Connect to the VM](#).
2. Check for `cloud init` errors in the following log files:
 - `/var/log/cloud-init-output.log`
 - `/var/log/cloud-init.log`
 - `/var/log/waagent/log`

To check for some of the most common issues that prevent `cloud init` from running successfully, do these steps:

1. Make sure the VM image is based on `cloud init`. Run the following command:

```
cloud-init --version
```

The command should return the cloud init version number. If the image is not `cloud init`-based, the command won't return version information.

To get help with `cloud init` options, run the following command:

```
cloud-init --help
```

2. Make sure the `cloud init` instance can run successfully with the data source set to *Azure*.

When the data source is set to *Azure*, the entry in the `cloud init` logs looks similar to the following one.

```
2021-02-02 02:44:29,521 - __init__.py[DEBUG]: Searching for local data source
in: ['DataSourceAzure']
2021-02-02 02:44:29,522 - handlers.py[DEBUG]: start: init-local/search-Azure:
searching for local data from DataSourceAzure
2021-02-02 02:44:29,522 - __init__.py[DEBUG]: Seeing if we can get any data from
<class 'cloudinit.sources.DataSourceAzure.DataSourceAzure'>
2021-02-02 02:44:29,522 - __init__.py[DEBUG]: Update datasource metadata and
network config due to events: New instance first boot
2021-02-02 02:44:29,522 - handlers.py[DEBUG]: start: azure-ds/_get_data:
_get_data
2021-02-02 02:44:29,522 - handlers.py[DEBUG]: start: azure-ds/check-platform-
viability: found azure asset tag
```

If the data source is not set to Azure, you may need to revise your `cloud init` script. For more information, see [Diving deeper into cloud-init](#).

Provisioning flags set incorrectly (Linux VMs)

Error description: To successfully deploy a Linux VM in Azure, provisioning must be disabled on the image, and provisioning using `cloud init` must be enabled. The Provisioning flags that set these values are configured correctly for standard VM images. If you use a custom VM image, you need to make sure they're correct.

Suggested solution: Make sure the Provisioning flags in the `/etc/waagent.conf` file have the following values:

CAPABILITY	REQUIRED VALUE
Enable provisioning	<code>Provisioning.Enabled=n</code>
Rely on cloud-init to provision	<code>Provisioning.UseCloudInit=y</code>

Network interface creation issues

This section provides guidance for issues that cause network interface creation to fail during a VM deployment.

NIC creation timeout

Error description: Creation of the network interface on the VM didn't complete within the allowed timeout period. This failure can be caused by DHCP server issues in your environment.

To verify whether the network interface was created successfully, do these steps:

1. In the Azure portal, go to the Azure Stack Edge resource for your device (go to **Edge Services > Virtual machines**). Then select **Deployments**, and navigate to the VM deployment.
2. If a network interface was not created successfully, you'll see the following error.

edge-ubuntu01

Refresh

✖ Your deployment failed

Resource	Type	Status
edge-ubuntu01-osdisk	Microsoft.Compute/disks	Completed
edge-ubuntu01nic	Microsoft.Network/networkInterfaces	Failed

✖ Creation of virtual machine failed.

Possible Causes

DeploymentFailed : At least one resource deployment operation failed. Please list deployment operations for details. Please see <https://aka.ms/DeployOperations> for usage details.

RequestTimeout : [

```
    "error": {  
        "code": "ResourceDeploymentFailure",  
        "message": "The resource provision operation did not complete within the allowed timeout period."  
    }  
]
```

Recommended Action

In the local web UI of the device, go to Troubleshooting > Diagnostic tests and click Run diagnostic tests. Resolve the reported issues. If the issue persists, contact [Microsoft Support](#).

Suggested solution: Create the VM again, and assign it a static IP address.

VM creation issues

This section covers common issues that occur during VM creation.

Not enough memory to create the VM

Error description: When VM creation fails because of insufficient memory, you'll see the following error.

✖ Creation of virtual machine failed.

Possible Causes

- DeploymentFailed : At least one resource deployment operation failed. Please list deployment operations for details. Please see <https://aka.ms/DeployOperations> for usage details.
- Conflict : [

```
    "status": "Failed",  
    "error": {  
        "code": "ResourceDeploymentFailure",  
        "message": "The resource operation completed with terminal provisioning state 'Failed'.",  
        "details": [  
            {  
                "code": "FabricVmPlacementErrorNotEnoughCapacity",  
                "message": "Failed to create VM 'vm4'"  
            }  
        ]  
    }  
}
```

Suggested solution: Check the available memory on the device, and choose the VM size accordingly. For more information, see [Supported virtual machine sizes on Azure Stack Edge](#).

The memory available for the deployment of a VM is constrained by several factors:

- The amount of available memory on the device. For more information, see compute and memory specifications in [Azure Stack Edge Pro GPU technical specifications](#) and [Azure Stack Edge Mini R technical specifications](#).
- If Kubernetes is enabled, the compute memory required for Kubernetes and apps on the Kubernetes cluster.
- The overhead for each virtual machine in Hyper-V.

Suggested solutions:

- Use a VM size that requires less memory.

- Stop any VMs that aren't in use from the portal before you deploy the new VM.
- Delete any VMs that are no longer in use.

Insufficient number of GPUs to create GPU VM

If you try to deploy a VM on a GPU device that already has Kubernetes enabled, no GPUs will be available, and VM provisioning will fail with the following error:

 Creation of virtual machine failed.

Possible Causes

- DeploymentFailed : At least one resource deployment operation failed. Please list deployment operations for details. Please see <https://aka.ms/DeployOperations> for usage details.
- Conflict : {
 "status": "Failed",
 "error": {
 "code": "ResourceDeploymentFailure",
 "message": "The resource operation completed with terminal provisioning state 'Failed'.",
 "details": [
 {
 "code": "FabricVmPlacementErrorInsufficientGpuCapacity",
 "message": "Failed to create VM 'GPUVM2'"
 }
]
 }
}

Possible causes: If Kubernetes is enabled before the VM is created, Kubernetes will use all the available GPUs, and you won't be able to create any GPU-size VMs. You can create as many GPU-size VMs as the number of available GPUs. Your Azure Stack Edge device can be equipped with 1 or 2 GPUs.

Suggested solution: For VM deployment options on a 1-GPU or 2-GPU device with Kubernetes configured, see [GPU VMs and Kubernetes](#).

Next steps

- [Collect a Support package that includes guest logs for a failed VM](#)
- [Troubleshoot issues with a failed GPU extension installation](#)
- [Troubleshoot issues with Azure Resource Manager](#)

Troubleshoot GPU extension issues for GPU VMs on Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

This article gives guidance for resolving the most common issues that cause installation of the GPU extension on a GPU VM to fail on an Azure Stack Edge Pro GPU device.

For installation steps, see [Install GPU extension](#).

In versions lower than 2205, Linux GPU extension installs old signing keys: signature and/or required key missing

Error description: The Linux GPU extension installs old signing keys, preventing download of the required GPU driver. In this case, you'll see the following error in the syslog of the Linux VM:

```
/var/log/syslog and /var/log/waagent.log
May 5 06:04:53 gpuvml2 kernel: [ 833.601805]nvidia:module verification failed: signature and/or required key
missing- tainting kernel
```

Suggested solutions: You have two options to mitigate this issue:

- **Option 1:** Apply the Azure Stack Edge 2205 updates to your device.
- **Option 2:** After creating a GPU virtual machine of size in NCasT4_v3-series, manually install the new signing keys before installing the extension, then set required signing keys using steps in [Updating the CUDA Linux GPG Repository Key | NVIDIA Technical Blog](#).

Here's an example that installs signing keys on an Ubuntu 1804 virtual machine:

```
$ sudo apt-key adv --fetch-
keys https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/3bf863cc.pub
```

Failure to install GPU extension on a Windows 2016 VHD

Error description: This is a known issue in versions lower than 2205. The GPU extension requires TLS 1.2. In this case, you may see the following error message:

```
Failed to download https://go.microsoft.com/fwlink/?linkid=871664 after 10 attempts. Exiting!
```

Additional details:

- Check the guest log for the associated error. To collect the guest logs, see [Collect guest logs for VMs on an Azure Stack Edge Pro GPU device](#).
- On a Linux VM, look in `/var/log/waagent.log` or `/var/log/azure/nvidia-vmext-status`.
- On a Windows VM, find the error status in `C:\Packages\Plugins\Microsoft.HpcCompute.NvidiaGpuDriverWindows\1.3.0.0>Status`.
- Review the complete execution log in `C:\WindowsAzure\Logs\WaAppAgent.txt`.

If the installation failed during the package download, that error indicates the VM couldn't access the public network to download the driver.

Suggested solution: Use the following steps to enable TLS 1.2 on a Windows 2016 VM, and then deploy the GPU extension.

1. Run the following command inside the VM to enable TLS 1.2:

```
sphklm:\SOFTWARE\Microsoft\NETFramework\v4.0.30319SchUseStrongCrypto1
```

2. Deploy the template `addGPUextensiontoVM.json` to install the extension on an existing VM. You can install the extension manually, or you can install the extension from the Azure portal.

- To install the extension manually, see [Install GPU extension on VMs for your Azure Stack Edge Pro GPU device](#)
- To install the template using the Azure portal, see [Deploy GPU VMs on your Azure Stack Edge Pro GPU device](#).

NOTE

The extension deployment is a long running job and takes about 10 minutes to complete.

Manually install the Nvidia driver on RHEL 7

Error description: When installing the GPU extension on an RHEL 7 VM, the installation may fail due to a certificate rotation issue and an incompatible driver version.

Suggested solution: In this case, you have two options:

- **Option 1:** Resolve the certificate rotation issue and then install an Nvidia driver lower than version 510.

1. To resolve the certificate rotation issue, run the following command:

```
$sudo yum-config-manager --add-repo  
https://developer.download.nvidia.com/compute/cuda/repos/rhel7/$arch/cuda-rhel7.repo
```

2. Install an Nvidia driver lower than version 510.

- **Option 2:** Deploy the GPU extension. Use the following settings when deploying the ARM extension:

```
settings": {  
  "isCustomInstall": true,  
  "InstallMethod": 0,  
  "DRIVER_URL": " https://developer.download.nvidia.com/compute/cuda/11.4.4/local_installers/cuda-repo-rhel7-11-4-local-11.4.4_470.82.01-1.x86_64.rpm",  
  "DKMS_URL" : " https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm",  
  "LIS_URL": " https://aka.ms/lis",  
  "LIS_RHEL_ver": "3.10.0-1062.9.1.el7"  
}
```

VM size is not GPU VM size

Error description: A GPU VM must be either Standard_NC4as_T4_v3 or Standard_NC8as_T4_v3 size. If any other VM size is used, the GPU extension will fail to be attached.

Suggested solution: Create a VM with the Standard_NC4as_T4_v3 or Standard_NC8as_T4_v3 VM size. For

more information, see [Supported VM sizes for GPU VMs](#). For information about specifying the size, see [Create GPU VMs](#).

Image OS is not supported

Error description: The GPU extension doesn't support the operating system that's installed on the VM image.

Suggested solution: Prepare a new VM image that has an operating system that the GPU extension supports.

- For a list of supported operating systems, see [Supported OS and GPU drivers for GPU VMs](#).
- For image preparation requirements for a GPU VM, see [Create GPU VMs](#).

Extension parameter is incorrect

Error description: Incorrect extension settings were used when deploying the GPU extension on a Linux VM.

Suggested solution: Edit the parameters file before deploying the GPU extension. For more information, see [Install GPU extension](#).

VM extension installation failed in downloading package

Error description: Extension provisioning failed during extension installation or while in the Enable state.

1. Check the guest log for the associated error. To collect the guest logs, see [Collect guest logs for VMs on an Azure Stack Edge Pro](#).

On a Linux VM:

- Look in `/var/log/waagent.log` or `/var/log/azure/nvidia-vmext-status`.

On a Windows VM:

- Find out the error status in `C:\Packages\Plugins\Microsoft.HpcCompute.NvidiaGpuDriverWindows\1.3.0.0>Status`.
- Review the complete execution log: `c:\WindowsAzure\Logs\WaAppAgent.txt`.

If installation failed during the package download, that error indicates the VM couldn't access the public network to download the driver.

Suggested solution:

1. Enable compute on a port that's connected to the Internet. For guidance, see [Create GPU VMs](#).
2. Deallocate the VM by stopping the VM in the portal. To stop the VM, go to **Virtual machines > Overview**, and select the VM. Then, on the VM properties page, select **Stop**.
3. Create a new VM.

VM Extension failed with error `dpkg is used/yum lock is used` (Linux VM)

Error description: GPU extension deployment on a Linux VM failed because another process was using `dpkg` or another process has created a `yum lock`.

Suggested solution: To resolve the issue, do these steps:

1. To find out what process is applying the lock, search the `\var\log\azure\nvidia-vmext-status` log for an error such as "dpkg is used by another process" or "Another app is holding `yum lock`".

2. Either wait for the process to finish, or end the process.
3. [Install the GPU extension](#) again.
4. If extension deployment fails again, create a new VM and make sure the lock isn't present before you install the GPU extension.

Next steps

[Collect guest logs, and create a Support package](#)

Kubernetes on your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

Kubernetes is a popular open-source platform to orchestrate containerized applications. This article provides an overview of Kubernetes and then describes how Kubernetes works on your Azure Stack Edge device.

About Kubernetes

Kubernetes provides an easy and reliable platform to manage container-based applications and their associated networking and storage components. You can rapidly build, deliver, and scale containerized apps with Kubernetes.

As an open platform, you can use Kubernetes to build applications with your preferred programming language, OS libraries, or messaging bus. To schedule and deploy releases, Kubernetes can integrate with existing continuous integration and continuous delivery tools.

For more information, see [How Kubernetes works](#).

Kubernetes on Azure Stack Edge

On your Azure Stack Edge device, you can create a Kubernetes cluster by configuring the compute. When the compute role is configured, the Kubernetes cluster including the master and worker nodes are all deployed and configured for you. This cluster is then used for workload deployment via `kubectl`, IoT Edge, or Azure Arc.

The Azure Stack Edge device is available as a 1-node configuration or a 2-node configuration (for Pro GPU model only) that constitutes the infrastructure cluster. The Kubernetes cluster is separate from the infrastructure cluster and is deployed on top of the infrastructure cluster. The infrastructure cluster provides the persistent storage for your Azure Stack Edge device while the Kubernetes cluster is responsible solely for application orchestration.

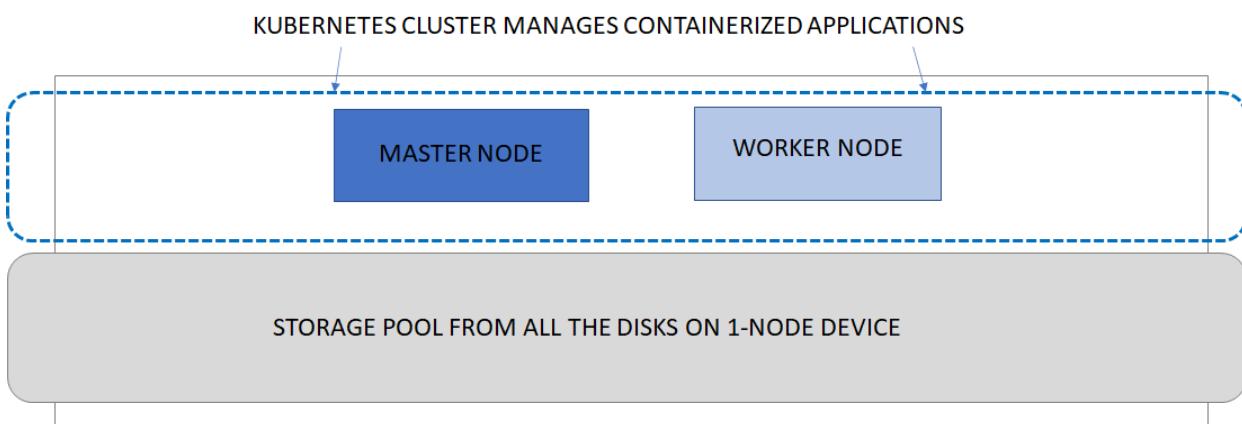
The Kubernetes cluster has master node and worker nodes. The Kubernetes nodes in a cluster are virtual machines that run your applications and cloud workflows.

The Kubernetes master node is responsible for maintaining the desired state for your cluster. The master node also controls the worker node which in turn runs the containerized applications.

Kubernetes cluster on single node device

The following diagram illustrates the implementation of Kubernetes on a 1-node Azure Stack Edge device. The 1-node device has one master node and one worker node. The 1-node device is not highly available and if the single node fails, the device goes down. The Kubernetes cluster also goes down.

KUBERNETES CLUSTER ON A 1-NODE AZURE STACK EDGE DEVICE



Kubernetes cluster on two-node device

The 2-node Azure Stack Edge device has one master node and two worker nodes. The 2-node device is highly available and if one of the node fails, the master node fails over to the other node. Both the device and the Kubernetes cluster keep running.

For more information on the Kubernetes cluster architecture, go to [Kubernetes core concepts](#).

Kubernetes compute requirements

The Kubernetes master and the worker nodes are virtual machines that consume CPU and memory. When deploying Kubernetes workloads, it is important to understand the compute requirements for the master and worker VMs.

KUBERNETES VM TYPE	CPU AND MEMORY REQUIREMENT
Master VM	4 cores, 4-GB RAM
Worker VM	12 cores, 32-GB RAM

Storage volume provisioning

To support application workloads, you can mount storage volumes for persistent data on your Azure Stack Edge device shares. Both static and dynamic volumes can be used.

For more information, see storage provisioning options for applications in [Kubernetes storage for your Azure Stack Edge device](#).

Networking

Kubernetes networking enables you to configure communication within your Kubernetes network including container-to-container networking, pod-to-pod networking, pod-to-service networking, and Internet-to-service networking. For more information, see the networking model in [Kubernetes networking for your Azure Stack Edge device](#).

Updates

As new Kubernetes versions become available, your cluster can be upgraded using the standard updates available for your Azure Stack Edge device. For steps on how to upgrade, see [Apply updates for your Azure Stack Edge](#).

Access, monitoring

The Kubernetes cluster on your Azure Stack Edge device allows Kubernetes role-based access control (Kubernetes RBAC). For more information, see [Kubernetes role-based access control on your Azure Stack Edge Pro GPU device](#).

You can also monitor the health of your cluster and resources via the Kubernetes dashboard. Container logs are also available. For more information, see [Use the Kubernetes dashboard to monitor the Kubernetes cluster health on your Azure Stack Edge device](#).

Azure Monitor is also available as an add-on to collect health data from containers, nodes, and controllers. For more information, see [Azure Monitor overview](#)

Edge container registry

Kubernetes on Azure Stack Edge device allows for the private storage of your images by providing a local container registry. For more information, see [Enable Edge container registry on your Azure Stack Edge Pro GPU device](#).

Application management

After a Kubernetes cluster is created on your Azure Stack Edge device, you can manage the applications deployed on this cluster via any of the following methods:

- Native access via `kubectl`
- IoT Edge
- Azure Arc

These methods are explained in the following sections.

Kubernetes and `kubectl`

Once the Kubernetes cluster is deployed, then you can manage the applications deployed on the cluster locally from a client machine. You use a native tool such as `kubectl` via the command line to interact with the applications.

For more information on deploying Kubernetes cluster, go to [Deploy a Kubernetes cluster on your Azure Stack Edge device](#). For information on management, go to [Use kubectl to manage Kubernetes cluster on your Azure Stack Edge device](#).

Kubernetes and IoT Edge

Kubernetes can also be integrated with IoT Edge workloads on Azure Stack Edge device where Kubernetes provides scale and the ecosystem and IoT provides the IoT centric ecosystem. The Kubernetes layer is used as an infrastructure layer to deploy Azure IoT Edge workloads. The module lifetime and network load balancing are managed by Kubernetes whereas the edge application platform is managed by IoT Edge.

For more information on deploying applications on your Kubernetes cluster via IoT Edge, go to:

- [Expose stateless applications on Azure Stack Edge device via IoT Edge](#).

Kubernetes and Azure Arc

Azure Arc is a hybrid management tool that will allow you to deploy applications on your Kubernetes clusters. Azure Arc also allows you to use Azure Monitor for containers to view and monitor your clusters. For more information, go to [What is Azure Arc-enabled Kubernetes?](#). For information on Azure Arc pricing, go to [Azure Arc pricing](#).

Beginning March 2021, Azure Arc-enabled Kubernetes will be generally available to the users and standard

usage charges apply. As a valued preview customer, the Azure Arc-enabled Kubernetes will be available to you at no charge for Azure Stack Edge device(s). To avail the preview offer, create a [Support request](#):

1. Under **Issue type**, select **Billing**.
2. Under **Subscription**, select your subscription.
3. Under **Service**, select **My services**, then select **Azure Stack Edge**.
4. Under **Resource**, select your resource.
5. Under **Summary**, type a description of your issue.
6. Under **Problem type**, select **Unexpected Charges**.
7. Under **Problem subtype**, select **Help me understand charges on my free trial**.

Next steps

- Learn more about Kubernetes storage on [Azure Stack Edge device](#).
- Understand the Kubernetes networking model on [Azure Stack Edge device](#).
- Deploy [Azure Stack Edge](#) in Azure portal.

Kubernetes storage management on your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

On your Azure Stack Edge Pro device, a Kubernetes cluster is created when you configure compute role. Once the Kubernetes cluster is created, then containerized applications can be deployed on the Kubernetes cluster in pods. There are distinct ways to provide storage to pods in your Kubernetes cluster.

This article describes the methods to provision storage on a Kubernetes cluster in general and specifically in the context of your Azure Stack Edge Pro device.

Storage requirements for Kubernetes pods

Kubernetes pods are stateless but the applications they run are usually stateful. Because pods can be short-lived, and they restart, fail over, or move between Kubernetes nodes, the following requirements must be met for storage associated with the pod.

The storage must:

- Live outside of the pod.
- Be independent of pod lifecycle.
- Be accessible from all the Kubernetes nodes.

To understand how storage is managed for Kubernetes, one needs to understand two API resources:

- **PersistentVolume (PV)**: This is a piece of storage in the Kubernetes cluster. Kubernetes storage can be statically provisioned as `PersistentVolume`. It can also be dynamically provisioned as `StorageClass`.
- **PersistentVolumeClaim (PVC)**: This is a request for storage by a user. PVCs consume PV resources. PVCs can request specific size and access modes.

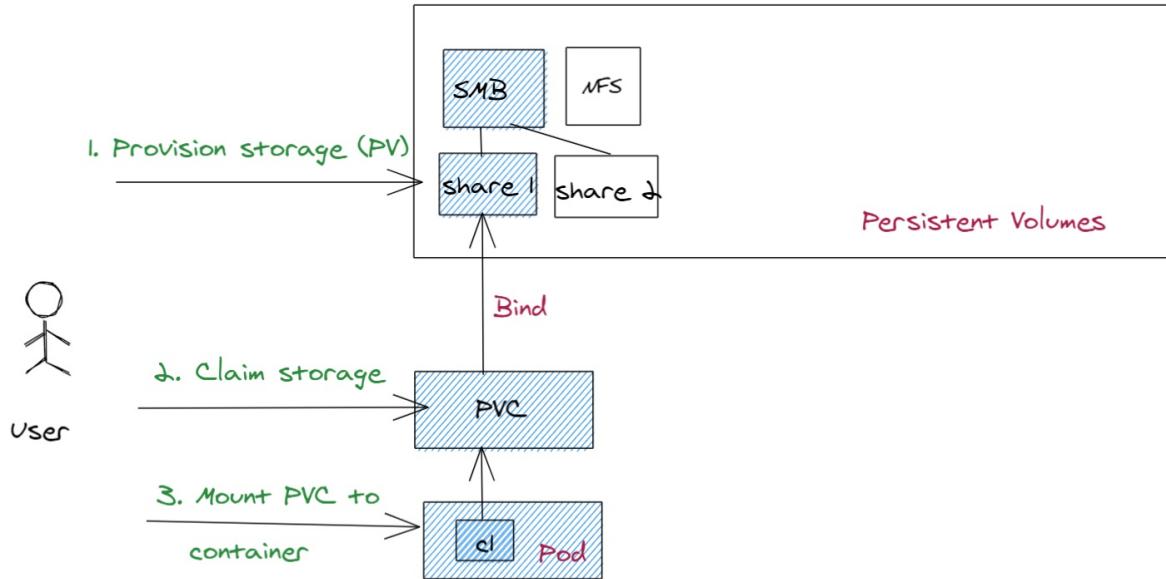
Because users need `PersistentVolumes` with varying properties for different problems, hence cluster admins need to be able to offer a variety of `PersistentVolumes` that differ in more ways than just size and access modes. For these needs, you need the `StorageClass` resource.

Storage provisioning can be static or dynamic. Each of the provisioning types is discussed in the following sections.

Static provisioning

Kubernetes cluster admins can statically provision the storage. To do so, they can use storage backend based on SMB/NFS filesystems or use iSCSI disks that attach locally over the network in an on-premises environment, or even use Azure Files or Azure Disks in the cloud. This type of storage is not provisioned by default and cluster admins have to plan and manage this provisioning.

Here is a diagram that depicts how statically provisioned storage is consumed in Kubernetes:

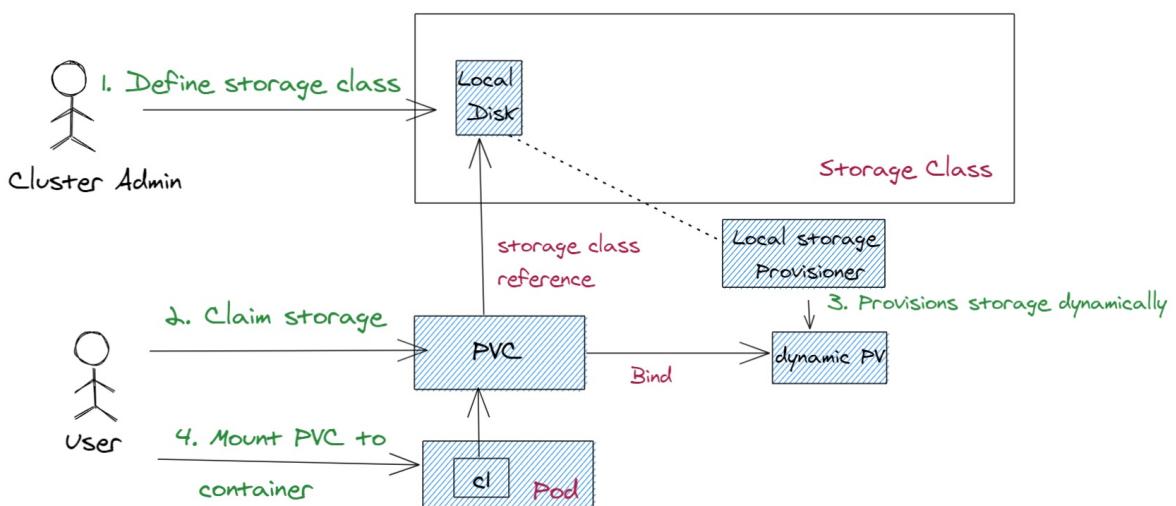


The following steps occur:

- 1. Provision storage:** The cluster admin provisions the storage. In this example, the cluster admin creates one or more SMB shares that automatically create persistent volume objects in the Kubernetes cluster corresponding to these shares.
- 2. Claim storage:** You submit a PVC deployment that requests the storage. This claim for storage is the PersistentVolumeClaim (PVC). If the size and the access mode of the PV match that of the PVC, then the PVC is bound to the PV. The PVC and PV map one-to-one.
- 3. Mount PVC to the container:** Once the PVC is bound to the PV, you can mount this PVC onto a path in your container. When the application logic in the container reads/writes from/into this path, the data is written into the SMB storage.

Dynamic provisioning

Here is a diagram that depicts how statically provisioned storage is consumed in Kubernetes:



The following steps occur:

- 1. Define storage class:** Cluster admin defines a storage class depending on the operating environment for your Kubernetes cluster. The cluster admin also deploys a provisioner, which is yet another pod or

application deployed on the Kubernetes cluster. The provisioner has all the details to provision the shares dynamically.

2. **Claim storage:** You submit an application that would claim the storage. Once a PVC is created with this storage class reference, the provisioner is invoked.
3. **Provision storage dynamically:** The provisioner dynamically creates the share associated with the local disk storage. Once the share is created, it also creates a PV object automatically corresponding to this share.
4. **Mount PVC to container:** Once the PVC is bound to the PV, you can mount the PVC on to the container onto a path in the same way as static provisioning and read from or write into the share.

Storage provisioning on Azure Stack Edge Pro

On the Azure Stack Edge Pro device, statically provisioned **PersistentVolumes** are created using the device's storage capabilities. When you provision a share and **Use the share with Edge compute** option is enabled, this action creates a PV resource automatically in the Kubernetes cluster.

The screenshot shows the Azure Stack Edge Pro interface for managing cloud storage gateways. On the left, the 'Shares' list is displayed with two entries: 'myasesmbcloudshare1' (SMB) and 'myasesmblocalshare1' (SMB). The 'Shares' link is highlighted with a red box. On the right, a modal dialog titled 'Add share' is open. It contains fields for 'Name' (set to 'localshare1'), 'Type' (set to 'SMB'), and a checkbox for 'Use the share with Edge compute' which is checked. Below these are sections for 'User details' (with 'Create new' selected) and a note about using an Edge local share. A 'Create' button at the bottom is highlighted with a red box.

To use cloud tiering, you can create an Edge cloud share with the **Use the share with Edge compute** option enabled. A PV is again created automatically for this share. Any application data that you write to the Edge share is tiered to the cloud.

This screenshot shows the same interface as the previous one, but the 'Shares' list now includes a third entry: 'myasesmbcloudshare1'. The 'Shares' link is highlighted with a red box. The 'Add share' dialog is still open, but the configuration has changed. The 'Name' field is set to 'cloudshare1', and the 'Configure as Edge local share' checkbox is unchecked. Under 'Storage account', 'myasesa' is selected. Under 'Storage service', 'Block Blob' is selected. Under 'Select blob container', 'Create new' is selected with the name 'myasenbscloudshare1'. The 'Create' button at the bottom is highlighted with a red box.

You can create both SMB and NFS shares to statically provision PVs on Azure Stack Edge Pro device. Once the PV is provisioned, you will submit a PVC to claim this storage. Here is an example of a PVC deployment [yaml](#) that claims the storage and uses the shares you provisioned.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-smb-flexvol
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 10Gi
  volumeName: <nfs-or-smb-share-name-here>
  storageClassName: ""
```

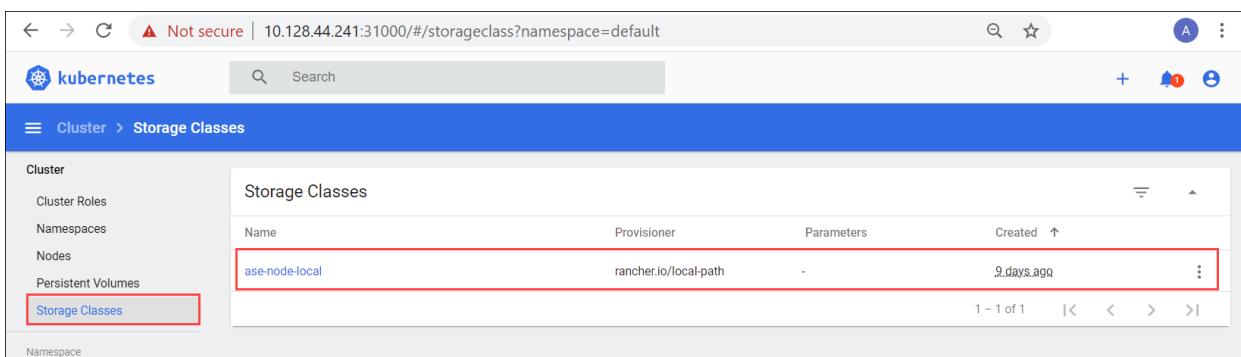
To get the value of the `volumeName` field, select the Local mount point for Edge compute modules when you select the SMB or NFS share after creation. This is the same as the share name.

For more information, see [Deploy a stateful application via static provisioning on your Azure Stack Edge Pro via kubectl](#).

To access the same statically provisioned storage, the corresponding volume mount options for storage bindings for IoT are as follows. The `/home/input` is the path at which the volume is accessible within the container.

```
{
  "HostConfig": {
    "Mounts": [
      {
        "Target": "/home/input",
        "Source": "<nfs-or-smb-share-name-here>",
        "Type": "volume"
      },
      {
        "Target": "/home/output",
        "Source": "<nfs-or-smb-share-name-here>",
        "Type": "volume"
      }
    ]
  }
}
```

Azure Stack Edge Pro also has a builtin `StorageClass` called `ase-node-local` that uses a data disk storage attached to the Kubernetes node. This `StorageClass` supports dynamic provisioning. You can make a `StorageClass` reference in the pod applications and a PV is automatically created for you. For more information, see the [Kubernetes dashboard](#) to query for `ase-node-local StorageClass`.



The screenshot shows the Kubernetes Storage Classes page. The URL is 10.128.44.241:31000/#/storageclass?namespace=default. The left sidebar has a 'Storage Classes' link highlighted with a red box. The main table lists one Storage Class:

Name	Provisioner	Parameters	Created
ase-node-local	rancher.io/local-path	-	9.days.ago

For more information, see [Deploy a stateful application via dynamic provisioning on your Azure Stack Edge Pro via kubectl](#).

Choose storage type

You may need to choose your storage type depending on the workload you are deploying.

- If you want `ReadWriteMany` access mode for your `PersistentVolumes` where the volumes are mounted as read-write by many nodes deploying, use static provisioning for the SMB/NFS shares.
- If the applications you are deploying have a POSIX compliance requirement, for example, applications such as MongoDB, PostgreSQL, MySQL or Prometheus, use the built-in StorageClass. The access modes are `ReadWriteOnce` or the volume is mounted as read-write by a single node.

For more information on access modes, see [Kubernetes volumes access mode](#).

Next steps

To understand how you can statically provision a `PersistentVolume`, see:

- [Deploy a stateful application via static provisioning on your Azure Stack Edge Pro via kubectl](#).

To learn how you can dynamically provision a `StorageClass`, see:

- [Deploy a stateful application via dynamic provisioning on your Azure Stack Edge Pro via kubectl](#).

Kubernetes networking on Azure Stack Edge Pro GPU device

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

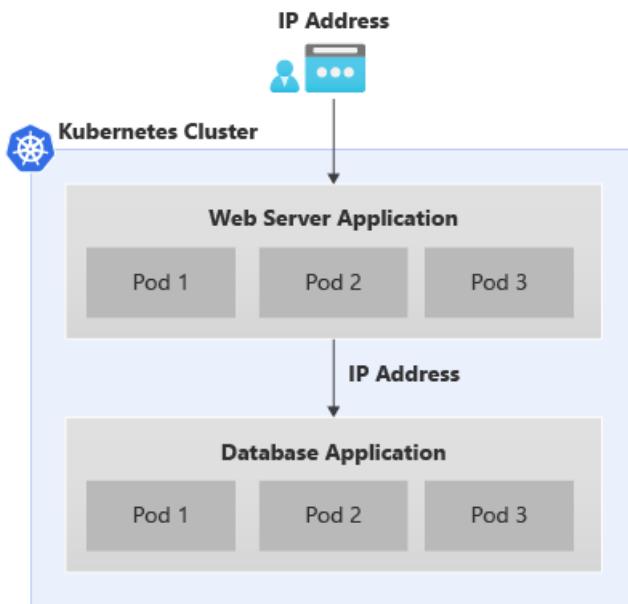
On your Azure Stack Edge Pro GPU device, a Kubernetes cluster is created when you configure compute role. Once the Kubernetes cluster is created, then containerized applications can be deployed on the Kubernetes cluster in Pods. There are distinct ways that networking is used for the Pods in your Kubernetes cluster.

This article describes the networking in a Kubernetes cluster in general and specifically in the context of your Azure Stack Edge Pro GPU device.

Networking requirements

Here is an example of a typical two-tier app that is deployed to the Kubernetes cluster.

- The app has a web server front end and a database application in the backend.
- Every pod is assigned an IP but these IPs can change on restart and failover of the pod.
- Each app is made up of multiple pods and there should be load balancing of the traffic across all the pod replicas.



The above scenario results in the following networking requirements:

- There is a need for the external facing application to be accessed by an application user outside of the Kubernetes cluster via a name or an IP address.
- The applications within the Kubernetes cluster, for example, front end and the backend pods here should be able to talk to each other.

To solve both the above needs, we introduce a Kubernetes service.

Networking services

There are two types of Kubernetes services:

- **Cluster IP service** - think of this service as providing a constant endpoint for the application pods. Any pod associated with these services cannot be accessed from outside of the Kubernetes cluster. The IP address used with these services comes from the address space in the private network.

To expose the pods within the Kubernetes cluster for access as other pods and not as an externally exposed load balancer service, see how to [Expose Kubernetes service as cluster IP service for internal communication](#).

- **Load balancer IP** - like the cluster IP service but the associated IP comes from the external network and can be accessed from outside of the Kubernetes cluster.

Kubernetes network configuration

The IP addresses used for Kubernetes nodes and the external services are provided via the **Compute** page in the local UI of the device.

Azure Stack Edge

Compute myasegpu1

Configure one network interface on your device for compute. Use running on your device.

Name	Network
Port 1	192.168.100.0
Port 2	10.128.44.0
Port 3	5.5.0.0
Port 4	5.5.0.0
Port 5	5.5.0.0
Port 6	5.5.0.0

Network settings (Port2)

* Enable for compute
Yes No

Compute is enabled on this network interface.

Compute IPs

For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:

Kubernetes node IPs
Enter a contiguous range of 2 static IPs for your device.
10.128.44.241-10.128.44.242

Kubernetes external service IPs
Specify the static IP range for services exposed outside of Kubernetes cluster.
10.128.44.243-10.128.44.245 ✓

< Back to Overview Next: Web proxy >

Apply

The IP assignment is for:

- **Kubernetes node IPs:** This IP range is used for Kubernetes master and worker nodes. These IPs are used when Kubernetes nodes communicate with each other.
- **Kubernetes external service IPs:** This IP range is used for external services (also known as the Load Balancer services) that are exposed outside of the Kubernetes cluster.

Kubernetes networking components

Calico, Metallb, and Core DNS are all the components that are installed for networking on your Azure Stack Edge Pro GPU.

- **Calico** assigns an IP address from a private IP range to every pod and configures networking for these pods so that pod on one node can communicate with the pod on another node.
- **Metallb** runs on an in-cluster pod and assigns IP address to services of type **load balancer**. Load balancer

IP addresses are chosen from the service IP range provided via the local UI.

- **Core DNS** - This add-on configures DNS records mapping service name to cluster IP address.

When you connect to the PowerShell interface of your device, you can see the above networking components running on your Kubernetes cluster.

Network interfaces, switches

Your device is available as a 1-node configuration that constitutes the infrastructure cluster. The Kubernetes cluster is separate from the infrastructure cluster and is deployed on top of the infrastructure cluster. The Kubernetes cluster has a master node and a worker node. Both the Kubernetes nodes are virtual machines that run your applications and cloud workflows.

The master and worker VMs each have two network interfaces, one that connects to the internal virtual switch and another that connects to the external virtual switch.

- **External virtual switch:** This switch is created when we enable a device port for compute via the **Compute** page in the local UI. This is the switch that you use for your compute infrastructure, for example, this switch is used for the virtual machines that you deploy on your device.
- **Internal virtual switch:** This switch is created as a part of the factory default settings on your device. The internal virtual switch uses Network Address Translation (NAT) to route the traffic through the port that is configured with a default gateway. For example, this switch routes all the IoT runtime requests from VMs to the Azure portal.

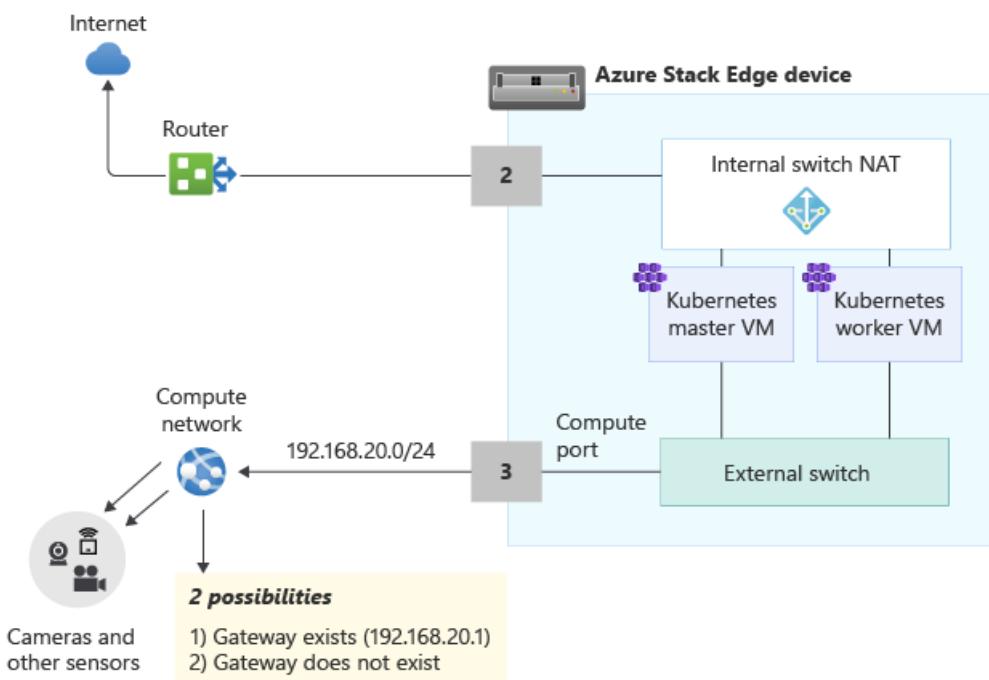
Network routes

For the Kubernetes VMs on your device, you can route the traffic by adding a new route configuration. A route configuration is a routing table entry that includes the following fields:

PARAMETER	DESCRIPTION
Destination	Either an IP address or an IP address prefix.
Prefix length	The prefix length corresponding to the address or range of addresses in the destination.
Next hop	The IP address to which the packet is forwarded.
Interface	The network interface that forwards the IP packet.
Metric	Routing metric determines the preferred network interface used to reach the destination.

Change routing on compute network

Use the `Add-HcsNetRoute` cmdlet to modify the routing on the Kubernetes worker and master VMs. Consider the layout in the diagram below.



- Port 2 is connected to the internet and is your desired path for outbound traffic.
- You've enabled compute on Port 3 and this has created an external virtual switch on this network interface.
- Port 3 is connected to a private network that has cameras and other sensors that are feeding raw data to the Azure Stack Edge device for processing.

If a gateway is configured in your environment in the private network, consider setting custom routes for the Kubernetes master and worker VMs so that they can communicate with your gateway for only the relevant traffic. This lets you be in control of the traffic that flows on the compute network versus the other ports that you might have configured on your Azure Stack Edge device. For example, you may want all other internet-facing traffic to flow over the other physical ports on your device. In this case, internet-facing traffic can go through Port 2.

You should also factor these other considerations:

- If you have a flat subnet, then you don't need to add these routes to the private network. You can (optionally) add these routes when there are multiple subnets on your private network.
- You can add these routes only to the Kubernetes master and worker VMs and not to the device (Windows host).
- The Kubernetes compute need not be configured before you add this route. You can also add or update routes after the Kubernetes compute is configured.
- You can only add a new route configuration via the PowerShell interface of the device and not through the local UI.
- Make sure that the network interface that you'll use has a static configuration.

Add a route configuration

To add a new custom route to the private network, use the cmdlet as follows:

```
Add-HcsNetRoute -InterfaceAlias <Port number> -DestinationPrefix <Destination IP address or IP address prefix> -NextHop <IP address of next hop> -RouteMetric <Route metric number>
```

Here is an example output.

```
Add-HcsNetRoute -InterfaceAlias "Port3" -DestinationPrefix "192.168.20.0/24" -NextHop "192.168.20.1" -  
RouteMetric 100
```

The above command will create an entry in the routing table that defines a destination subnet 192.168.20.0/24, specifies the next hop as 192.168.20.1, and assigns this routing entry a routing metric of 100. Lower the routing metric, higher the priority assigned to the route.

Check route configuration

Use this cmdlet to check for all the custom route configurations that you added on your device. These routes do not include all the system routes or default routes that already exist on the device.

```
Get-HcsNetRoute -InterfaceAlias <Port number>
```

Remove a route configuration

Use this cmdlet to remove a route configuration that you added on your device.

```
Remove-HcsNetRoute -InterfaceAlias <Port number> -DestinationPrefix <Destination IP or IP prefix>
```

Routing with multiple network interfaces

If multiple device ports are connected, then standard NIC teaming or Switch Embedded Teaming (SET) that lets you group several physical network adapters into a single virtual network adapter in a Hyper-V environment, is not supported.

Next steps

To configure Kubernetes networking on your Azure Stack Edge Pro GPU see:

- [Expose a stateless application externally on your Azure Stack Edge Pro GPU via IoT Edge.](#)
- [Expose a stateless application externally on your Azure Stack Edge Pro GPU via kubectl.](#)

Kubernetes role-based access control on your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

On your Azure Stack Edge Pro device, when you configure compute role, a Kubernetes cluster is created. You can use Kubernetes role-based access control (Kubernetes RBAC) to limit access to the cluster resources on your device.

This article provides an overview for the Kubernetes RBAC system provided by Kubernetes, and how it is implemented on your Azure Stack Edge Pro device.

Kubernetes RBAC

Kubernetes RBAC lets you assign users, or groups of users, permission to do things like create or modify resources, or view logs from running application workloads. These permissions can be scoped to a single namespace, or granted across the entire cluster.

When you set up the Kubernetes cluster, a single user is created corresponding to this cluster and is called the cluster admin user. A `kubeconfig` file is associated with the cluster admin user. The `kubeconfig` file is a text file that contains all the configuration information required to connect to the cluster to authenticate the user.

Namespaces types

Kubernetes resources, such as pods and deployments, are logically grouped into a namespace. These groupings provide a way to logically divide a Kubernetes cluster and restrict access to create, view, or manage resources. Users can only interact with resources within their assigned namespaces.

Namespaces are intended for use in environments with many users spread across multiple teams, or projects. For more information, see [Kubernetes namespaces](#).

Your Azure Stack Edge Pro device has the following namespaces:

- **System namespace** - This namespace is where core resources exist, such as network features like DNS and proxy, or the Kubernetes dashboard. You typically don't deploy your own applications into this namespace. Use this namespace to debug any Kubernetes cluster issues.

There are multiple system namespaces on your device and the names corresponding to these system namespaces are reserved. Here is a list of the reserved system namespaces:

- kube-system
- metallb-system
- dbe-namespace
- default
- kubernetes-dashboard
- kube-node-lease
- kube-public

Make sure to not use any reserved names for user namespaces that you create.

- **User namespace** - These are the namespaces that you can create via **kubectl** or via the PowerShell interface of the device to locally deploy applications.
- **IoT Edge namespace** - You connect to this `iotedge` namespace to manage applications deployed via IoT Edge.
- **Azure Arc namespace** - You connect to this `azure-arc` namespace to manage applications deployed via Azure Arc. With Azure Arc, you can also deploy applications in other user namespaces.

Namespaces and users

In the real world, it is important to divide the cluster into multiple namespaces.

- **Multiple users:** If you have multiple users, then multiple namespaces will allow those users to each deploy their applications and services in their specific namespaces in isolation from one another.
- **Single user:** Even if there is a single user, multiple namespaces would allow that user to run multiple versions of the applications in the same Kubernetes cluster.

Roles and RoleBindings

Kubernetes has the concept of role and role binding that lets you give permissions to user or resources at a namespace level and at a cluster level.

- **Roles:** You can define permissions to users as a **Role** and then use **Roles** to grant permissions within a namespace.
- **RoleBindings:** Once you have defined the roles, you can use **RoleBindings** to assign roles for a given namespace.

This approach lets you logically segregate a single Kubernetes cluster, with users only able to access the application resources in their assigned namespace.

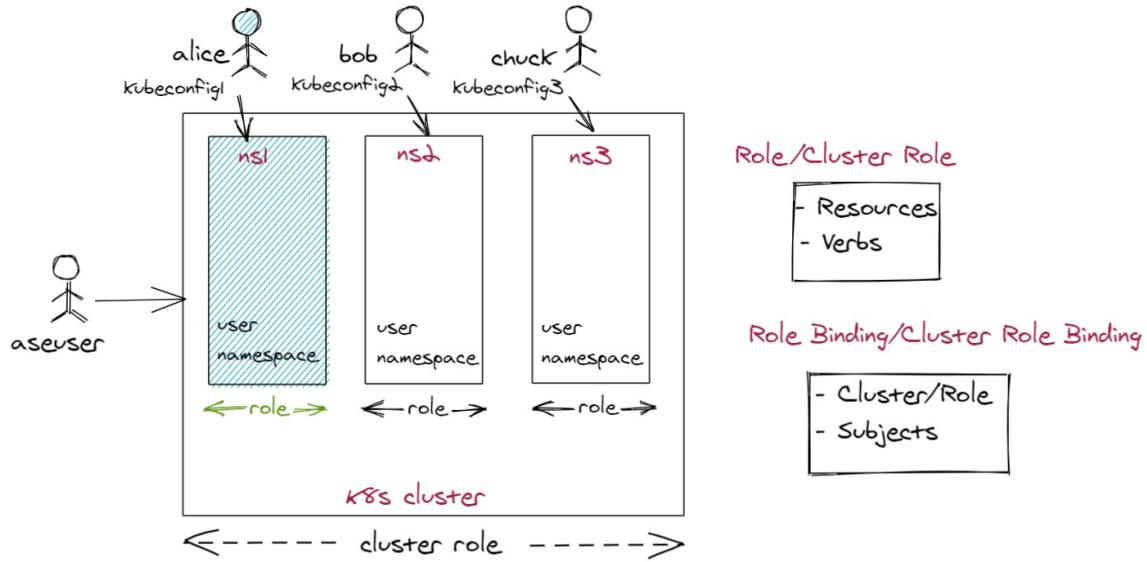
Kubernetes RBAC on Azure Stack Edge Pro

In the current implementation of Kubernetes RBAC, Azure Stack Edge Pro allows you to take the following actions from a restricted PowerShell runspace:

- Create namespaces.
- Create additional users.
- Grant you admin access to the namespaces that you created. Keep in mind that you won't have access to cluster admin role or a view of the cluster-wide resources.
- Get `kubeconfig` file with information to access the Kubernetes cluster.

The Azure Stack Edge Pro device has multiple system namespaces and you can create user namespaces with `kubeconfig` files to access those namespaces. The users have full control over these namespaces and can create or modify users, or grant users access. Only the cluster admin has full access to system namespaces and cluster-wide resources. An `aseuser` has read-only access to system namespaces.

Here is a diagram that depicts the implementation of Kubernetes RBAC on Azure Stack Edge Pro device.



In this diagram, Alice, Bob, and Chuck have access to assigned user namespaces only, which in this case are `ns1`, `ns2`, and `ns3` respectively. Within these namespaces, they have admin access. The cluster admin on the other hand has admin access to system namespaces and cluster-wide resources.

As a user, you can create namespaces and users, assign users to namespaces, or download `kubeconfig` files. For detailed step-by-step instructions, go to [Access Kubernetes cluster via kubectl on your Azure Stack Edge Pro](#).

When working with namespaces and users on your Azure Stack Edge Pro devices, the following caveats apply:

- You are not allowed to perform any operations such as create users, grant or revoke namespace access to user, for any of the system namespaces. Examples of system namespaces include `kube-system`, `metallb-system`, `kubernetes-dashboard`, `default`, `kube-node-lease`, `kube-public`. System namespaces also include the namespaces reserved for deployment types such as `iotedge` (IoT Edge namespace) and `azure-arc` (Azure Arc namespace).
- You can create user namespaces and within those namespaces create additional users and grant or revoke namespace access to those users.
- You are not allowed to create any namespaces with names that are identical to those for any system namespace. The names for system namespaces are reserved.
- You are not allowed to create any user namespaces with names that are already in use by other user namespaces. For example, if you have a `test-ns` that you created, you cannot create another `test-ns` namespace.
- You are not allowed to create users with names that are already reserved. For example, `aseuser` is a reserved user and cannot be used.

Next steps

To understand how you can create a user, create a namespace, and grant user access to the namespace, see [Access a Kubernetes cluster via kubectl](#).

Kubernetes workload management on your Azure Stack Edge Pro device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

On your Azure Stack Edge Pro device, a Kubernetes cluster is created when you configure compute role. Once the Kubernetes cluster is created, then containerized applications can be deployed on the Kubernetes cluster in Pods. There are distinct ways to deploy workloads in your Kubernetes cluster.

This article describes the various methods that can be used to deploy workloads on your Azure Stack Edge Pro device.

Workload types

The two common types of workloads that you can deploy on your Azure Stack Edge Pro device are stateless applications or stateful applications.

- **Stateless applications** do not preserve their state and save no data to persistent storage. All of the user and session data stays with the client. Some examples of stateless applications include web frontends like Nginx, and other web applications.

You can create a Kubernetes deployment to deploy a stateless application on your cluster.

- **Stateful applications** require that their state be saved. Stateful applications use persistent storage, such as persistent volumes, to save data for use by the server or by other users. Examples of stateful applications include databases like [Azure SQL Edge](#) and MongoDB.

You can create a Kubernetes deployment to deploy a stateful application.

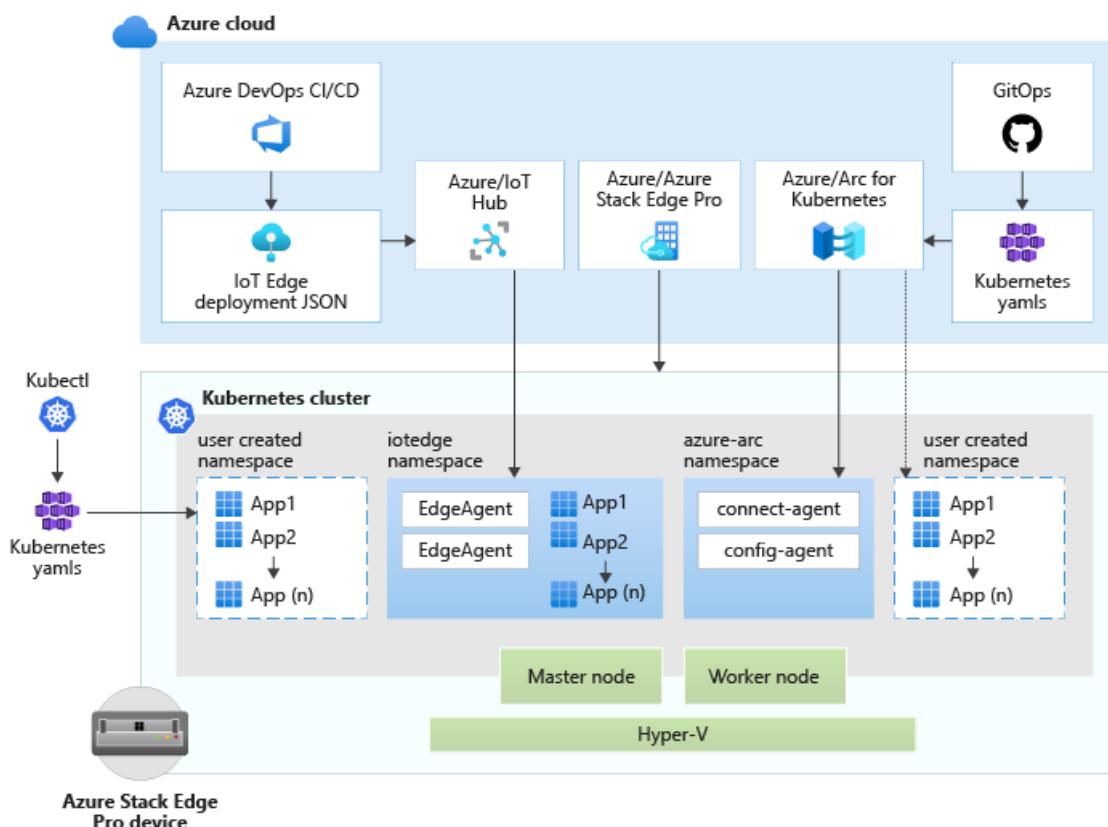
Deployment flow

To deploy applications on an Azure Stack Edge Pro device, you will follow these steps:

1. **Configure access:** First, you will use the PowerShell runspace to create a user, create a namespace, and grant user access to that namespace.
2. **Configure storage:** Next, you will use the Azure Stack Edge resource in the Azure portal to create persistent volumes using either static or dynamic provisioning for the stateful applications that you will deploy.
3. **Configure networking:** Finally, you will use the services to expose applications externally and within the Kubernetes cluster.

Deployment types

There are three primary ways of deploying your workloads. Each of these deployment methodologies allows you to connect to a distinct namespace on the device and then deploy stateless or stateful applications.



- **Local deployment:** This deployment is through the command-line access tool such as `kubectl` that allows you to deploy Kubernetes `yamls`. You access the Kubernetes cluster on your Azure Stack Edge Pro via a `kubeconfig` file. For more information, go to [Access a Kubernetes cluster via kubectl](#).
- **IoT Edge deployment:** This is through IoT Edge, which connects to the Azure IoT Hub. You connect to the Kubernetes cluster on your Azure Stack Edge Pro device via the `iotedge` namespace. The IoT Edge agents deployed in this namespace are responsible for connectivity to Azure. You apply the `IoT Edge deployment.json` configuration using Azure DevOps CI/CD. Namespace and IoT Edge management is done through cloud operator.
- **Azure Arc-enabled Kubernetes deployment:** Azure Arc-enabled Kubernetes is a hybrid management tool that will allow you to deploy applications on your Kubernetes clusters. You connect to the Kubernetes cluster on your Azure Stack Edge Pro device via the `azure-arc` namespace. The agents deployed in this namespace are responsible for connectivity to Azure. You apply the deployment configuration by using the GitOps-based configuration management.

Azure Arc-enabled Kubernetes will also allow you to use Azure Monitor for containers to view and monitor your cluster. For more information, go to [What is Azure Arc-enabled Kubernetes?](#).

Beginning March 2021, Azure Arc-enabled Kubernetes will be generally available to the users and standard usage charges apply. As a valued preview customer, the Azure Arc-enabled Kubernetes will be available to you at no charge for Azure Stack Edge device(s). To avail the preview offer, create a [Support request](#):

1. Under **Issue type**, select **Billing**.
2. Under **Subscription**, select your subscription.
3. Under **Service**, select **My services**, then select **Azure Stack Edge**.
4. Under **Resource**, select your resource.
5. Under **Summary**, type a description of your issue.
6. Under **Problem type**, select **Unexpected Charges**.
7. Under **Problem subtype**, select **Help me understand charges on my free trial**.

Choose the deployment type

While deploying applications, consider the following information:

- **Single or multiple types:** You can choose a single deployment option or a mix of different deployment options.
- **Cloud versus local:** Depending on your applications, you can choose local deployment via kubectl or cloud deployment via IoT Edge and Azure Arc.
 - When you choose a local deployment, you are restricted to the network in which your Azure Stack Edge Pro device is deployed.
 - If you have a cloud agent that you can deploy, you should deploy your cloud operator and use cloud management.
- **IoT vs Azure Arc:** Choice of deployment also depends on the intent of your product scenario. If you are deploying applications or containers that have deeper integration with IoT or IoT ecosystem, then select IoT Edge to deploy your applications. If you have existing Kubernetes deployments, Azure Arc would be the preferred choice.

Next steps

To locally deploy an app via kubectl, see:

- [Deploy a stateless application on your Azure Stack Edge Pro via kubectl.](#)

To deploy an app via IoT Edge, see:

- [Deploy a sample module on your Azure Stack Edge Pro via IoT Edge.](#)

To deploy an app via Azure Arc, see:

- [Deploy an application using Azure Arc.](#)

Tutorial: Configure compute on Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role and create a Kubernetes cluster on your Azure Stack Edge Pro GPU device.

This procedure can take around 20 to 30 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Get Kubernetes endpoints

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro device:

- Make sure that you've activated your Azure Stack Edge Pro device as described in [Activate Azure Stack Edge Pro](#).
- Make sure that you've followed the instructions in [Enable compute network](#) and:
 - Enabled a network interface for compute.
 - Assigned Kubernetes node IPs and Kubernetes external service IPs.

NOTE

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are on the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

Configure compute

To configure compute on your Azure Stack Edge Pro, you'll create an IoT Hub resource via the Azure portal.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**, and select **IoT Edge**.

The screenshot shows the Azure Stack Edge device overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Your device is running fine!' message. Below it, the 'Deployed edge services' section shows 'No deployed services'. The 'Edge services' section contains three cards: 'Virtual machines' (with a 'New' button), 'IoT Edge' (which is selected and has a red box around its card), and 'Cloud storage gateway'. Each card has a 'How to get started?' link.

2. In **Enable IoT Edge service**, select **Add**.

The screenshot shows the IoT Edge | Overview page. The left sidebar has a red box around the 'Overview' link. The main content area has a red box around the 'Enable IoT Edge service' section. This section contains instructions to enable the service by setting up the network and configuring the Azure subscription, followed by a large 'Add' button. Below this is a 'Steps to deploy IoT Edge services' section. At the bottom, there's a 'What's next' section with a link to 'Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services'.

3. On the **Configure Edge compute** blade, input the following information:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.

FIELD	VALUE
IoT Hub	<p>Choose from New or Existing. By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.</p>
Name	Accept the default name or enter a name for your IoT Hub resource.

Home > myasetest > IoT Edge >

Create IoT Edge service ⊕

Azure Stack Edge

[Basics](#) [Review + Create](#)

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription * <small>(i)</small>	Edge Gateway Test
Resource group * <small>(i)</small>	myaserg
IoT Hub * <small>(i)</small>	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing myasetest-iothub ✓

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

*IoT Edge device: myasetest-edge
 IoT Gateway device: myasetest-storagegateway*

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

4. When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

The screenshot shows the IoT Edge Overview page. At the top, there's a search bar and several action buttons: 'Add module', 'Add trigger', 'Refresh configuration', 'Remove', and 'Refresh'. Below the header, a red box highlights the 'Overview' tab. A message box says 'IoT Edge service is running fine!' with the subtext 'Start processing the data using IoT Edge modules. Learn more'. On the left, there are navigation links for 'Modules', 'Triggers', and 'Properties'. The main area has two sections: 'Modules' and 'Triggers'. The 'Modules' section contains a sub-section for 'Edge Shares' with a 'Configure Shares' link, and another for 'Edge Storage account' with a 'Configure Storage account' link. The 'Triggers' section has a 'Add trigger' button. At the bottom, there are three links: 'Edge Shares', 'Edge Storage account', and 'Network bandwidth usage'.

5. To confirm the Edge compute role has been configured, go to **IoT Edge > Properties**.

The screenshot shows the IoT Edge Properties page. At the top, there's a search bar and a 'Refresh' button. Below the header, a red box highlights the 'Properties' tab. The main area displays device configurations in a table:

IoT Hub	myasetest-iohub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

When the Edge compute role is set up on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

It can take 20-30 minutes to configure compute because, behind the scenes, virtual machines and a Kubernetes cluster are being created.

After you have successfully configured compute in the Azure portal, a Kubernetes cluster and a default user associated with the IoT namespace (a system namespace controlled by Azure Stack Edge) exist.

Get Kubernetes endpoints

To configure a client to access Kubernetes cluster, you'll need the Kubernetes endpoint. Follow these steps to get Kubernetes API endpoint from the local UI of your Azure Stack Edge Pro device.

1. In the local web UI of your device, go to **Device** page.
2. Under the **Device endpoints**, copy the **Kubernetes API endpoint**. This endpoint is a string in the

following format: [https://compute.<device-name>.<DNS-domain>\[Kubernetes-cluster-IP-address\]](https://compute.<device-name>.<DNS-domain>[Kubernetes-cluster-IP-address]).

The screenshot shows the 'Device' configuration page for a device named 'dl115'. The 'Device endpoints' section is highlighted with a red box. It lists various services with their certificate requirements and endpoints. The 'Kubernetes API service' endpoint is highlighted with a blue box: [https://compute.dl115.teatraining1.com \[10.128.45.200\]](https://compute.dl115.teatraining1.com [10.128.45.200]).

Service	Certificate Required	Endpoint
SMB server	No	\\\dl115.teatraining1.com\Share name]
NFS server	No	\\\[Device IP address]\Share name]
Azure Resource Manager login	Yes	https://login.dl115.teatraining1.com
Azure Resource Manager	Yes	https://management.dl115.teatraining1.com
Blob Storage	Yes	https://[Account name].blob.dl115.teatraining1.com
Kubernetes API service	No	https://compute.dl115.teatraining1.com [10.128.45.200]
Edge IoT hub	Yes	Endpoint not yet created.

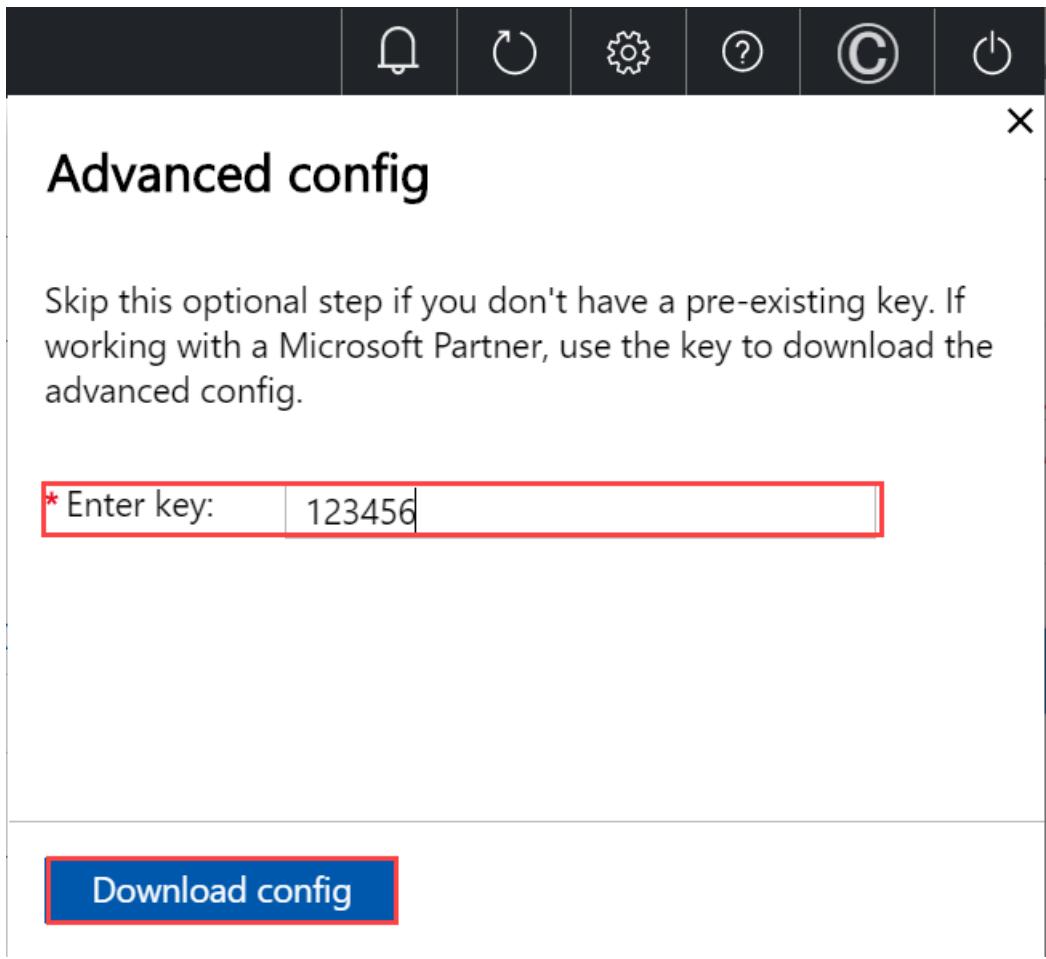
3. Save the endpoint string. You'll use this endpoint string later when configuring a client to access the Kubernetes cluster via kubectl.

4. While you are in the local web UI, you can:

- If you've been provided a key from Microsoft (select users may have a key), go to Kubernetes API, select **Advanced config**, and download an advanced configuration file for Kubernetes.

The screenshot shows the 'Device' configuration page for a device named 'myasegpu1'. The 'Device endpoints' section is highlighted with a red box. The 'Kubernetes API' endpoint is highlighted with a red box and has a 'Advanced config' button next to it. The endpoint URL is [https://compute.myasegpu1.wdshcsso.com \[10.128.44.241\]](https://compute.myasegpu1.wdshcsso.com [10.128.44.241]).

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\Share name]
NFS server	No	\\\[Device IP address]\Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241] Advanced config
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]



- You can also go to **Kubernetes dashboard** endpoint and download an `aseuser` config file.

The screenshot shows the 'Azure Stack Edge' device configuration page. The left sidebar lists various tabs: Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device), Maintenance (Power, Hardware health, Software update, Password change). The 'Device' tab is currently selected. On the right, under 'Device name', the name 'myasegpu1' is listed. In the 'Device endpoints' section, there is a table:

Service	Certificate Required	Endpoint
SMB server	No	\\\myasegpu1.wdshcsso.com\[Share name]
NFS server	No	\\\[Device IP address]\[Share name]
Azure Resource Manager login	Yes	https://login.myasegpu1.wdshcsso.com
Azure Resource Manager	Yes	https://management.myasegpu1.wdshcsso.com
Blob Storage	Yes	https://[Account name].blob.myasegpu1.wdshcsso.com
Kubernetes API	No	https://compute.myasegpu1.wdshcsso.com [10.128.44.241]
Kubernetes dashboard	No	https://10.128.44.241:31000 Download config
Edge IoT hub	Yes	myasegpures1-edge [10.128.44.243]

At the bottom, there are buttons for 'Apply', '< Back to Overview', and 'Next: Update server >'. A red box highlights the 'Download config' link for the Kubernetes dashboard endpoint.

You can use this config file to sign into the Kubernetes dashboard or debug any issues in your Kubernetes cluster. For more information, see [Access Kubernetes dashboard](#).

Next steps

In this tutorial, you learned how to:

- Configure compute
- Get Kubernetes endpoints

To learn how to administer your Azure Stack Edge Pro device, see:

[Use local web UI to administer an Azure Stack Edge Pro](#)

Connect to and manage a Kubernetes cluster via kubectl on your Azure Stack Edge Pro GPU device

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

On your Azure Stack Edge Pro device, a Kubernetes cluster is created when you configure compute role. Once the Kubernetes cluster is created, then you can connect to and manage the cluster locally from a client machine via a native tool such as *kubectl*.

This article describes how to connect to a Kubernetes cluster on your Azure Stack Edge Pro device and then manage it using *kubectl*.

Prerequisites

Before you begin, make sure that:

1. You've access to an Azure Stack Edge Pro device.
2. You've activated your Azure Stack Edge Pro device as described in [Activate Azure Stack Edge Pro](#).
3. You've enabled compute role on the device. A Kubernetes cluster was also created on the device when you configured compute on the device as per the instructions in [Configure compute on your Azure Stack Edge Pro device](#).
4. You've access to a Windows client system running PowerShell 5.0 or later to access the device. You can have any other client with a [Supported operating system](#) as well.
5. You have the Kubernetes API endpoint from the **Device** page of your local web UI. For more information, see the instructions in [Get Kubernetes API endpoint](#)

Connect to PowerShell interface

After the Kubernetes cluster is created, you can access this cluster to create namespaces and users and assign users to namespaces. This will require you to connect to the PowerShell interface of the device. Follow these steps on the Windows client running PowerShell.

Depending on the operating system of client, the procedures to remotely connect to the device are different.

Remotely connect from a Windows client

Prerequisites

Before you begin, make sure that:

- Your Windows client is running Windows PowerShell 5.0 or later.
- Your Windows client has the signing chain (root certificate) corresponding to the node certificate installed on the device. For detailed instructions, see [Install certificate on your Windows client](#).
- The `hosts` file located at `C:\Windows\System32\drivers\etc` for your Windows client has an entry corresponding to the node certificate in the following format:

```
<Device IP> <Node serial number>.<DNS domain of the device>
```

Here is an example entry for the `hosts` file:

```
10.100.10.10 1HXQG13.wdshcsso.com
```

Detailed steps

Follow these steps to remotely connect from a Windows client.

1. Run a Windows PowerShell session as an administrator.
2. Make sure that the Windows Remote Management service is running on your client. At the command prompt, type:

```
winrm quickconfig
```

For more information, see [Installation and configuration for Windows Remote Management](#).

3. Assign a variable to the connection string used in the `hosts` file.

```
$Name = "<Node serial number>.<DNS domain of the device>"
```

Replace `<Node serial number>` and `<DNS domain of the device>` with the node serial number and DNS domain of your device. You can get the values for node serial number from the **Certificates** page and DNS domain from the **Device** page in the local web UI of your device.

4. To add this connection string for your device to the client's trusted hosts list, type the following command:

```
Set-Item WSMan:\localhost\Client\TrustedHosts $Name -Concatenate -Force
```

5. Start a Windows PowerShell session on the device:

```
Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName Minishell -UseSSL
```

If you see an error related to trust relationship, then check if the signing chain of the node certificate uploaded to your device is also installed on the client accessing your device.

6. Provide the password when prompted. Use the same password that is used to sign into the local web UI. The default local web UI password is *Password1*. When you successfully connect to the device using remote PowerShell, you see the following sample output:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> winrm quickconfig
WinRM service is already running on this machine.
PS C:\WINDOWS\system32> $Name = "1HXQG13.wdshcsso.com"
PS C:\WINDOWS\system32> Set-Item WSMan:\localhost\Client\TrustedHosts $Name -Concatenate -Force
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName
Minishell -UseSSL

WARNING: The Windows PowerShell interface of your device is intended to be used only for the initial
network configuration. Please engage Microsoft Support if you need to access this interface to
troubleshoot any potential issues you may be experiencing. Changes made through this interface
without involving Microsoft Support could result in an unsupported configuration.

[1HXQG13.wdshcsso.com]: PS>
```

When you use the `-UseSSL` option, you are remoting via PowerShell over *https*. We recommend that you always

use *https* to remotely connect via PowerShell. Within trusted networks, remoting via PowerShell over http is acceptable. You first enable remote PowerShell over http in the local UI. Then you can connect to PowerShell interface of the device by using the preceding procedure without the `-UseSSL` option.

If you are not using the certificates (we recommend that you use the certificates!), you can skip the certificate validation check by using the session options: `-SkipCACheck -SkipCNCheck -SkipRevocationCheck`.

```
$sessOptions = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck  
Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName Minishell -UseSSL -  
SessionOption $sessOptions
```

Here is an example output when skipping the certificate check:

```
PS C:\WINDOWS\system32> $Name = "1HXQG13.wdshcsso.com"  
PS C:\WINDOWS\system32> $sessOptions = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck  
PS C:\WINDOWS\system32> $sessOptions  
  
MaximumConnectionRedirectionCount : 5  
NoCompression : False  
NoMachineProfile : False  
ProxyAccessType : None  
ProxyAuthentication : Negotiate  
ProxyCredential :  
SkipCACheck : True  
SkipCNCheck : True  
SkipRevocationCheck : True  
OperationTimeout : 00:03:00  
NoEncryption : False  
UseUTF16 : False  
IncludePortInSPN : False  
OutputBufferingMode : None  
MaxConnectionRetryCount : 0  
Culture :  
UICulture :  
MaximumReceivedDataSizePerCommand :  
MaximumReceivedObjectSize :  
ApplicationArguments :  
OpenTimeout : 00:03:00  
CancelTimeout : 00:01:00  
IdleTimeout : -00:00:00.0010000  
  
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName  
Minishell -UseSSL -SessionOption $sessOptions  
WARNING: The Windows PowerShell interface of your device is intended to be used only for the initial network  
configuration. Please  
engage Microsoft Support if you need to access this interface to troubleshoot any potential issues you may  
be experiencing.  
Changes made through this interface without involving Microsoft Support could result in an unsupported  
configuration.  
[1HXQG13.wdshcsso.com]: PS>
```

IMPORTANT

In the current release, you can connect to the PowerShell interface of the device only via a Windows client. The `-UseSSL` option does not work with the Linux clients.

Configure cluster access via Kubernetes RBAC

After the Kubernetes cluster is created, you can use the *kubectl*/via cmdline to access the cluster.

In this approach, you create a namespace and a user. You then associate the user with the namespace. You also need to get *config* file that allows you to use a Kubernetes client to talk directly to the Kubernetes cluster that you created without having to connect to PowerShell interface of your Azure Stack Edge Pro device.

1. Create a namespace. Type:

```
New-HcsKubernetesNamespace -Namespace <string>
```

NOTE

For both namespace and user names, the [DNS subdomain naming conventions](#) apply.

Here is a sample output:

```
[10.100.10.10]: PS> New-HcsKubernetesNamespace -Namespace "myasetest1"
```

2. Create a user and get a config file. Type:

```
New-HcsKubernetesUser -UserName <string>
```

NOTE

You can't use *aseuser* as the username as it is reserved for a default user associated with IoT namespace for Azure Stack Edge Pro.

Here is a sample output of the config file:

```
[10.100.10.10]: PS> New-HcsKubernetesUser -UserName "aseuser1"
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ01CQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd
0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJd01ERXI1PVEUyT1RFeE4xb1hEVE13TURFeU5qRTJOVEV4TjFvd0ZURVRNQK
VHQTFRQpBeE1LYTNWaVpYSnVaWFJsY3pDQ0FTSXdEUv1KS29aSwh2Y05BUUVQ1FBGdnRVBBRENDQVfvQ2dnRUJBTXNpCkdZUH
0U1VwCdhKZEdVcHE1MVBURWhsZm8wWkk3YXFBDu1rOHZwdUFczhJQK1FBszFxcEN1di93NjIwbUtpZ0QKak1aT3Q4QREREpWHF6
UDZRZm50c0U2VXBHMnh0YnYrcTZHV2R5K0t6WkxBMx1wWGY3Vj1zZEJnejVKVDNvYQpIdzFja2NTUK1HS1V3UwxTbk1NaHJUS3JUN
DZFUUp3d282Tm1NUzzMDZieVk3WkUrTgg30S9aNeHLaNhTRmhMc1c5ZG8veThzR3FXUDzMTfMmVmSkhUeGtwR05HZE1UVjNuOF
1CZ0pSRzdrNjh0N2MrZ1NhB1VwVJptUNSNAKY1FxcpscWVv2REZEJHOFh6aDJ0M114SkVIMm00T0Z1cSsvUitMYm95aHdKbmN
MdVJ50EpNZWlwTEQ3U1N0QwpZTDNNR0EzN2JieTRYm4zVzg4Q0F3RUFBYU1qTUNFd0RnWURWUjBQQVFI0JBURBZ0trTUE4R0Ex
VWRFd0VCCi93UUZNQU1CQWY4d0RRWUpLb1pJaHZjTkFRRUXCUUFEZ2dFQkFmbzFwW1BtQzV1cmRPZUjhSWQ4eEQzRkxCMG8KT1ErB
XBXMWpDd0ZtY3h6dUtlWmRsNx2N0tuS2JtCDR0TXo1cXg3bUtSc0UxcnBwlkh2VH1KUXg1ZFk2ZE1Kdgp5d2FQZjbpt05TN1U2Cc
9INE12U1dJaEtJZ1FuTne1dH4TjJCnNzPQw41RmzoRkx6WEqrUlZGSm42cnovWkZnCmV6MhpTknKymcve1FucFR0cmQ2cnFFRHp
oSVFZ0VdYVWQycFh3ZXrqUXJpMkpZamh4NmtEcTvOrkZTM0FLUnIK0W1QTVQxaWNkr1NUMFvvM1hIZ1k2ck45WGP3MHFrY2I0Sy83
U1VVWlRvs3dKamR0R31NTnpad000L2puR0p5SwpQTE9ycU5Dd1kvb01kVEM5eVZVY3VRbXV1R0Vqt20xUnN1RDFHYVE0RTZwakppV
WJpMVdrajJ1bFh0Wt0KLS0tLS1FTkQgQ0VSVE1GSUNBVETLS0tLQo=
server: https://10.128.47.90:6443
name: kubernetes
contexts:
- context:
  cluster: kubernetes
  user: aseuser1
  name: aseuser1@kubernetes
current-context: aseuser1@kubernetes
kind: Config
preferences: {}
users:
- name: aseuser1
  user:
    client-certificate-data:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMwVENDQWjtZ0F3SUJBZ01JW1FXcjY2cGFWSm93RFFZSktrWklodmNOQVF
EJRQxdGVEVUTUJFR0ExVUUKQXhNS2EzVm1aWEp1WlhSbGN6QWVGdzB5TURBe1qa3h0alv4Tvrkyuz3Mh1NVEF4TwPneU1qVTJNVG
```

RhTUJNeApFVEFQQmdOVkJBTVRDR0Z6WlhWe1pYSXhNSU1CSWpBTkJna3Foa21HOXcwQkFRRUZBQU9DQVE4QU1JSUJDZ0tDCkFRRUF4R3RDaXJ2cVhGym5wVmtaY1VPRWQ3cXg2UzNVZ092M1hHRHNKM2VYWXN0bUxQVjMrQn1BclwvN211L1AKaLdmaWt6MG9QS1iYmtvcVJkam1YckxFZnk0N3dHcEhdUhUOHNLY2tHTnJ1eFE2bXhaZ29xaU1nL2FuMuPMDwp1oFEvVn1QaWdVdUt6eVBseEhUZm1mSVM5MzR1VnZVZUc0dz1MRjAyZ2s2Nitpc0ZtanhsvmhseWRM1c2UmZTcj10OGpNMEFkdEpJL0xNbE13RHJJRVdFKzM4WDVNelJhQkJYN1zNDFWskZxeckwdW14dHdxN2pGOXp1UTE4ekIKalRzaD130WVKcDJwS2Fvak5tNE9SSdh4SzVSaUhocj2anFJWXkxRdd2WDh0b0U1K05HNmxHzjh5L1NvQnNRbQpm0G9vL1k3SEZmQXVGd1N6WUc1RU1QTFM4UU1EQVFBQm95Y3dKVEFPQmd0VkhROEJBZhFQkFNQ0JhQXdFd11EC1ZSMGxCQxd3Q2dZSUt3WUJCUVV1QXjd0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dFQkFNR1BxY0YzS1BCbHZ0K24KN1NoGE3anhWYkhZVGxyNTgwVWzek93WEwwVnVPUU1CYmN2dj1zzk9HNkhDz1Q0bWxBu0JRWVNZcmpLMjJTTwpTWld4cJNQUD1hVzNhajkxc0ttSnc1ZUF1WFhQbUjpK1RWQzBvY0ZLaEqvZ0o1aC93YnBaVndpVjVyRWE5Kzc2CnhnCFazR1d6dG5tT1hPaE16UFN1R3B4YwpwQXd3ZXd4Q0U0yb0xGRFZFc9XTFFMODJZM3NFcE93NVNaSVJJNMXMKUHHMTVnV1ZPM2x2SXcwZ3IrdkJ1anZSOUZKaWVuTWFRdGdjSVgyRmpDaDBRMHVYRkdtsTVNxWE1jbjRLRTR0TApQSFFMa1RSVUwyVnRXcW1Y1RBm3RzN01DcGNRTFdPZFJUYkpSejZCbkc1aXVwcDd0s1FvYw9YcWpNvk5VDZCC11YMEd0Skk9Ci0tLS0tRU5EIEFU1RJRK1DQVRFLS0tLS0K

client-key-data:

LS0tLS1CRudJTibSU0EgUFJJVkfURSBLRVktLS0tLQpNSU1Fb2dJQkFBs0NB0UVBeEd0Q21ydnFYRmjucFZrWmJVT0Vkn3F4N1MzVWdPdjYR0RzSjN1WF1zdG1MUFYzCitCeUFxbDI3bXuvUGlnZmlrejBvUEltYmJrb3FSZGppWHJMRWZ5NDd3R3B1c3ViVDhzS2NrR05yZxhRNm14WmcKb3FpTwcvYw4xSkx3YjhRL1Z5UGlnVXLen1QbHhIVGzpZk1TOTM0dVZ2VWVHNhC5TEywMmdrNjYraXNGbWp4bApWaGx5ZEw2VzZS1M5dDhqTTBBZHRKS9MTwNd0RySUVXRSszOfg1TxpSYUJCWDZ5czQxVkpGcXpHMVteHR3CnE3akY5enVRMTh6QmpUWwg5dz11SnAycEthb2p0bTRPUkg4eEs1Um1iaHiYdmpxSV15MUQ3d1g4d9FNST0RzYkbEdm0HkvU29Cc1Ftzjhbvby9Zn0hGZkF1RnZTe11HNUVJUExTOFFJREFRQUJBb01CQUVVSUVXM2kxMTQycU5raQo5RjNEWWZZV1pscTJZYjRoc0FjTmhWSGxwUTN5d0dsQ3FEuktDQ3BZSVF3MkJqSF6R6WnpEM0xwu0E0K0NmMuoxCkE4QVdnahJVCstsWE1QVzhpcG9DTGJaT1NzUuord0x3b1d2dF10MhfQagZtd0p2M1UrK1RUQkwyOHNVVUw3ZVkkLzh0aw1hbno3ZU5mNk1lIMENyZmgxcnQ3WhsemtdRd1hBVHNScVJja0dMaTgrdGN5WnVzdGFhbENUSzBGRTdCaQpBUGe5a2w1SG56eCs4TtvCNWladHkwTUIxWpwM1gb1bkUmlKsfVCb1AxVV0QutHjyVzu0RvN11kZ2pIUTRHCjNWn111YwZobnVFMXA0VVIvUkloVvdjR1VvaTfBOFpZMFdnd1BDTmhnMwpQZU5vb2Y1UhRpEY10TRBREVwUUyKoFR2bG92RUnnWUVB0WZZbUxyY0t1Q0j1MTFoQvhotoi91Z1RtbU5xNhpFL1pPSW16M0xwckdjRdhWddCvW9Gcgp1ekxbkts2tkczE50ERnvj1QZUhunZl1QTRoMjM5RkIwNFFhMuJbdUVMRzRsdHj3V1NxaFBENUR6YKcrSEhScnjyThVMEpUsmVvS0tjVjRUUGx1TzFtK2tjbkRjVXY1ckpwZDVXU3RvcUhXdk9RzkEvRUF0V1VDZ11FQxpHOTcKTitCZVvbFnirettvungdtdPZghYsxjyr3RnSEorZ2J0MD1nSHURG5PY0IxZ1NzNkpza1FPQU9qbWFxk051RAp5SUF1Nythew1FRmpyT2tzTGhkSTREUXNkWFZveFFGVko1V1Jw1k3UTVRaFzpyR2enR4ND1zSD1KSkp1M2U0Cn13NwdpNGkxKy90MnY2eWRKcldNQ0xx0H1EdFRrcE9PSitkbk5MENnWUjwZ31pcUrAzU9KTU9CUTdpSk12QssKQ211VmJ1K0hTaEd6Tu9HSHPBamc2V3IybEh1Mk94S31qb1M5jdWtmtLNDhGQitwVfpnUm1ru19Cz0Q4T2tLUQp1YXFOZnFYazViQ1AxZ3dKcVpwazRVTfd0ZmNoQ1NLY01ES1Z2VFFTSTRr0RQk29kYws0Nkt6WnVhwGrTxDjCmvdZ2FhZkFhdmpaeVhhSDRmT0NDN1FLQmdHVXJCaDh3dVh5KzJEc1RGWnF40E9McjNoS2Q0c1UyRXRSODJic1ckbk1xbEgraVzxu0x3VfdFTWJBUnUzTVU3cV1CyNbxw1RNwdVNG1UcmR4Z3Fpk0tEUTEwd2RJL3IrbdBEt1CTApCRG1kajlaeGg4M0tZlwhtSTXbzLzJULys1TDVsru4zcnozczl2RkZtcisxS3pycENqek1DdDbtZmtrd0hV0pGCjhaWkJbb0dBVXB3aUircw1hbkpxu1FtzHNSZFVabGFBaTRpbGhAA01RYTRHem95ZFQ30TVHtm44ZThBrj3WHMKTGpyyjde1FwakdCMnZpUlkySUZBvMiyKzsd1lw0VJRTMznSmxpnu5ZrxvQwRowXBsWdBZGFHWHNGNhdabwo3SHFHThBgdUmUxVU5Gb0dQdkxpWUNrUFVYdGduQ3dNb0R2SEpKnzVYMX16ckh6cmxus1k9ci0tLS0tRU5EIFJTQSBQuk1WQVRFIEtFWS0tLS0tCg==

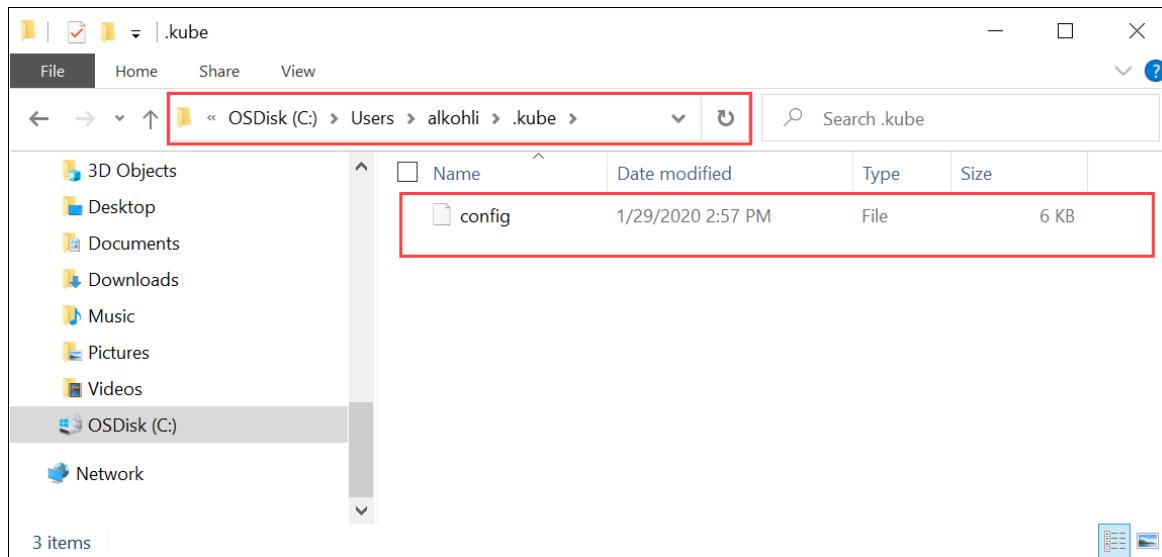
[10.100.10.10]: PS>

3. A config file is displayed in plain text. Copy this file and save it as a *config* file.

IMPORTANT

Do not save the config file as *.txt* file, save the file without any file extension.

4. The config file should live in the `.kube` folder of your user profile on the local machine. Copy the file to that folder in your user profile.



5. Associate the namespace with the user you created. Type:

```
Grant-HcsKubernetesNamespaceAccess -Namespace <string> -UserName <string>
```

Here is a sample output:

```
[10.100.10.10]: PS>Grant-HcsKubernetesNamespaceAccess -Namespace "myasetest1" -UserName "aseuser1"
```

Once you have the config file, you do not need physical access to the cluster. If your client can ping the Azure Stack Edge Pro device IP, you should be able to direct the cluster using `kubectl` commands.

6. Start a new PowerShell session on your client. You don't need to be connected to the device interface. You can now install `kubectl` on your client using the following command:

```
PS C:\windows\system32> curl https://storage.googleapis.com/kubernetes-
release/release/v1.15.2/bin/windows/amd64/kubectl.exe -O kubectl.exe
```

```
PS C:\windows\system32>
```

For example, if the Kubernetes master node was running v1.15.2, install v1.15.2 on the client.

IMPORTANT

Download a client that is skewed no more than one minor version from the master. The client version but may lead the master by up to one minor version. For example, a v1.3 master should work with v1.1, v1.2, and v1.3 nodes, and should work with v1.2, v1.3, and v1.4 clients. For more information on Kubernetes client version, see [Kubernetes version and version skew support policy](#). For more information on Kubernetes server version on Azure Stack Edge Pro, go to Get Kubernetes server version. Sometimes, `kubectl` is preinstalled on your system if you are running Docker for Windows or other tools. It is important to download the specific version of `kubectl` as indicated in this section to work with this Kubernetes cluster.

The installation takes several minutes.

7. Verify the version installed is the one that you downloaded. You should specify the absolute path to where the `kubectl.exe` was installed on your system.

```
PS C:\Users\myuser> C:\windows\system32\kubectl.exe version
Client Version: version.Info{Major:"1", Minor:"15", GitVersion:"v1.15.2",
GitCommit:"f6278300bebbb750328ac16ee6dd3aa7d3549568", GitTreeState:"clean", BuildDate:"2019-08-
05T09:23:26Z", GoVersion:"go1.12.5", Compiler:"gc", Platform:"windows/amd64"}
Server Version: version.Info{Major:"1", Minor:"15", GitVersion:"v1.15.1",
GitCommit:"4485c6f18cee9a5d3c3b4e523bd27972b1b53892", GitTreeState:"clean", BuildDate:"2019-07-
18T09:09:21Z", GoVersion:"go1.12.5", Compiler:"gc", Platform:"linux/amd64"}
PS C:\Users\myuser>
```

For more information on `kubectl` commands used to manage the Kubernetes cluster, go to [Overview of kubectl](#).

8. Add a DNS entry to the hosts file on your system.

- Run Notepad as administrator and open the `hosts` file located at

```
C:\windows\system32\drivers\etc\hosts .
```

- Use the information that you saved from the **Device** page in the local UI in the earlier step to create the entry in the hosts file.

For example, copy this endpoint `https://compute.asedevice.microsoftdatabox.com/[10.100.10.10]` to create the following entry with device IP address and DNS domain:

```
10.100.10.10 compute.asedevice.microsoftdatabox.com
```

9. To verify that you can connect to the Kubernetes pods, type:

```
PS C:\Users\myuser> kubectl get pods -n "myasetest1"
No resources found.
PS C:\Users\myuser>
```

You can now deploy your applications in the namespace, then view those applications and their logs.

IMPORTANT

There are many commands that you won't be able to run, for example, the commands that require you to have admin access. You can only perform operations that are allowed on the namespace.

Remove Kubernetes cluster

To remove the Kubernetes cluster, you will need to remove the IoT Edge configuration.

For detailed instructions, go to [Manage IoT Edge configuration](#).

Next steps

- Deploy a stateless application on your Azure Stack Edge Pro.

Use compute acceleration on Azure Stack Edge Pro GPU for Kubernetes deployment

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to use compute acceleration on Azure Stack Edge devices when using Kubernetes deployments.

About compute acceleration

The Central Processing Unit (CPU) is your default general purpose compute for most processes running on a computer. Often a specialized computer hardware is used to perform some functions more efficiently than running those in the software in a CPU. For example, a Graphics Processing Unit (GPU) can be used to accelerate the processing of pixel data.

Compute acceleration is a term used specifically for Azure Stack Edge devices where a Graphical Processing Unit (GPU), a Vision Processing Unit (VPU), or a Field Programmable Gate Array (FPGA) are used for hardware acceleration. Most workloads deployed on your Azure Stack Edge device involve critical timing, multiple camera streams, and/or high frame rates, all of which require specific hardware acceleration.

The article will discuss compute acceleration only using GPU or VPU for the following devices:

- **Azure Stack Edge Pro GPU** - These devices can have 1 or 2 Nvidia T4 Tensor Core GPU. For more information, see [NVIDIA T4](#).
- **Azure Stack Edge Pro R** - These devices have 1 Nvidia T4 Tensor Core GPU. For more information, see [NVIDIA T4](#).
- **Azure Stack Edge Mini R** - These devices have 1 Intel Movidius Myriad X VPU. For more information, see [Intel Movidius Myriad X VPU](#).

Use GPU for Kubernetes deployment

The following example `yaml` can be used for an Azure Stack Edge Pro GPU or an Azure Stack Edge Pro R device with a GPU.

```
apiVersion: v1
kind: Pod
metadata:
  name: gpu-pod
spec:
  containers:
    - name: cuda-container
      image: nvidia/cuda:9.0-devel
      resources:
        limits:
          nvidia.com/gpu: 1 # requesting 1 GPU
    - name: digits-container
      image: nvidia/digits:6.0
      resources:
        limits:
          nvidia.com/gpu: 1 # requesting 1 GPU
```

Use VPU for Kubernetes deployment

The following example `yaml` can be used for an Azure Stack Edge Mini R device that has a VPU.

```
apiVersion: batch/v1
kind: Job
metadata:
  name: intelvpu-demo-job
  labels:
    jobgroup: intelvpu-demo
spec:
  template:
    metadata:
      labels:
        jobgroup: intelvpu-demo
    spec:
      restartPolicy: Never
      containers:
        -
          name: intelvpu-demo-job-1
          image: ubuntu-demo-openvino:devel
          imagePullPolicy: IfNotPresent
          command: [ "/do_classification.sh" ]
          resources:
            limits:
              vpu.intel.com/hddl: 1
```

Next steps

Learn how to [Use kubectl to run a Kubernetes stateful application with a PersistentVolume on your Azure Stack Edge Pro GPU device](#).

Deploy a Kubernetes stateless application via kubectl on your Azure Stack Edge Pro GPU device

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to deploy a stateless application using `kubectl` commands on an existing Kubernetes cluster. This article also walks you through the process of creating and setting up pods in your stateless application.

Prerequisites

Before you can create a Kubernetes cluster and use the `kubectl` command-line tool, you need to ensure that:

- You have sign-in credentials to a 1-node Azure Stack Edge Pro device.
- Windows PowerShell 5.0 or later is installed on a Windows client system to access the Azure Stack Edge Pro device. You can have any other client with a Supported operating system as well. This article describes the procedure when using a Windows client. To download the latest version of Windows PowerShell, go to [Installing Windows PowerShell](#).
- Compute is enabled on the Azure Stack Edge Pro device. To enable compute, go to the [Compute](#) page in the local UI of the device. Then select a network interface that you want to enable for compute. Select **Enable**. Enabling compute results in the creation of a virtual switch on your device on that network interface. For more information, see [Enable compute network on your Azure Stack Edge Pro](#).
- Your Azure Stack Edge Pro device has a Kubernetes cluster server running that is version v1.9 or later. For more information, see [Create and manage a Kubernetes cluster on Microsoft Azure Stack Edge Pro device](#).
- You have installed `kubectl`.

Deploy a stateless application

Before we begin, you should have:

1. Created a Kubernetes cluster.
2. Set up a namespace.
3. Associated a user with the namespace.
4. Saved the user configuration to `C:\Users\<username>\.kube`.
5. Installed `kubectl`.

Now you can begin running and managing stateless application deployments on an Azure Stack Edge Pro device. Before you start using `kubectl`, you need to verify that you have the correct version of `kubectl`.

Verify you have the correct version of `kubectl` and set up configuration

To check the version of `kubectl`:

1. Verify that the version of `kubectl` is greater or equal to 1.9:

```
kubectl version
```

An example of the output is shown below:

```
PS C:\WINDOWS\system32> C:\windows\system32\kubectl.exe version
Client Version: version.Info{Major:"1", Minor:"15", GitVersion:"v1.15.2",
GitCommit:"f627830beb7b750328ac16ee6dd3aa7d3549568", GitTreeState:"clean", BuildDate:"2019-08-
05T09:23:26Z", GoVersion:"go1.12.5", Compiler:"gc", Platform:"windows/amd64"}
Server Version: version.Info{Major:"1", Minor:"15", GitVersion:"v1.15.1",
GitCommit:"4485c6f18cee9a5d3c3b4e523bd27972b1b53892", GitTreeState:"clean", BuildDate:"2019-07-
18T09:09:21Z", GoVersion:"go1.12.5", Compiler:"gc", Platform:"linux/amd64"}
```

In this case, the client version of kubectl is v1.15.2 and is compatible to continue.

- Get a list of the pods running on your Kubernetes cluster. A pod is an application container, or process, running on your Kubernetes cluster.

```
kubectl get pods -n <namespace-string>
```

An example of command usage is shown below:

```
PS C:\WINDOWS\system32> kubectl get pods -n "test1"
No resources found.
PS C:\WINDOWS\system32>
```

The output should state that no resources (pods) are found because there are no applications running on your cluster.

The command will populate the directory structure of "C:\Users\<username>\.kube" with configuration files. The kubectl command-line tool will use these files to create and manage stateless applications on your Kubernetes cluster.

- Manually check the directory structure of "C:\Users\<username>\.kube" to verify *kubectl* has populated it with the following subfolders:

```
PS C:\Users\username> ls .kube

Directory: C:\Users\user\.kube

Mode                LastWriteTime        Length Name
----                -----          -----
d----
```

NOTE

To view a list of all kubectl commands, type `kubectl --help`.

Create a stateless application using a deployment

Now that you've verified that the kubectl command-line version is correct and you have the required configuration files, you can create a stateless application deployment.

A pod is the basic execution unit of a Kubernetes application, the smallest and simplest unit in the Kubernetes object model that you create or deploy. A pod also encapsulates storage resources, a unique network IP, and options that govern how the container(s) should run.

The type of stateless application that you create is an nginx web server deployment.

All kubectl commands you use to create and manage stateless application deployments need to specify the namespace associated with the configuration. You created the namespace while connected to the cluster on the Azure Stack Edge Pro device in the [Create and manage a Kubernetes cluster on Microsoft Azure Stack Edge Pro device](#) tutorial with `New-HcsKubernetesNamespace`.

To specify the namespace in a kubectl command, use `kubectl <command> -n <namespace-string>`.

Follow these steps to create an nginx deployment:

1. Apply a stateless application by creating a Kubernetes deployment object:

```
kubectl apply -f <yaml-file> -n <namespace-string>
```

In this example, the path to the application YAML file is an external source.

Here is a sample use of the command and its output:

```
PS C:\WINDOWS\system32> kubectl apply -f https://k8s.io/examples/application/deployment.yaml -n "test1"
deployment.apps/nginx-deployment created
```

Alternatively, you can save the following markdown to your local machine and substitute the path and filename in the `-f` parameter. For instance, "C:\Kubernetes\deployment.yaml". The configuration for the application deployment would be:

```
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  selector:
    matchLabels:
      app: nginx
  replicas: 2 # tells deployment to run 2 pods matching the template
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.7.9
          ports:
            - containerPort: 80
```

This command creates a default nginx-deployment that has two pods to run your application.

2. Get the description of the Kubernetes nginx-deployment you created:

```
kubectl describe deployment nginx-deployment -n <namespace-string>
```

A sample use of the command, with output, is shown below:

```
PS C:\Users\user> kubectl describe deployment nginx-deployment -n "test1"

Name:           nginx-deployment
Namespace:      test1
CreationTimestamp:  Tue, 18 Feb 2020 13:35:29 -0800
Labels:          <none>
Annotations:    deployment.kubernetes.io/revision: 1
                  kubectl.kubernetes.io/last-applied-configuration:
                  {"apiVersion":"apps/v1","kind":"Deployment","metadata":{"annotations":{},"name":"nginx-deployment","namespace":"test1"},"spec":{"repl...
Selector:        app=nginx
Replicas:        2 desired | 2 updated | 2 total | 2 available | 0 unavailable
StrategyType:   RollingUpdate
MinReadySeconds: 0
RollingUpdateStrategy: 25% max unavailable, 25% max surge
Pod Template:
  Labels:  app=nginx
  Containers:
    nginx:
      Image:      nginx:1.7.9
      Port:       80/TCP
      Host Port:  0/TCP
      Environment: <none>
      Mounts:     <none>
      Volumes:    <none>
  Conditions:
    Type     Status  Reason
    ----  -----
    Available  True    MinimumReplicasAvailable
    Progressing  True    NewReplicaSetAvailable
  OldReplicaSets: <none>
  NewReplicaSet:  nginx-deployment-5754944d6c (2/2 replicas created)
Events:
  Type     Reason          Age     From               Message
  ----  -----  ---  -----
  Normal  ScalingReplicaSet 2m22s  deployment-controller  Scaled up replica set nginx-deployment-5754944d6c to 2
```

For the *replicas* setting, you will see:

```
Replicas:        2 desired | 2 updated | 2 total | 2 available | 0 unavailable
```

The *replicas* setting indicates that your deployment specification requires two pods, and that those pods were created and updated and are ready for you to use.

NOTE

A replica set replaces pods that are deleted or terminated for any reason, such as in the case of device node failure or a disruptive device upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.

3. To list the pods in your deployment:

```
kubectl get pods -l app=nginx -n <namespace-string>
```

A sample use of the command, with output, is shown below:

```
PS C:\Users\user> kubectl get pods -l app=nginx -n "test1"

NAME                      READY   STATUS    RESTARTS   AGE
nginx-deployment-5754944d6c-7wqjd  1/1     Running   0          3m13s
nginx-deployment-5754944d6c-nfj2h  1/1     Running   0          3m13s
```

The output verifies that we have two pods with unique names that we can reference using kubectl.

4. To view information on an individual pod in your deployment:

```
kubectl describe pod <podname-string> -n <namespace-string>
```

A sample use of the command, with output, is shown below:

```

PS C:\Users\user> kubectl describe pod "nginx-deployment-5754944d6c-7wqjd" -n "test1"

Name:           nginx-deployment-5754944d6c-7wqjd
Namespace:      test1
Priority:       0
Node:           k8s-1d9qh2cl-n1/10.128.46.184
Start Time:     Tue, 18 Feb 2020 13:35:29 -0800
Labels:          app=nginx
                 pod-template-hash=5754944d6c
Annotations:    <none>
Status:         Running
IP:             172.17.246.200
Controlled By:  ReplicaSet/nginx-deployment-5754944d6c
Containers:
  nginx:
    Container ID:   docker://280b0f76bfcd14cde481dc4f2b8180cf5fbfc90a084042f679d499f863c66979
    Image:          nginx:1.7.9
    Image ID:       docker-
pullable://nginx@sha256:e3456c851a152494c3e4ff5fcc26f240206abac0c9d794affb40e0714846c451
    Port:          80/TCP
    Host Port:     0/TCP
    State:         Running
      Started:     Tue, 18 Feb 2020 13:35:35 -0800
    Ready:          True
    Restart Count: 0
    Environment:   <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from default-token-8gksw (ro)
Conditions:
  Type        Status
  Initialized  True
  Ready        True
  ContainersReady  True
  PodScheduled  True
Volumes:
  default-token-8gksw:
    Type:            Secret (a volume populated by a Secret)
    SecretName:      default-token-8gksw
    Optional:        false
  QoS Class:      BestEffort
  Node-Selectors:  <none>
  Tolerations:    node.kubernetes.io/not-ready:NoExecute for 300s
                  node.kubernetes.io/unreachable:NoExecute for 300s
Events:
  Type  Reason  Age    From           Message
  ----  -----  ----  --  -----
  Normal Scheduled  4m58s  default-scheduler  Successfully assigned test1/nginx-deployment-5754944d6c-7wqjd to k8s-1d9qh2cl-n1
  Normal Pulling   4m57s  kubelet, k8s-1d9qh2cl-n1  Pulling image "nginx:1.7.9"
  Normal Pulled    4m52s  kubelet, k8s-1d9qh2cl-n1  Successfully pulled image "nginx:1.7.9"
  Normal Created   4m52s  kubelet, k8s-1d9qh2cl-n1  Created container nginx
  Normal Started   4m52s  kubelet, k8s-1d9qh2cl-n1  Started container nginx

```

Rescale the application deployment by increasing the replica count

Each pod is meant to run a single instance of a given application. If you want to scale your application horizontally to run multiple instances, you can increase the number of pods to one for each instance. In Kubernetes, this is referred to as replication. You can increase the number of pods in your application deployment by applying a new YAML file. The YAML file changes the replicas setting to 4, which increases the number of pods in your deployment to four pods. To increase the number of pods from 2 to 4:

```

PS C:\WINDOWS\system32> kubectl apply -f https://k8s.io/examples/application/deployment-scale.yaml -n
"test1"

```

Alternatively, you can save the following markdown on your local machine and substitute the path and filename for the `-f` parameter for `kubectl apply`. For instance, "C:\Kubernetes\deployment-scale.yaml". The configuration for the application deployment scale would be:

```
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  selector:
    matchLabels:
      app: nginx
  replicas: 4 # Update the replicas from 2 to 4
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: nginx:1.8
          ports:
            - containerPort: 80
```

To verify that the deployment has four pods:

```
kubectl get pods -l app=nginx
```

Example output for a rescaling deployment from two to four pods is shown below:

```
PS C:\WINDOWS\system32> kubectl get pods -l app=nginx
NAME                  READY   STATUS    RESTARTS   AGE
nginx-deployment-148880595-4zdqq  1/1     Running   0          25s
nginx-deployment-148880595-6zgi1  1/1     Running   0          25s
nginx-deployment-148880595-fxcez  1/1     Running   0          2m
nginx-deployment-148880595-rwovn  1/1     Running   0          2m
```

As you can see from the output, you now have four pods in your deployment that can run your application.

Delete a Deployment

To delete the deployment, including all the pods, you need to run `kubectl delete deployment` specifying the name of the deployment `nginx-deployment` and the namespace name. To delete the deployment:

```
kubectl delete deployment nginx-deployment -n <namespace-string>
```

An example of command usage, with output, is shown below:

```
PS C:\Users\user> kubectl delete deployment nginx-deployment -n "test1"
deployment.extensions "nginx-deployment" deleted
```

Next steps

[Kubernetes Overview](#)

Use kubectl to run a Kubernetes stateful application with a PersistentVolume on your Azure Stack Edge Pro device

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article shows you how to deploy a single-instance stateful application in Kubernetes using a PersistentVolume (PV) and a deployment. The deployment uses `kubectl` commands on an existing Kubernetes cluster and deploys the MySQL application.

This procedure is intended for those who have reviewed the [Kubernetes storage on Azure Stack Edge Pro device](#) and are familiar with the concepts of [Kubernetes storage](#).

Azure Stack Edge Pro also supports running Azure SQL Edge containers and these can be deployed in a similar way as detailed here for MySQL. For more information, see [Azure SQL Edge](#).

Prerequisites

Before you can deploy the stateful application, complete the following prerequisites on your device and the client that you will use to access the device:

For device

- You have sign-in credentials to a 1-node Azure Stack Edge Pro device.
 - The device is activated. See [Activate the device](#).
 - The device has the compute role configured via Azure portal and has a Kubernetes cluster. See [Configure compute](#).

For client accessing the device

- You have a Windows client system that will be used to access the Azure Stack Edge Pro device.
 - The client is running Windows PowerShell 5.0 or later. To download the latest version of Windows PowerShell, go to [Install Windows PowerShell](#).
 - You can have any other client with a [Supported operating system](#) as well. This article describes the procedure when using a Windows client.
 - You have completed the procedure described in [Access the Kubernetes cluster on Azure Stack Edge Pro device](#). You have:
 - Created a `usersns1` namespace via the `New-HcsKubernetesNamespace` command.
 - Created a user `user1` via the `New-HcsKubernetesUser` command.
 - Granted the `user1` access to `usersns1` via the `Grant-HcsKubernetesNamespaceAccess` command.
 - Installed `kubectl` on the client and saved the `kubeconfig` file with the user configuration to `C:\Users\<username>\.kube`.
 - Make sure that the `kubectl` client version is skewed no more than one version from the Kubernetes master version running on your Azure Stack Edge Pro device.
 - Use `kubectl version` to check the version of kubectl running on the client. Make a note of the

full version.

- In the local UI of your Azure Stack Edge Pro device, go to **Overview** and note the Kubernetes software number.
- Verify these two versions for compatibility from the mapping provided in the Supported Kubernetes version.

You are ready to deploy a stateful application on your Azure Stack Edge Pro device.

Provision a static PV

To statically provision a PV, you need to create a share on your device. Follow these steps to provision a PV against your SMB share.

NOTE

- The specific example used in this how-to article does not work with NFS shares. In general, NFS shares can be provisioned on your Azure Stack Edge device with non-database applications.
- To deploy stateful applications that use storage volumes to provide persistent storage, we recommend that you use `StatefulSet`. This example uses `Deployment` with only one replica and is suitable for development and testing.

1. Choose whether you want to create an Edge share or an Edge local share. Follow the instructions in [Add a share](#) to create a share. Make sure to select the check box for **Use the share with Edge compute**.

Add share

X

myasegpures1

Share details

Name *

mylocalsmbshare1



Type * ⓘ

SMB

NFS

Use the share with Edge compute ⓘ



Configure as Edge local share ⓘ



i Data in Edge local shares stays on the device. Use Edge modules to read from Edge local share, process, and upload data to an Edge share. To easily access share from Edge compute modules, use the local mount point. [Learn more](#)

User details

All privilege local user ⓘ

Create new

Use existing

User name *

myuser1



Password *

.....



Confirm password *

.....



Create

- Instead of creating a new share, if you decide to use an existing share, you will need to mount the share.

In the Azure portal for your Azure Stack Edge resource, go to **Shares**. From the existing list of shares, select and click a share that you want to use.

Home >

myasegpures1 | Shares

Azure Stack Edge / Data Box Gateway

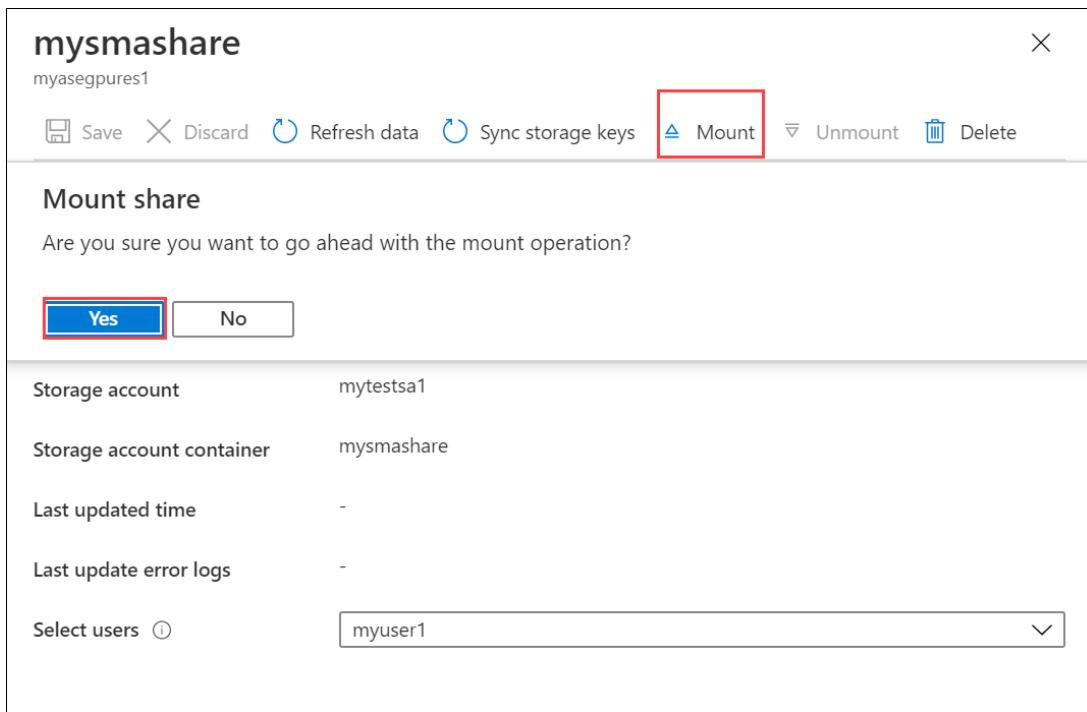
Search (Ctrl+ /) Add share Refresh

Properties Order details

Gateway Get started Users Shares Storage accounts Bandwidth

Name	Status	Type	Used for compu...	Storage account	Storage service	...
mysmashare	OK	SMB	Disabled	mytests1	Block Blob	...
mysmbshare1	OK	SMB	Enabled	mytests1	Block Blob	...

- b. Select **Mount** and confirm mounting when prompted.



2. Make a note of the share name. When this share is created, a persistent volume object is automatically created in the Kubernetes cluster corresponding to the SMB share you created.

Deploy MySQL

You will now run a stateful application by creating a Kubernetes Deployment and connecting it to the PV you created in the earlier step using a PersistentVolumeClaim (PVC).

All `kubectl` commands you use to create and manage stateful application deployments need to specify the namespace associated with the configuration. To specify the namespace in a `kubectl` command, use `kubectl <command> -n <your-namespace>`.

1. Get a list of the pods running on your Kubernetes cluster in your namespace. A pod is an application container, or process, running on your Kubernetes cluster.

```
kubectl get pods -n <your-namespace>
```

Here's an example of command usage:

```
C:\Users\user>kubectl get pods -n "userns1"
No resources found in userns1 namespace.
C:\Users\user>
```

The output should state that no resources (pods) are found because there are no applications running on your cluster.

2. You will use the following YAML files. The `mysql-deployment.yaml` file describes a deployment that runs MySQL and references the PVC. The file defines a volume mount for `/var/lib/mysql`, and then creates a PVC that looks for a 20-GB volume.

This claim is satisfied by any existing PV that was statically provisioned when you created the share in the earlier step. On your device, a large PV of 32 TB is created for each share. The PV meets the requirements set forth by PVC and the PVC should be bound to this PV.

Copy and save the following `mysql-deployment.yml` file to a folder on the Windows client that you are using to access the Azure Stack Edge Pro device.

```
apiVersion: v1
kind: Service
metadata:
  name: mysql
spec:
  ports:
  - port: 3306
  selector:
    app: mysql
  clusterIP: None
---
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: mysql
spec:
  selector:
    matchLabels:
      app: mysql
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        env:
          # Use secret in real usage
          - name: MYSQL_ROOT_PASSWORD
            value: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
        persistentVolumeClaim:
          claimName: mysql-pv-claim
```

3. Copy and save as a `mysql-pv.yml` file to the same folder where you saved the `mysql-deployment.yml`. To use the SMB share that you earlier created with `kubectl`, set the `volumeName` field in the PVC object to the name of the share.

NOTE

Make sure that the YAML files have correct indentation. You can check with [YAML lint](#) to validate and then save.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mysql-pv-claim
spec:
  volumeName: <smb-share-name-here>
  storageClassName: ""
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
```

4. Deploy the `mysql-pv.yaml` file.

```
kubectl apply -f <URI path to the mysql-pv.yml file> -n <your-user-namespace>
```

Here's a sample output of the deployment.

```
C:\Users\user>kubectl apply -f "C:\stateful-application\mysql-pv.yml" -n userns1
persistentvolumeclaim/mysql-pv-claim created

C:\Users\user>
```

Note the name of the PVC created. You will use it in a later step.

5. Deploy the contents of the `mysql-deployment.yaml` file.

```
kubectl apply -f <URI path to mysql-deployment.yml file> -n <your-user-namespace>
```

Here's a sample output of the deployment.

```
C:\Users\user>kubectl apply -f "C:\stateful-application\mysql-deployment.yml" -n userns1
service/mysql created
deployment.apps/mysql created
```

6. Display information about the deployment.

```
kubectl describe deployment <app-label> -n <your-user-namespace>
```

```
C:\Users\user>kubectl describe deployment mysql -n userns1
Name:           mysql
Namespace:      userns1
CreationTimestamp: Tue, 18 Aug 2020 09:44:58 -0700
Labels:         <none>
Annotations:   deployment.kubernetes.io/revision: 1
                kubectl.kubernetes.io/last-applied-configuration:
                  {"apiVersion":"apps/v1","kind":"Deployment","metadata":{"annotations":{},"name":"mysql","namespace":"userns1"},"spec":{"selector":{"matchL...
Selector:       app=mysql
Replicas:       1 desired | 1 updated | 1 total | 1 available | 0 unavailable
StrategyType:   Recreate
MinReadySeconds: 0
Pod Template:
  Labels:  app=mysql
  Containers:
    mysql:
      Image:      mysql:5.6
      Port:       3306/TCP
      Host Port:  0/TCP
      Environment:
        MYSQL_ROOT_PASSWORD: password
      Mounts:
        /var/lib/mysql from mysql-persistent-storage (rw)
  Volumes:
    mysql-persistent-storage:
      Type:      PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
      ClaimName: mysql-pv-claim
      ReadOnly:   false
  Conditions:
    Type     Status  Reason
    ----   -----  -----
    Progressing  True   NewReplicaSetAvailable
    Available    True   MinimumReplicasAvailable
  OldReplicaSets: <none>
  NewReplicaSet:  mysql-c85f7f79c (1/1 replicas created)
  Events:
    Type     Reason          Age     From               Message
    ----   -----  ----  -----
    Normal  ScalingReplicaSet 10m    deployment-controller  Scaled up replica set mysql-c85f7f79c to 1
C:\Users\user>
```

7. List the pods created by the deployment.

```
kubectl get pods -l <app=label> -n <your-user-namespace>
```

Here's a sample output.

```
C:\Users\user>kubectl get pods -l app=mysql -n userns1
NAME            READY   STATUS    RESTARTS   AGE
mysql-c85f7f79c-vzz7j  1/1     Running   1          14m
C:\Users\user>
```

8. Inspect the PersistentVolumeClaim.

```
kubectl describe pvc <your-pvc-name>
```

Here's a sample output.

```
C:\Users\user>kubectl describe pvc mysql-pv-claim -n userns1
Name:          mysql-pv-claim
Namespace:     userns1
StorageClass:
Status:        Bound
Volume:        mylocalsmbshare1
Labels:         <none>
Annotations:   kubectl.kubernetes.io/last-applied-configuration:
                {"apiVersion":"v1","kind":"PersistentVolumeClaim","metadata":{"annotations":{},"name":"mysql-pv-claim","namespace":"userns1"},"spec":{"acc...
                pv.kubernetes.io/bind-completed: yes
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      32Ti
Access Modes:  RWO,RWX
VolumeMode:    Filesystem
Mounted By:   mysql-c85f7f79c-vzz7j
Events:        <none>

C:\Users\user>
```

Verify MySQL is running

To run a command against a container in a pod that is running MySQL, type:

```
kubectl exec <your-pod-with-the-app> -i -t -n <your-namespace> -- mysql
```

Here's a sample output.

```
C:\Users\user>kubectl exec mysql-c85f7f79c-vzz7j -i -t -n userns1 -- mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.6.49 MySQL Community Server (GPL)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Delete a deployment

To delete the deployment, delete the deployed objects by name. These objects include deployment, service, and PVC.

```
kubectl delete deployment <deployment-name>,svc <service-name> -n <your-namespace>
kubectl delete pvc <your-pvc-name> -n <your-namespace>
```

Here's sample output of when you delete the deployment and the service.

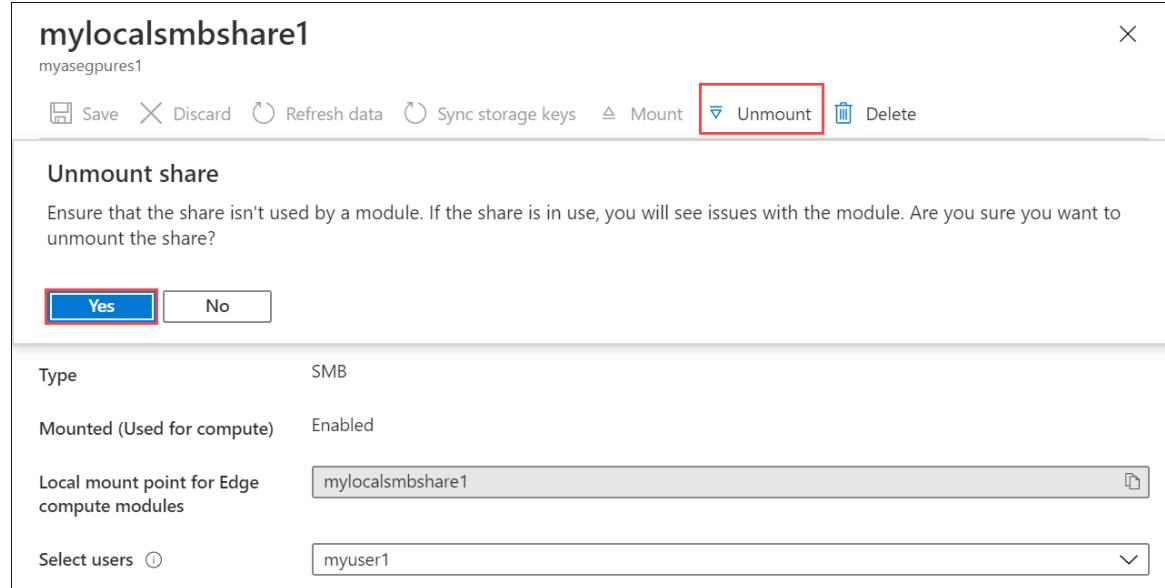
```
C:\Users\user>kubectl delete deployment,svc mysql -n userns1
deployment.apps "mysql" deleted
service "mysql" deleted
C:\Users\user>
```

Here's sample output of when you delete the PVC.

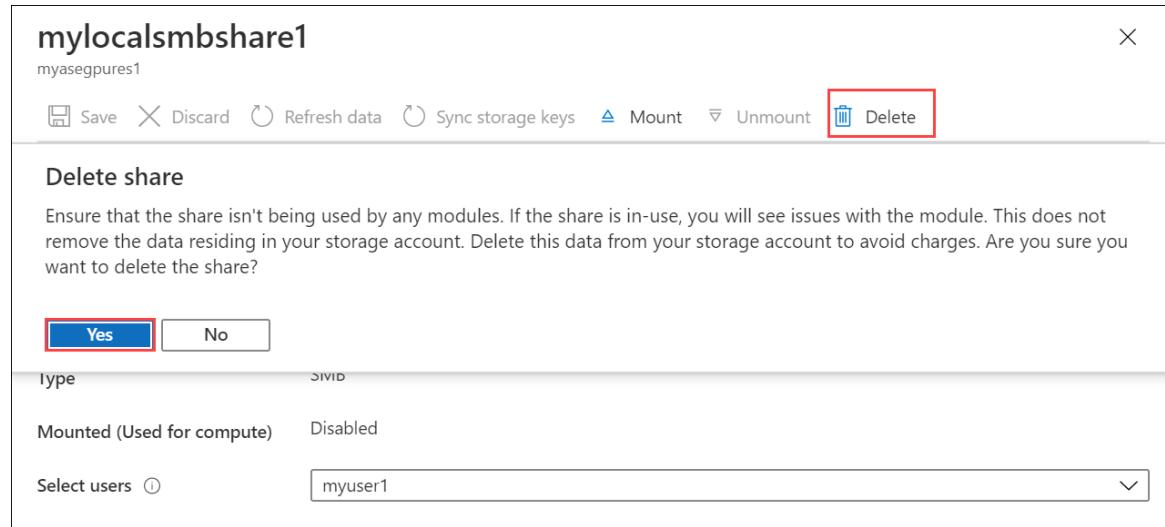
```
C:\Users\user>kubectl delete pvc mysql-pv-claim -n userns1
persistentvolumeclaim "mysql-pv-claim" deleted
C:\Users\user>
```

The PV is no longer bound to the PVC as the PVC was deleted. As the PV was provisioned when the share was created, you will need to delete the share. Follow these steps:

1. Unmount the share. In Azure portal, go to your **Azure Stack Edge resource > Shares** and select and click the share you want to unmount. Select **Unmount** and confirm the operation. Wait until the share is unmounted. The unmounting releases the share (and hence the associated PersistentVolume) from the Kubernetes cluster.



2. You can now select **Delete** and confirm deletion to delete your share. This should also delete the share and the corresponding PV.



Next steps

To understand how to dynamically provision storage, see [Deploy a stateful application via dynamic provisioning on an Azure Stack Edge Pro device](#)

Use kubectl to run a Kubernetes stateful application with StorageClass on your Azure Stack Edge Pro GPU device

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article shows you how to deploy a single-instance stateful application in Kubernetes using a StorageClass to dynamically provision storage and a deployment. The deployment uses `kubectl` commands on an existing Kubernetes cluster and deploys the MySQL application.

This procedure is intended for those who have reviewed the [Kubernetes storage on Azure Stack Edge Pro device](#) and are familiar with the concepts of [Kubernetes storage](#).

Prerequisites

Before you can deploy the stateful application, complete the following prerequisites on your device and the client that you will use to access the device:

For device

- You have sign-in credentials to a 1-node Azure Stack Edge Pro device.
 - The device is activated. See [Activate the device](#).
 - The device has the compute role configured via Azure portal and has a Kubernetes cluster. See [Configure compute](#).

For client accessing the device

- You have a Windows client system that will be used to access the Azure Stack Edge Pro device.
 - The client is running Windows PowerShell 5.0 or later. To download the latest version of Windows PowerShell, go to [Install Windows PowerShell](#).
 - You can have any other client with a [Supported operating system](#) as well. This article describes the procedure when using a Windows client.
 - You have completed the procedure described in [Access the Kubernetes cluster on Azure Stack Edge Pro device](#). You have:
 - Created a `userns1` namespace via the `New-HcsKubernetesNamespace` command.
 - Created a user `user1` via the `New-HcsKubernetesUser` command.
 - Granted the `user1` access to `userns1` via the `Grant-HcsKubernetesNamespaceAccess` command.
 - Installed `kubectl` on the client and saved the `kubeconfig` file with the user configuration to `C:\Users\<username>\.kube`.
 - Make sure that the `kubectl` client version is skewed no more than one version from the Kubernetes master version running on your Azure Stack Edge Pro device.
 - Use `kubectl version` to check the version of kubectl running on the client. Make a note of the full version.
 - In the local UI of your Azure Stack Edge Pro device, go to [Overview](#) and note the Kubernetes software number.

- Verify these two versions for compatibility from the mapping provided in the Supported Kubernetes version.

You are ready to deploy a stateful application on your Azure Stack Edge Pro device.

Deploy MySQL

You will now run a stateful application by creating a Kubernetes Deployment and connecting it to the built-in StorageClass using a PersistentVolumeClaim (PVC).

All `kubectl` commands you use to create and manage stateful application deployments need to specify the namespace associated with the configuration. To specify the namespace in a `kubectl` command, use `kubectl <command> -n <your-namespace>`.

1. Get a list of the pods running on your Kubernetes cluster in your namespace. A pod is an application container, or process, running on your Kubernetes cluster.

```
kubectl get pods -n <your-namespace>
```

Here's an example of command usage:

```
C:\Users\user>kubectl get pods -n "userns1"
No resources found in userns1 namespace.
C:\Users\user>
```

The output should state that no resources (pods) are found because there are no applications running on your cluster.

2. You will use the following YAML files. The `mysql-deployment.yml` file describes a deployment that runs MySQL and references the PVC. The file defines a volume mount for `/var/lib/mysql`, and then creates a PVC that looks for a 20-GB volume. A dynamic PV is provisioned and the PVC is bound to this PV.

Copy and save the following `mysql-deployment.yml` file to a folder on the Windows client that you are using to access the Azure Stack Edge Pro device.

```

apiVersion: v1
kind: Service
metadata:
  name: mysql
spec:
  ports:
  - port: 3306
  selector:
    app: mysql
  clusterIP: None
---
apiVersion: apps/v1 # for versions before 1.9.0 use apps/v1beta2
kind: Deployment
metadata:
  name: mysql
spec:
  selector:
    matchLabels:
      app: mysql
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        env:
          # Use secret in real usage
          - name: MYSQL_ROOT_PASSWORD
            value: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
        persistentVolumeClaim:
          claimName: mysql-pv-claim-sc

```

3. Copy and save as a `mysql-pvc.yml` file to the same folder where you saved the `mysql-deployment.yml`. To use the builtin StorageClass that Azure Stack Edge Pro device on an attached data disk, set the `storageClassName` field in the PVC object to `ase-node-local` and accessModes should be `ReadWriteOnce`.

NOTE

Make sure that the YAML files have correct indentation. You can check with [YAML lint](#) to validate and then save.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mysql-pv-claim-sc
spec:
  storageClassName: ase-node-local
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
```

4. Deploy the `mysql-pvc.yaml` file.

```
kubectl apply -f <URI path to the mysql-pv.yml file> -n <your-user-namespace>
```

Here's a sample output of the deployment.

```
C:\Users\user>kubectl apply -f "C:\stateful-application\mysql-pvc.yaml" -n userns1
persistentvolumeclaim/mysql-pv-claim-sc created
C:\Users\user>
```

Note the name of the PVC created - in this example, `mysql-pv-claim-sc`. You will use it in a later step.

5. Deploy the contents of the `mysql-deployment.yaml` file.

```
kubectl apply -f <URI path to mysql-deployment.yaml file> -n <your-user-namespace>
```

Here's a sample output of the deployment.

```
C:\Users\user>kubectl apply -f "C:\stateful-application\mysql-deployment.yaml" -n userns1
service/mysql created
deployment.apps/mysql created
C:\Users\user>
```

6. Display information about the deployment.

```
kubectl describe deployment <app-label> -n <your-user-namespace>
```

```
C:\Users\user>kubectl describe deployment mysql -n userns1
Name:           mysql
Namespace:      userns1
CreationTimestamp: Thu, 20 Aug 2020 11:14:25 -0700
Labels:         <none>
Annotations:   deployment.kubernetes.io/revision: 1
                kubectl.kubernetes.io/last-applied-configuration:
                  {"apiVersion":"apps/v1","kind":"Deployment","metadata":{"annotations":{},"name":"mysql","namespace":"userns1"},"spec":{"selector":{"matchL...
Selector:       app=mysql
Replicas:       1 desired | 1 updated | 1 total | 1 available | 0 unavailable
StrategyType:   Recreate
MinReadySeconds: 0
Pod Template:
  Labels:  app=mysql
  Containers:
    mysql:
      Image:  mysql:5.6
      Port:   3306/TCP
      Host Port: 0/TCP
      Environment:
        MYSQL_ROOT_PASSWORD: password
      Mounts:
        /var/lib/mysql from mysql-persistent-storage (rw)
  Volumes:
    mysql-persistent-storage:
      Type:     PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
      ClaimName: mysql-pv-claim-sc
      ReadOnly:  false
  Conditions:
    Type        Status  Reason
    ----        ----   -----
    Available   True    MinimumReplicasAvailable
    Progressing True    NewReplicaSetAvailable
  OldReplicaSets: <none>
  NewReplicaSet:  mysql-695c4d9dcd (1/1 replicas created)
Events:
  Type  Reason          Age   From            Message
  ----  -----          ---   ----            -----
  Normal  ScalingReplicaSet  24s   deployment-controller  Scaled up replica set mysql-695c4d9dcd to 1
C:\Users\user>
```

7. List the pods created by the deployment.

```
kubectl get pods -l <app=label> -n <your-user-namespace>
```

Here's a sample output.

```
C:\Users\user>kubectl get pods -l app=mysql -n userns1
NAME           READY   STATUS    RESTARTS   AGE
mysql-695c4d9dcd-rvzff  1/1     Running   0          40s
C:\Users\user>
```

8. Inspect the PersistentVolumeClaim.

```
kubectl describe pvc <your-pvc-name>
```

Here's a sample output.

```
C:\Users\user>kubectl describe pvc mysql-pv-claim-sc -n userns1
Name:      mysql-pv-claim-sc
Namespace:  userns1
StorageClass:  ase-node-local
Status:     Bound
Volume:    pvc-dc48253c-82dc-42a4-a7c6-aaddc97c9b8a
Labels:    <none>
Annotations:  kubectl.kubernetes.io/last-applied-configuration:
              {"apiVersion":"v1","kind":"PersistentVolumeClaim","metadata":{"annotations":{},"name":"mysql-pv-claim-sc","namespace":"userns1"},"spec":...
              pv.kubernetes.io/bind-completed: yes
              pv.kubernetes.io/bound-by-controller: yes
              volume.beta.kubernetes.io/storage-provisioner: rancher.io/local-path
              volume.kubernetes.io/selected-node: k8s-3q7lhq2cl-3q7lhq2
Finalizers: [kubernetes.io/pvc-protection]
Capacity:   20Gi
Access Modes: RWO
VolumeMode:  Filesystem
Mounted By:  mysql-695c4d9dcd-rvzff
Events:
  Type    Reason          Age           From
Message
  ----  -----  ----  -----
  Normal  WaitForFirstConsumer  71s (x2 over 77s)  persistentvolume-controller
  waiting for first consumer to be created before binding
  Normal  ExternalProvisioning  62s           persistentvolume-controller
  waiting for a volume to be created, either by external provisioner "rancher.io/local-path" or
  manually created by system administrator
  Normal  Provisioning        62s           rancher.io/local-path_local-path-provisioner-
  6b84988bf9-tx8mz_1896d824-f862-4cbf-912a-c8cc0ca05574  External provisioner is provisioning volume
  for claim "userns1/mysql-pv-claim-sc"
  Normal  ProvisioningSucceeded 60s           rancher.io/local-path_local-path-provisioner-
  6b84988bf9-tx8mz_1896d824-f862-4cbf-912a-c8cc0ca05574  Successfully provisioned volume pvc-dc48253c-
  82dc-42a4-a7c6-aaddc97c9b8a
C:\Users\user>
```

Verify MySQL is running

To verify that the application is running, type:

```
kubectl exec <your-pod-with-the-app> -i -t -n <your-namespace> -- mysql -p
```

When prompted, provide the password. The password is in your `mysql-deployment` file.

Here's a sample output.

```
C:\Users\user>kubectl exec mysql-695c4d9dcd-rvzff -i -t -n userns1 -- mysql -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.6.49 MySQL Community Server (GPL)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
```

Delete a deployment

To delete the deployment, delete the deployed objects by name. These objects include deployment, service, and PVC.

```
kubectl delete deployment <deployment-name>,svc <service-name> -n <your-namespace>
kubectl delete pvc <your-pvc-name> -n <your-namespace>
```

Here's sample output of when you delete the deployment and the service.

```
C:\Users\user>kubectl delete deployment,svc mysql -n userns1
deployment.apps "mysql" deleted
service "mysql" deleted
C:\Users\user>
```

Here's sample output of when you delete the PVC.

```
C:\Users\user>kubectl delete pvc mysql-pv-claim-sc -n userns1
persistentvolumeclaim "mysql-pv-claim-sc" deleted
C:\Users\user>
```

Next steps

To understand how to configure networking via kubectl, see [Deploy a stateless application on an Azure Stack Edge Pro device](#)

Deploy a Kubernetes workload using GPU sharing on your Azure Stack Edge Pro

9/21/2022 • 12 minutes to read • [Edit Online](#)

This article describes how containerized workloads can share the GPUs on your Azure Stack Edge Pro GPU device. In this article, you will run two jobs, one without the GPU context-sharing and one with the context-sharing enabled via the the Multi-Process Service (MPS) on the device. For more information, see the [Multi-Process Service](#).

Prerequisites

Before you begin, make sure that:

1. You've access to an Azure Stack Edge Pro GPU device that is [activated](#) and has [compute configured](#). You have the [Kubernetes API endpoint](#) and you have added this endpoint to the `hosts` file on your client that will be accessing the device.
2. You've access to a client system with a [Supported operating system](#). If using a Windows client, the system should run PowerShell 5.0 or later to access the device.
3. You have created a namespace and a user. You have also granted user the access to this namespace. You have the kubeconfig file of this namespace installed on the client system that you'll use to access your device. For detailed instructions, see [Connect to and manage a Kubernetes cluster via kubectl on your Azure Stack Edge Pro GPU device](#).
4. Save the following deployment `yml` on your local system. You'll use this file to run Kubernetes deployment. This deployment is based on [Simple CUDA containers](#) that are publicly available from Nvidia.

```

apiVersion: batch/v1
kind: Job
metadata:
  name: cuda-sample1
spec:
  template:
    spec:
      hostPID: true
      hostIPC: true
      containers:
        - name: cuda-sample-container1
          image: nvidia/samples:nbody
          command: ["/tmp/nbody"]
          args: ["-benchmark", "-i=1000"]
          env:
            - name: NVIDIA_VISIBLE_DEVICES
              value: "0"
      restartPolicy: "Never"
      backoffLimit: 1
  ---
apiVersion: batch/v1
kind: Job
metadata:
  name: cuda-sample2
spec:
  template:
    metadata:
      spec:
        hostPID: true
        hostIPC: true
        containers:
          - name: cuda-sample-container2
            image: nvidia/samples:nbody
            command: ["/tmp/nbody"]
            args: ["-benchmark", "-i=1000"]
            env:
              - name: NVIDIA_VISIBLE_DEVICES
                value: "0"
        restartPolicy: "Never"
        backoffLimit: 1

```

Verify GPU driver, CUDA version

The first step is to verify that your device is running required GPU driver and CUDA versions.

1. [Connect to the PowerShell interface of your device.](#)

2. Run the following command:

```
Get-HcsGpuNvidiaSmi
```

3. In the Nvidia smi output, make a note of the GPU version and the CUDA version on your device. If you are running Azure Stack Edge 2102 software, this version would correspond to the following driver versions:

- GPU driver version: 460.32.03
- CUDA version: 11.2

Here is an example output:

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Wed Mar  3 12:24:27 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2 |
|-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id     Disp.A | Volatile Uncorr. ECC | | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
| |          |          |             |            |          |          MIG M. |
|-----+-----+-----+-----+
| 0  Tesla T4           On   | 00002C74:00:00.0 Off  |          0 | | | | |
| N/A   34C   P8    9W / 70W |        0MiB / 15109MiB |       0%  Default |
| |          |          |             |            |          |          N/A |
+-----+-----+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory |
|       ID  ID
|-----+-----+-----+-----+-----+-----+
| No running processes found
+-----+
[10.100.10.10]: PS>
```

- Keep this session open as you will use it to view the Nvidia smi output throughout the article.

Job without context-sharing

You'll run the first job to deploy an application on your device in the namespace `mynamesp1`. This application deployment will also show that the GPU context-sharing is not enabled by default.

- List all the pods running in the namespace. Run the following command:

```
kubectl get pods -n <Name of the namespace>
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
No resources found.
```

- Start a deployment job on your device using the `deployment.yaml` provided earlier. Run the following command:

```
kubectl apply -f <Path to the deployment .yaml> -n <Name of the namespace>
```

This job creates two containers and runs an n-body simulation on both the containers. The number of simulation iterations are specified in the `.yaml`. For more information, see [N-body simulation](#).

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl apply -f -n mynamesp1 C:\gpu-sharing\k8-gpusharing.yaml
job.batch/cuda-sample1 created
job.batch/cuda-sample2 created
PS C:\WINDOWS\system32>
```

- To list the pods started in the deployment, run the following command:

```
kubectl get pods -n <Name of the namespace>
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
NAME        READY   STATUS    RESTARTS   AGE
cuda-sample1-27srm  1/1     Running   0          28s
cuda-sample2-db9vx  1/1     Running   0          27s
PS C:\WINDOWS\system32>
```

There are two pods, `cuda-sample1-cf979886d-xcwsq` and `cuda-sample2-68b4899948-vcv68` running on your device.

4. Fetch the details of the pods. Run the following command:

```
kubectl -n <Name of the namespace> describe <Name of the job>
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl -n mynamesp1 describe job.batch/cuda-sample1; kubectl -n mynamesp1
describe job.batch/cuda-sample2
Name:           cuda-sample1
Namespace:      mynamesp1
Selector:       controller-uid=22783f76-6af1-490d-b6eb-67dd4cda0e1f
Labels:         controller-uid=22783f76-6af1-490d-b6eb-67dd4cda0e1f
               job-name=cuda-sample1
Annotations:   kubectl.kubernetes.io/last-applied-configuration:
               {"apiVersion":"batch/v1","kind":"Job","metadata":{"annotations":{},"name":"cuda-
sample1","namespace":"mynamesp1"},"spec":{"backoffLimit":1...
Parallelism:   1
Completions:   1
Start Time:    Wed, 03 Mar 2021 12:25:34 -0800
Pods Statuses: 1 Running / 0 Succeeded / 0 Failed
Pod Template:
  Labels:  controller-uid=22783f76-6af1-490d-b6eb-67dd4cda0e1f
           job-name=cuda-sample1
  Containers:
    cuda-sample-container1:
      Image:      nvidia/samples:nbody
      Port:       <none>
      Host Port: <none>
      Command:
        /tmp/nbody
      Args:
        -benchmark
        -i=10000
      Environment:
        NVIDIA_VISIBLE_DEVICES:  0
      Mounts:             <none>
      Volumes:            <none>
  Events:
    Type      Reason     Age     From           Message
    ----      -----     --     --              --
    Normal    SuccessfulCreate  60s    job-controller  Created pod: cuda-sample1-27srm
Name:           cuda-sample2
Namespace:      mynamesp1
Selector:       controller-uid=e68c8d5a-718e-4880-b53f-26458dc24381
Labels:         controller-uid=e68c8d5a-718e-4880-b53f-26458dc24381
               job-name=cuda-sample2
Annotations:   kubectl.kubernetes.io/last-applied-configuration:
               {"apiVersion":"batch/v1","kind":"Job","metadata":{"annotations":{},"name":"cuda-
sample2","namespace":"mynamesp1"},"spec":{"backoffLimit":1...
```

```
Parallelism: 1
Completions: 1
Start Time: Wed, 03 Mar 2021 12:25:35 -0800
Pods Statuses: 1 Running / 0 Succeeded / 0 Failed
Pod Template:
  Labels: controller-uid=e68c8d5a-718e-4880-b53f-26458dc24381
           job-name=cuda-sample2
  Containers:
    cuda-sample-container2:
      Image: nvidia/samples:nbody
      Port: <none>
      Host Port: <none>
      Command:
        /tmp/nbody
      Args:
        -benchmark
        -i=10000
      Environment:
        NVIDIA_VISIBLE_DEVICES: 0
      Mounts: <none>
      Volumes: <none>
  Events:
    Type      Reason          Age   From            Message
    ----      -----          ---   ----
    Normal    SuccessfulCreate 60s   job-controller  Created pod: cuda-sample2-db9vx
PS C:\WINDOWS\system32>
```

The output indicates that both the pods were successfully created by the job.

5. While both the containers are running the n-body simulation, view the GPU utilization from the Nvidia smi output. Go to the PowerShell interface of the device and run `Get-HcsGpuNvidiaSmi`.

Here is an example output when both the containers are running the n-body simulation:

As you can see, there are two containers (Type = C) running with n-body simulation on GPU 0.

6. Monitor the n-body simulation. Run the `get pod` commands. Here is an example output when the simulation is running.

```
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
NAME             READY   STATUS    RESTARTS   AGE
cuda-sample1-27srm  1/1     Running   0          70s
cuda-sample2-db9vx  1/1     Running   0          69s
PS C:\WINDOWS\system32>
```

When the simulation is complete, the output will indicate that. Here is an example output:

```
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
NAME             READY   STATUS      RESTARTS   AGE
cuda-sample1-27srm  0/1     Completed   0          2m54s
cuda-sample2-db9vx  0/1     Completed   0          2m53s
PS C:\WINDOWS\system32>
```

- After the simulation is complete, you can view the logs and the total time for the completion of the simulation. Run the following command:

```
kubectl logs -n <Name of the namespace> <pod name>
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl logs -n mynamesp1 cuda-sample1-27srm
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// CUT =====// CUT =====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 170398.766 ms
= 98.459 billion interactions per second
= 1969.171 single-precision GFLOP/s at 20 flops per interaction
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> kubectl logs -n mynamesp1 cuda-sample2-db9vx
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// CUT =====// CUT =====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 170368.859 ms
= 98.476 billion interactions per second
= 1969.517 single-precision GFLOP/s at 20 flops per interaction
PS C:\WINDOWS\system32>
```

- There should be no processes running on the GPU at this time. You can verify this by viewing the GPU utilization using the Nvidia smi output.

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Wed Mar  3 12:32:52 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2    |
+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A  | Volatile Uncorr. ECC  | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M.  |
| |          |          |              |             | MIG M.               |
+-----+
|  0  Tesla T4           On     | 00002C74:00:00.0 Off    |                0 | | | |
| N/A   38C   P8    9W / 70W |        0MiB / 15109MiB |      0%     Default |
| |          |          |              |             | N/A                 |
+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory  |
|       ID  ID
+-----+
| No running processes found
+-----+
[10.100.10.10]: PS>
```

Job with context-sharing

You'll run the second job to deploy the n-body simulation on two CUDA containers when GPU context-sharing is enabled through the MPS. First, you'll enable MPS on the device.

1. [Connect to the PowerShell interface of your device](#).
2. To enable MPS on your device, run the `Start-HcsGpuMPS` command.

```
[10.100.10.10]: PS>Start-HcsGpuMPS
K8S-1HXQG13CL-1HXQG13:

Set compute mode to EXCLUSIVE_PROCESS for GPU 00002C74:00:00.0.
All done.
Created nvidia-mps.service
[10.100.10.10]: PS>
```

3. Run the job using the same deployment `yaml` you used earlier. You may need to delete the existing deployment. See [Delete deployment](#).

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl -n mynamesp1 delete -f C:\gpu-sharing\k8-gpusharing.yaml
job.batch "cuda-sample1" deleted
job.batch "cuda-sample2" deleted
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
No resources found.
PS C:\WINDOWS\system32> kubectl -n mynamesp1 apply -f C:\gpu-sharing\k8-gpusharing.yaml
job.batch/cuda-sample1 created
job.batch/cuda-sample2 created
PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
NAME          READY  STATUS    RESTARTS  AGE
cuda-sample1-vcznt  1/1    Running   0          21s
cuda-sample2-zkx4w  1/1    Running   0          21s
PS C:\WINDOWS\system32> kubectl -n mynamesp1 describe job.batch/cuda-sample1; kubectl -n mynamesp1
describe job.batch/cuda-sample2
Name:          cuda-sample1
```

```

Namespace:      mynamesp1
Selector:       controller-uid=ed06bdf0-a282-4b35-a2a0-c0d36303a35e
Labels:         controller-uid=ed06bdf0-a282-4b35-a2a0-c0d36303a35e
                job-name=cuda-sample1
Annotations:   kubectl.kubernetes.io/last-applied-configuration:
                  {"apiVersion":"batch/v1","kind":"Job","metadata":{"annotations":{},"name":"cuda-sample1"},"namespace":"mynamesp1"},"spec":{"backoffLimit":1...
Parallelism:   1
Completions:   1
Start Time:    Wed, 03 Mar 2021 21:51:51 -0800
Pods Statuses: 1 Running / 0 Succeeded / 0 Failed
Pod Template:
  Labels:  controller-uid=ed06bdf0-a282-4b35-a2a0-c0d36303a35e
            job-name=cuda-sample1
  Containers:
    cuda-sample-container1:
      Image:    nvidia/samples:nbody
      Port:     <none>
      Host Port: <none>
      Command:
        /tmp/nbody
      Args:
        -benchmark
        -i=10000
      Environment:
        NVIDIA_VISIBLE_DEVICES:  0
      Mounts:          <none>
      Volumes:         <none>
  Events:
    Type   Reason        Age   From           Message
    ----  -----        ---  --  -----
    Normal SuccessfulCreate 46s   job-controller  Created pod: cuda-sample1-vcznt
Name:      cuda-sample2
Namespace:  mynamesp1
Selector:   controller-uid=6282b8fa-e76d-4f45-aa85-653ee0212b29
Labels:     controller-uid=6282b8fa-e76d-4f45-aa85-653ee0212b29
            job-name=cuda-sample2
Annotations: kubectl.kubernetes.io/last-applied-configuration:
                  {"apiVersion":"batch/v1","kind":"Job","metadata":{"annotations":{},"name":"cuda-sample2"},"namespace":"mynamesp1"},"spec":{"backoffLimit":1...
Parallelism: 1
Completions: 1
Start Time:  Wed, 03 Mar 2021 21:51:51 -0800
Pods Statuses: 1 Running / 0 Succeeded / 0 Failed
Pod Template:
  Labels:  controller-uid=6282b8fa-e76d-4f45-aa85-653ee0212b29
            job-name=cuda-sample2
  Containers:
    cuda-sample-container2:
      Image:    nvidia/samples:nbody
      Port:     <none>
      Host Port: <none>
      Command:
        /tmp/nbody
      Args:
        -benchmark
        -i=10000
      Environment:
        NVIDIA_VISIBLE_DEVICES:  0
      Mounts:          <none>
      Volumes:         <none>
  Events:
    Type   Reason        Age   From           Message
    ----  -----        ---  --  -----
    Normal SuccessfulCreate 47s   job-controller  Created pod: cuda-sample2-zkx4w
PS C:\WINDOWS\system32>
```

4. While the simulation is running, you can view the Nvidia smi output. The output shows processes

corresponding to the cuda containers (M + C type) with n-body simulation and the MPS service (C type) as running. All these processes share GPU 0.

```
PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Mon Mar  3 21:54:50 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2    |
|-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id     Disp.A | Volatile Uncorr. ECC | | |
| Fan  Temp  Perf  Pwr:Usage/Cap|          Memory-Usage | GPU-Util  Compute M. |
| |           |                               |             |          MIG M. |
|-----+-----+-----+-----+
| 0  Tesla T4          On | 0000E00B:00:00.0 Off |          0 | | |
| N/A   45C   P0    68W /  70W |      242MiB / 15109MiB |    100%   E. Process |
| |           |                               |             |          N/A |
+-----+-----+-----+
+-----+
| Processes:                               |
| GPU  GI  CI      PID  Type  Process name        GPU Memory |
|       ID  ID                               Usage  |
|-----+-----+-----+-----+
| 0    N/A N/A  144377  M+C   /tmp/nbody          107MiB |
| 0    N/A N/A  144379  M+C   /tmp/nbody          107MiB |
| 0    N/A N/A  144443    C   nvidia-cuda-mps-server  25MiB |
+-----+
```

5. After the simulation is complete, you can view the logs and the total time for the completion of the simulation. Run the following command:

```

PS C:\WINDOWS\system32> kubectl get pods -n mynamesp1
NAME          READY   STATUS    RESTARTS   AGE
cuda-sample1-vcznt  0/1     Completed  0          5m44s
cuda-sample2-zkx4w  0/1     Completed  0          5m44s
PS C:\WINDOWS\system32> kubectl logs -n mynamesp1 cuda-sample1-vcznt
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// CUT //=====// CUT //=====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 154979.453 ms
= 108.254 billion interactions per second
= 2165.089 single-precision GFLOP/s at 20 flops per interaction

PS C:\WINDOWS\system32> kubectl logs -n mynamesp1 cuda-sample2-zkx4w
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// CUT //=====// CUT //=====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 154986.734 ms
= 108.249 billion interactions per second
= 2164.987 single-precision GFLOP/s at 20 flops per interaction
PS C:\WINDOWS\system32>

```

- After the simulation is complete, you can view the Nvidia smi output again. Only the nvidia-cuda-mps-server process for the MPS service shows as running.

```

PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Mon Mar  3 21:59:55 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2 |
+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A | Volatile Uncorr. ECC | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
|                   |             |           |               MIG M. |
+-----+
|  0  Tesla T4          On  | 0000E00B:00:00.0 Off |          0 | |
| N/A   37C   P8    9W /  70W |    28MiB / 15109MiB |     0%   E. Process |
|                   |             |           |               N/A |
+-----+
+-----+
| Processes:                               |
| GPU  GI  CI      PID  Type  Process name        GPU Memory |
|       ID  ID                  |                 Usage  |
|-----+
|  0  N/A  N/A  144443      C  nvidia-cuda-mps-server  25MiB |
+-----+

```

Delete deployment

You may need to delete deployments when running with MPS enabled and with MPS disable on your device.

To delete the deployment on your device, run the following command:

```
kubectl delete -f <Path to the deployment .yaml> -n <Name of the namespace>
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl delete -f 'C:\gpu-sharing\k8-gpusharing.yaml' -n mynamesp1
deployment.apps "cuda-sample1" deleted
deployment.apps "cuda-sample2" deleted
PS C:\WINDOWS\system32>
```

Next steps

- [Deploy an IoT Edge workload with GPU sharing on your Azure Stack Edge Pro.](#)

Use IoT Edge module to run a Kubernetes stateless application on your Azure Stack Edge Pro GPU device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how you can use an IoT Edge module to deploy a stateless application on your Azure Stack Edge Pro device.

To deploy the stateless application, you'll take the following steps:

- Ensure that prerequisites are completed before you deploy an IoT Edge module.
- Add an IoT Edge module to access compute network on your Azure Stack Edge Pro.
- Verify the module can access the enabled network interface.

In this how-to article, you'll use a webserver app module to demonstrate the scenario.

Prerequisites

Before you begin, you'll need:

- An Azure Stack Edge Pro device. Make sure that:
 - Compute network settings are configured on the device.
 - Device is activated as per the steps in [Tutorial: Activate your device](#).
- You've completed **Configure compute** step as per the [Tutorial: Configure compute on your Azure Stack Edge Pro device](#) on your device. Your device should have an associated IoT Hub resource, an IoT device, and an IoT Edge device.

Add webserver app module

Take the following steps to add a webserver app module on your Azure Stack Edge Pro device.

1. In the IoT Hub resource associated with your device, go to **Automatic Device Management > IoT Edge**.
2. Select and click the IoT Edge device associated with your Azure Stack Edge Pro device.

The screenshot shows the Azure IoT Edge devices management interface. On the left, there's a sidebar with sections like Built-in endpoints, Failover, Properties, Locks, Export template, Explorers (Query explorer, IoT devices), Automatic Device Management (IoT Edge, IoT device configuration), Messaging (File upload, Message routing), and a Search bar at the top.

The main area displays IoT Edge devices. A summary table shows one device: myasegpures1-edge. The table columns are Device ID, Runtime Response, IoT Edge Module Count, Connected Client Count, and Deployment Count. The first row is highlighted with a red box.

Device ID	Runtime Response	IoT Edge Module Count	Connected Client Count	Deployment Count
myasegpures1-edge	OK	3	1	0

3. Select **Set modules**. On **Set modules on device**, select **+ Add** and then select **IoT Edge Module**.

The screenshot shows the 'Set modules on device' page for the device 'myasegpures1-edge'. The 'Modules' tab is selected. In the 'IoT Edge Modules' section, there's a table with columns: NAME, ADDRESS, USER NAME, and PASSWORD. Below the table, there's a section for 'Container Registry Credentials' with fields for Name, Address, User name, and Password.

The 'IoT Edge Modules' table has three rows:

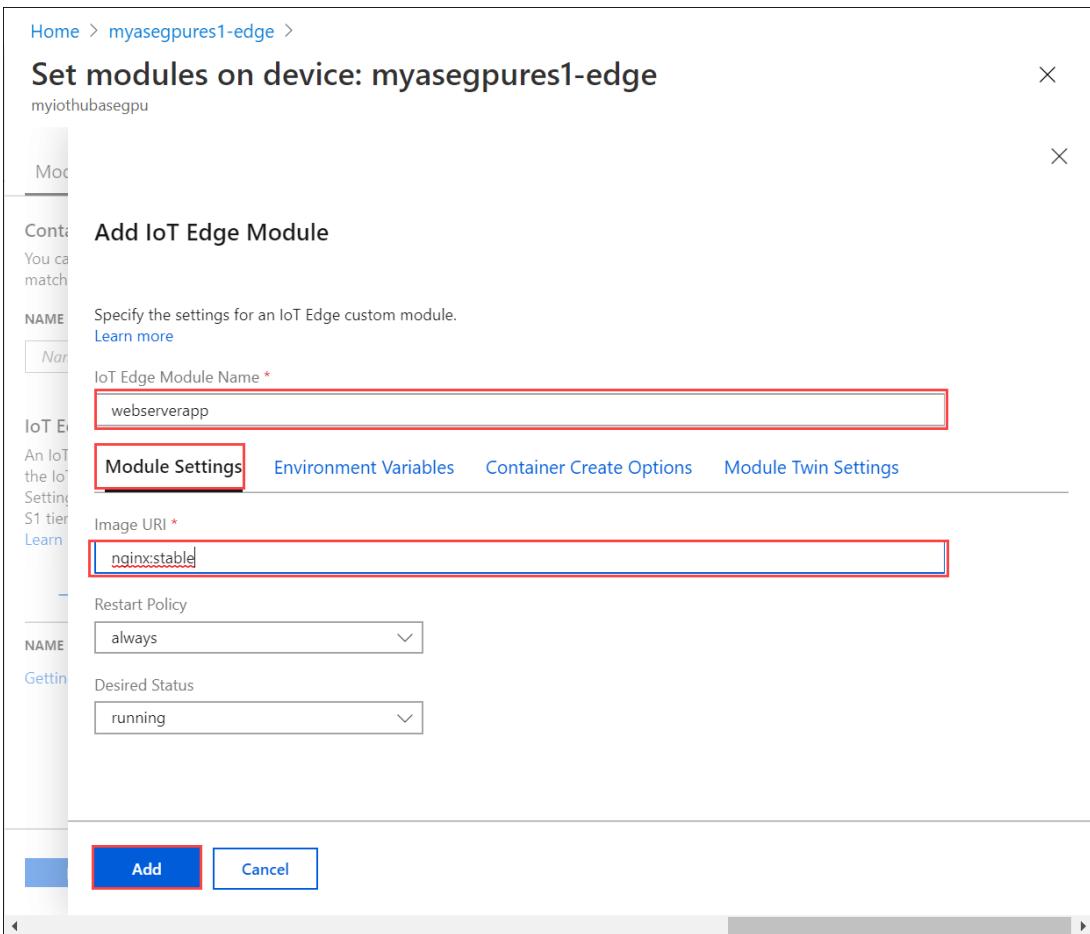
NAME	ADDRESS	USER NAME	PASSWORD
Name	Address	User name	Password
Get			

Below the table, there's a section for 'IoT Edge Modules' with a list of modules: IoT Edge Module, Marketplace Module, and Azure Stream Analytics Module. The 'IoT Edge Module' item is selected and highlighted with a red box. There are 'Add' and 'Runtime Settings' buttons above the list.

At the bottom, there are navigation buttons: 'Review + create' (highlighted with a red box), '< Previous', 'Next: Routes >', and a horizontal scrollbar.

4. In the **Add IoT Edge module**:

- Specify a **Name** for your webserver app module that you want to deploy.
- Under **Module settings** tab, provide an **Image URI** for your module image. A module matching the provided name and tags is retrieved. In this case, `mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine` will pull an nginx image (tagged as 1.15.5-alpine) from the public `mcr.microsoft.com` registry.



c. In the **Container Create Options** tab, paste the following sample code:

```
{  
    "HostConfig": {  
        "PortBindings": {  
            "80/tcp": [  
                {  
                    "HostPort": "8080"  
                }  
            ]  
        }  
    }  
}
```

This configuration lets you access the module using the compute network IP over *http* on TCP port 8080 (with the default webserver port being 80). Select **Add**.

Device ID: myasegpures1-edge

Primary Key:
Secondary Key:

Primary Connection String:
Secondary Connection String:

IoT Edge Runtime Response: 200 -- OK

Enable connection to IoT Hub: Enable Disable

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME ST...	EXIT CO...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
GettingStartedwithGPUs	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
webserverapp	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

d. Select **Review + create**. Review the module details and select **Create**.

Verify module access

1. Verify the module is successfully deployed and is running. On the **Modules** tab, the runtime status of the module should be **running**.

Device ID: myasegpures1-edge

Primary Key:
Secondary Key:

Primary Connection String:
Secondary Connection String:

IoT Edge Runtime Response: 200 -- OK

Enable connection to IoT Hub: Enable Disable

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME ST...	EXIT CO...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
GettingStartedwithGPUs	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
webserverapp	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

2. To get the external endpoint of the webserver app, [access the Kubernetes dashboard](#).
3. In the left-pane of the dashboard, filter by **iotedge** namespace. Go to **Discovery and Load balancing > Services**. Under the list of services listed, locate the external endpoint for the webserver app module.

The screenshot shows the Kubernetes Services page with the following details:

Name	Labels	Cluster IP	Internal Endpoints	External Endpoints	Created
edgehub	net.azure-devices.edge.deviceId: myasequires1-edge net.azure-devices.edge.module: edgehub	10.103.52.225	edghub.iotedge:443 TCP edghub.iotedge:31987 TCP edghub.iotedge:5671 TCP edghub.iotedge:3238 TCP edghub.iotedge:8883 TCP edghub.iotedge:30618 TCP	10.128.44.243:443 10.128.44.243:5671 10.128.44.243:8883	18 hours ago
iotedge	app.kubernetes.io/instance: iotedge-gw app.kubernetes.io/managed-by: Helm	10.107.236.20	iotedge.iotedge:35000 TCP iotedge.iotedge:0 TCP iotedge.iotedge:35001 TCP iotedge.iotedge:0 TCP		2 days ago
webserverapp	net.azure-devices.edge.deviceId: myasequires1-edge net.azure-devices.edge.module: webserverapp	10.105.186.35	webserviceapp.iotedge:8080 TCP webserviceapp.iotedge:30976 TCP	10.128.44.244:8080 10.128.44.244:30976	a minute ago

- Select the external endpoint to open a new browser window.

You should see that the webserver app is running.

The browser screenshot shows the following content:

- Address bar: Not secure | 10.128.44.244:8080
- Page title: Welcome to nginx!
- Page content: If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
- Page content: For online documentation and support please refer to nginx.org. Commercial support is available at nginx.com.
- Page content: Thank you for using nginx.

Next steps

- Learn how to Expose stateful application via an IoT Edge module.

Deploy an IoT Edge workload using GPU sharing on your Azure Stack Edge Pro

9/21/2022 • 12 minutes to read • [Edit Online](#)

This article describes how containerized workloads can share the GPUs on your Azure Stack Edge Pro GPU device. The approach involves enabling the Multi-Process Service (MPS) and then specifying the GPU workloads via an IoT Edge deployment.

Prerequisites

Before you begin, make sure that:

1. You've access to an Azure Stack Edge Pro GPU device that is [activated](#) and has [compute configured](#). You have the [Kubernetes API endpoint](#) and you have added this endpoint to the `hosts` file on your client that will be accessing the device.
2. You've access to a client system with a [Supported operating system](#). If using a Windows client, the system should run PowerShell 5.0 or later to access the device.
3. Save the following deployment `json` on your local system. You'll use information from this file to run the IoT Edge deployment. This deployment is based on [Simple CUDA containers](#) that are publicly available from Nvidia.

```
{  
    "modulesContent": {  
        "$edgeAgent": {  
            "properties.desired": {  
                "modules": {  
                    "cuda-sample1": {  
                        "settings": {  
                            "image": "nvidia/samples:nbody",  
                            "createOptions": "{\"Entrypoint\": [\"/bin/sh\"], \"Cmd\": [\"-c\", \"/tmp/nbody -benchmark -i=1000; while true; do echo no-op; sleep 10000;done\"], \"HostConfig\": {\"IpcMode\": \"host\", \"PidMode\": \"host\"}}"  
                        },  
                        "type": "docker",  
                        "version": "1.0",  
                        "env": {  
                            "NVIDIA_VISIBLE_DEVICES": {  
                                "value": "0"  
                            }  
                        },  
                        "status": "running",  
                        "restartPolicy": "never"  
                    },  
                    "cuda-sample2": {  
                        "settings": {  
                            "image": "nvidia/samples:nbody",  
                            "createOptions": "{\"Entrypoint\": [\"/bin/sh\"], \"Cmd\": [\"-c\", \"/tmp/nbody -benchmark -i=1000; while true; do echo no-op; sleep 10000;done\"], \"HostConfig\": {\"IpcMode\": \"host\", \"PidMode\": \"host\"}}"  
                        },  
                        "type": "docker",  
                        "version": "1.0",  
                        "env": {  
                            "NVIDIA_VISIBLE_DEVICES": {  
                                "value": "0"  
                            }  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```

```

        }
    },
    "status": "running",
    "restartPolicy": "never"
}
},
"runtime": {
    "settings": {
        "minDockerVersion": "v1.25"
    },
    "type": "docker"
},
"schemaVersion": "1.1",
"systemModules": {
    "edgeAgent": {
        "settings": {
            "image": "mcr.microsoft.com/azureiotedge-agent:1.0",
            "createOptions": ""
        },
        "type": "docker"
    },
    "edgeHub": {
        "settings": {
            "image": "mcr.microsoft.com/azureiotedge-hub:1.0",
            "createOptions": "{\"HostConfig\":{\"PortBindings\":{\"443/tcp\":[{\"HostPort\":\"4431\"}],\"5671/tcp\":[{\"HostPort\":\"5671\"}],\"8883/tcp\":[{\"HostPort\":\"8883\"}]}\"}"
        },
        "type": "docker",
        "status": "running",
        "restartPolicy": "always"
    }
}
},
"$edgeHub": {
    "properties.desired": {
        "routes": {
            "route": "FROM /messages/* INTO $upstream"
        },
        "schemaVersion": "1.1",
        "storeAndForwardConfiguration": {
            "timeToLiveSecs": 7200
        }
    }
},
"cuda-sample1": {
    "properties.desired": {}
},
"cuda-sample2": {
    "properties.desired": {}
}
}
}
}

```

Verify GPU driver, CUDA version

The first step is to verify that your device is running required GPU driver and CUDA versions.

1. [Connect to the PowerShell interface of your device.](#)

2. Run the following command:

```
Get-HcsGpuNvidiaSmi
```

3. In the Nvidia smi output, make a note of the GPU version and the CUDA version on your device. If you are

running Azure Stack Edge 2102 software, this version would correspond to the following driver versions:

- GPU driver version: 460.32.03
- CUDA version: 11.2

Here is an example output:

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Tue Feb 23 10:34:01 2021
+-----+
| NVIDIA-SMI 460.32.03     Driver Version: 460.32.03     CUDA Version: 11.2 |
|-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id     Disp.A | Volatile Uncorr. ECC | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap|          Memory-Usage | GPU-Util  Compute M. |
| |           |                |              |          | MIG M. |
|-----+-----+-----+-----+
|  0  Tesla T4          On   | 0000041F:00:00.0 Off |          0 | | | |
| N/A  40C    P8    15W /  70W |        0MiB / 15109MiB |       0%     Default |
| |           |                |              |          | N/A |
+-----+-----+-----+
+-----+
| Processes:
| GPU  GI  CI          PID  Type  Process name          GPU Memory |
|       ID  ID
|-----+-----+-----+-----+
| No running processes found
+-----+
[10.100.10.10]: PS>
```

4. Keep this session open as you will use it to view the Nvidia smi output throughout the article.

Deploy without context-sharing

You can now deploy an application on your device when the Multi-Process Service is not running and there is no context-sharing. The deployment is via the Azure portal in the `iotedge` namespace that exists on your device.

Create user in IoT Edge namespace

First you'll create a user that will connect to the `iotedge` namespace. The IoT Edge modules are deployed in the `iotedge` namespace. For more information, see [Kubernetes namespaces on your device](#).

Follow these steps to create a user and grant user the access to the `iotedge` namespace.

1. [Connect to the PowerShell interface of your device](#).
2. Create a new user in the `iotedge` namespace. Run the following command:

```
New-HcsKubernetesUser -UserName <user name>
```

Here is an example output:

```
[10.100.10.10]: PS>New-HcsKubernetesUser -UserName iotedgeuser
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
=====
server: https://compute.myasegpudev.wdshcsso.com:6443
  name: kubernetes
contexts:
- context:
  cluster: kubernetes
  user: iotedgeuser
  name: iotedgeuser@kubernetes
current-context: iotedgeuser@kubernetes
kind: Config
preferences: {}
users:
- name: iotedgeuser
  user:
    client-certificate-data:
=====
  client-key-data:
=====
=====
PQotLS0tLUVORCBSU0EgUFJJVkJURSLRVktLS0tLQo=
```

3. Copy the output displayed in plain text. Save the output as a *config* file (with no extension) in the `.kube` folder of your user profile on your local machine, for example, `C:\Users\<username>\.kube`.
4. Grant the user that you created, access to the `iotedge` namespace. Run the following command:

```
Grant-HcsKubernetesNamespaceAccess -Namespace iotedge -UserName <user name>
```

Here is an example output:

```
[10.100.10.10]: PS>Grant-HcsKubernetesNamespaceAccess -Namespace iotedge -UserName iotedgeuser
[10.100.10.10]: PS>
```

For detailed instructions, see [Connect to and manage a Kubernetes cluster via kubectl on your Azure Stack Edge Pro GPU device](#).

Deploy modules via portal

Deploy IoT Edge modules via the Azure portal. You'll deploy publicly available Nvidia CUDA sample modules that run n-body simulation. For more information, see [N-body simulation](#).

1. Make sure that the IoT Edge service is running on your device.

The screenshot shows the Azure Stack Edge device overview page for 'myasegpudev1'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Properties, Order details, Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring. The main content area displays the status of the device: 'Your device is running fine!' and lists 'Deployed edge services' with 'IoT Edge' shown as 'Running'. Below this, there's a section for 'Edge services' with tiles for Virtual machines, IoT Edge, and Cloud storage gateway, each with a 'How to get started?' link.

2. Select the IoT Edge tile in the right-pane. Go to **IoT Edge > Properties**. In the right-pane, select the IoT Hub resource associated with your device.

The screenshot shows the 'IoT Edge | Properties' page for 'myasegpudev1-edge'. The left sidebar includes Overview, Modules, Triggers, and Properties. The main pane displays device properties: IoT Hub (ase-myasegpudev1-iothub), IoT Edge device (myasegpudev1-edge), IoT device for storage gateway (myasegpudev1-storagegateway), and Platform (Linux). The 'Properties' link in the sidebar is highlighted with a red box.

3. In the IoT Hub resource, go to **Automatic Device Management > IoT Edge**. In the right-pane, select the IoT Edge device associated with your device.

The screenshot shows the 'ase-myasegpudev1-iothub | IoT Edge' page under Automatic Device Management. The left sidebar has sections for Built-in endpoints, Failover, Properties, Locks, Query explorer, IoT devices, and IoT Edge (which is selected and highlighted with a red box). The main pane shows 'IoT Edge devices' and a query interface. A table at the bottom lists devices with columns: Device ID, Runtime Response, IoT Edge Module Count, Connected Client Count, and Deployment Count. The row for 'myasegpudev1-edge' is highlighted with a red box.

4. Select **Set modules**.

Home > ase-myasegpudev1-iothub >
myasegpudev1-edge ⌂ ...

Save Set modules Manage child devices Device twin Manage keys Refresh

Device ID: myasegpudev1-edge
Primary Key:
Secondary Key:
Primary Connection String:
Secondary Connection String:
IoT Edge Runtime Response: 417 -- The device's deployment configuration is not set
Enable connection to IoT Hub: Enable Disable
Parent device: No parent device

Modules IoT Edge hub connections Deployments and Configurations

Name	Type	Specified in Deployment	Reported by Device	Runtime Status	Exit C...
\$EdgeAgent	IoT Edge System Module	<input type="radio"/> No	✓ Yes	running	0
\$edgeHub	Module Identity	NA	NA	NA	NA

5. Select + Add > + IoT Edge module.

Home > ase-myasegpudev1-iothub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge ⌂ ...

ase-myasegpudev1-iothub

Modules Routes Review + create

Container Registry Credentials

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
Name	Address	User name	Password

IoT Edge Modules

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub. [Learn more](#)

+ Add ⌂ Runtime Settings

- + IoT Edge Module
- + Marketplace Module
- + Azure Stream Analytics Module

Send usage data to Microsoft to help improve our products and services. Read our [privacy statement](#) to learn more. See [details](#) of what data is collected.

Review + create < Previous Next: Routes >

6. On the **Module Settings** tab, provide the **IoT Edge module name** and **Image URI**. Set **Image pull policy** to **On create**.

Home > ase-myasgpudev1-iohub > myasgpudev1-edge >

Set modules on device: myasgpudev1-edge

ase-myasgpudev1-iohub

Add IoT Edge Module

Specify the settings for an IoT Edge custom module.

[Learn more](#)

IoT Edge Module Name *

cuda-sample1

Module Settings Environment Variables Container Create Options Module Twin Settings

Image URI *

nvidia/samples:nbody

Restart Policy

always

Desired Status

running

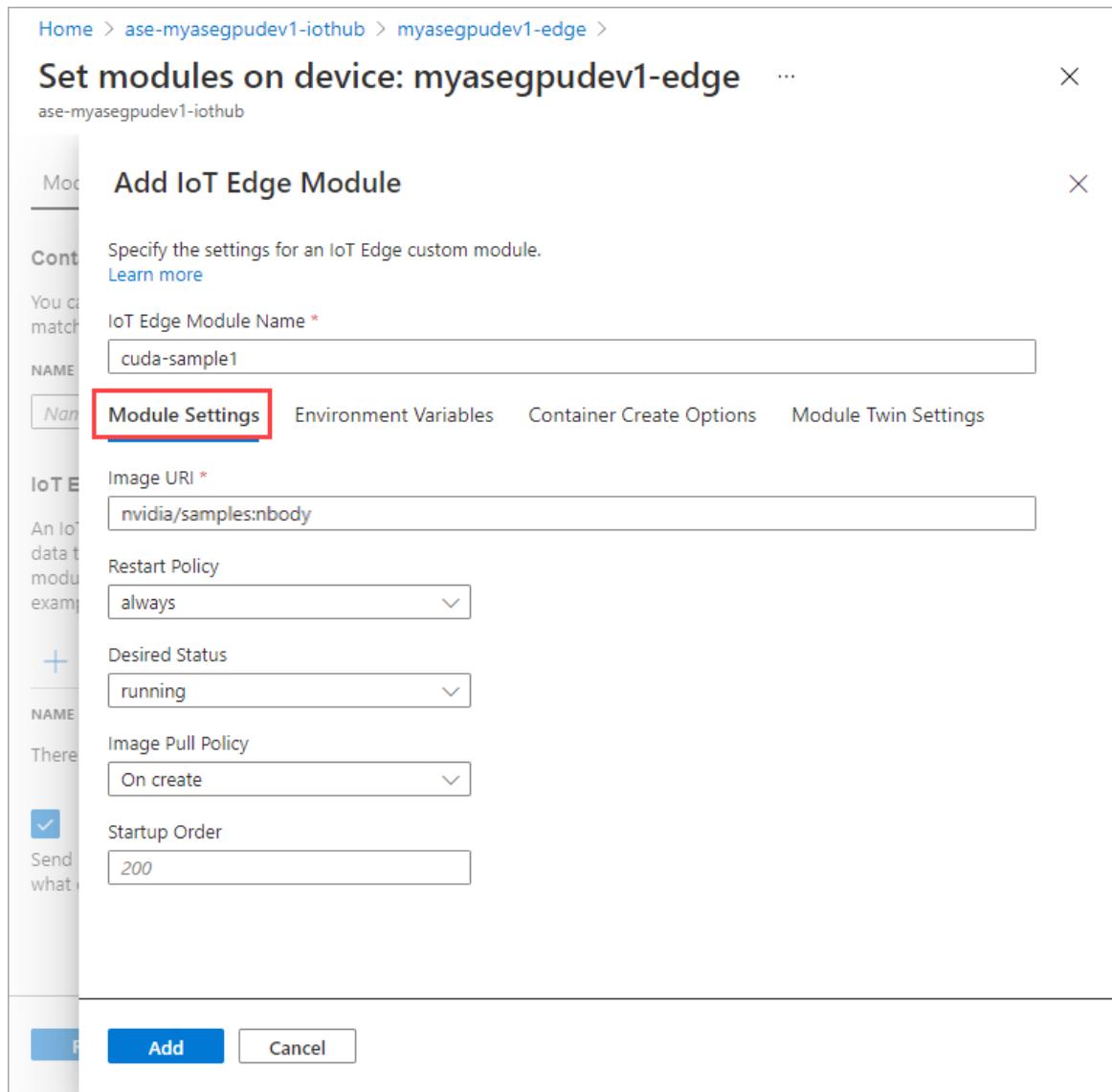
Image Pull Policy

On create

Startup Order

200

Add Cancel



7. On the **Environment Variables** tab, specify **NVIDIA_VISIBLE_DEVICES** as 0.

Home > ase-myasgpudev1-iohub > myasgpudev1-edge >

Set modules on device: myasgpudev1-edge

ase-myasgpudev1-iohub

Add IoT Edge Module

Specify the settings for an IoT Edge custom module.

[Learn more](#)

IoT Edge Module Name *

cuda-sample1

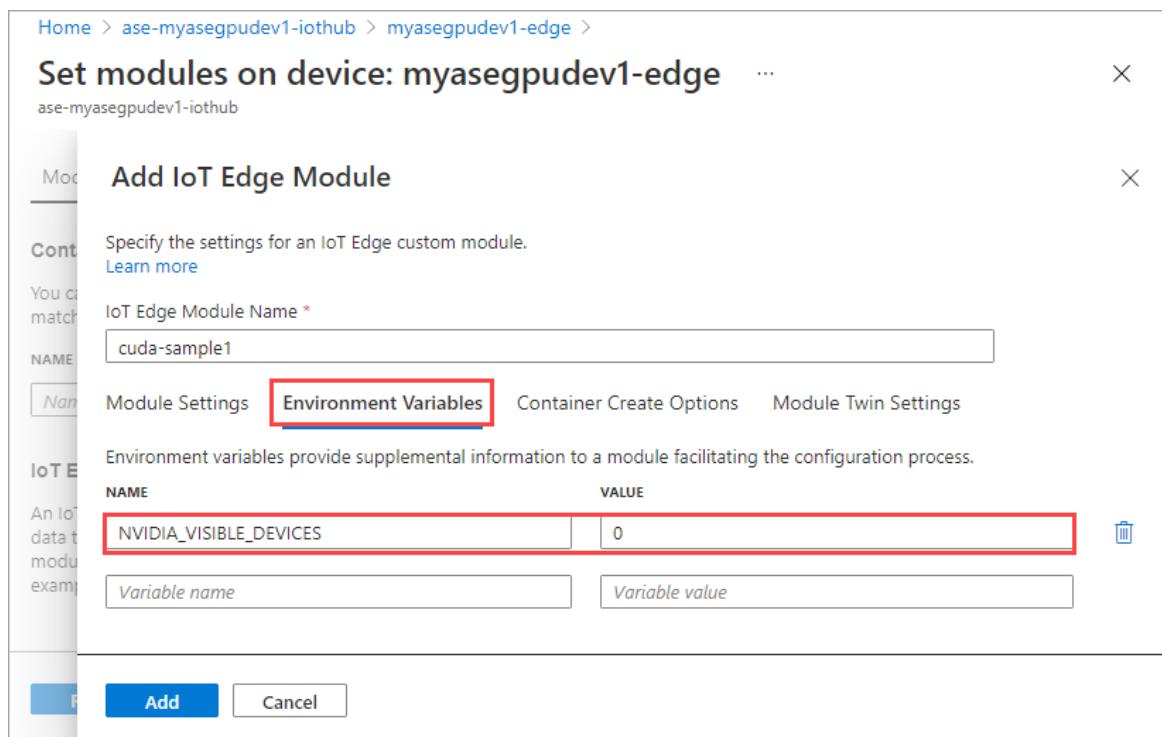
Module Settings Environment Variables Container Create Options Module Twin Settings

Environment variables provide supplemental information to a module facilitating the configuration process.

NAME	VALUE
NVIDIA_VISIBLE_DEVICES	0

Variable name Variable value

Add Cancel



8. On the **Container Create Options** tab, provide the following options:

```
{
    "Entrypoint": [
        "/bin/sh"
    ],
    "Cmd": [
        "-c",
        "/tmp/nbody -benchmark -i=1000; while true; do echo no-op; sleep 10000;done"
    ],
    "HostConfig": {
        "IpcMode": "host",
        "PidMode": "host"
    }
}
```

The options are displayed as follows:

The screenshot shows the 'Update IoT Edge Module' dialog for a module named 'cuda-sample1'. The 'Container Create Options' tab is selected, highlighting the JSON configuration code. The code defines the Docker container setup, including the entrypoint, command, and host configuration.

```

1  {
2      "Entrypoint": [
3          "/bin/sh"
4      ],
5      "Cmd": [
6          "-c",
7          "/tmp/nbody -benchmark -i=1000; while true; do echo no-op; sleep 10000;done"
8      ],
9      "HostConfig": {
10         "IpcMode": "host",
11         "PidMode": "host"
12     }
13 }

```

Module Settings **Environment Variables** **Container Create Options** (highlighted) **Module Twin Settings**

Create options direct the creation of the IoT Edge module Docker container.
[View all options](#)

NAME: cuda-sample1

Update Cancel

Select Add.

9. The module that you added should show as **Running**.

Set modules on device: myasegpudev1-edge

X

ase-myasegpudev1-iohub

[Modules](#) [Routes](#) [Review + create](#)

Container Registry Credentials

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
<input type="text" value="Name"/>	<input type="text" value="Address"/>	<input type="text" value="User name"/>	<input type="text" value="Password"/>

IoT Edge Modules

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub. [Learn more](#)

 [Add](#) [Runtime Settings](#)

NAME	DESIRED STATUS	
cuda-sample1	running	



Send usage data to Microsoft to help improve our products and services. Read our [privacy statement](#) to learn more. See [details](#) of what data is collected.

[Review + create](#)[< Previous](#)[Next: Routes >](#)

10. Repeat all the steps to add a module that you followed when adding the first module. In this example, provide the name of the module as .

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge

ase-myasegpudev1-iohub

Add IoT Edge Module

Specify the settings for an IoT Edge custom module.

Learn more

IoT Edge Module Name *

cuda-sample2

Module Settings Environment Variables Container Create Options Module Twin Settings

Image URI *

nvidia/samples:nbody

Restart Policy

always

Desired Status

running

Image Pull Policy

On create

Startup Order

200

Send more.

Add Cancel

The screenshot shows the 'Add IoT Edge Module' dialog. The 'Module Settings' tab is active. The 'IoT Edge Module Name' field is filled with 'cuda-sample2'. Other settings like Image URI, Restart Policy, and Startup Order are also visible. At the bottom are 'Add' and 'Cancel' buttons.

Use the same environment variable as both the modules will share the same GPU.

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge

ase-myasegpudev1-iohub

Add IoT Edge Module

Specify the settings for an IoT Edge custom module.

Learn more

IoT Edge Module Name *

cuda-sample2

Module Settings Environment Variables Container Create Options Module Twin Settings

Environment variables provide supplemental information to a module facilitating the configuration process.

NAME	VALUE
NVIDIA_VISIBLE_DEVICES	0

Variable name Variable value

Add Cancel

The screenshot shows the 'Add IoT Edge Module' dialog with the 'Environment Variables' tab selected. It lists an environment variable 'NVIDIA_VISIBLE_DEVICES' with value '0'. There are 'Variable name' and 'Variable value' input fields below the table. Buttons at the bottom are 'Add' and 'Cancel'.

Use the same container create options that you provided for the first module and select **Add**.

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge

ase-myasegpudev1-iohub

Add IoT Edge Module

Specify the settings for an IoT Edge custom module. [Learn more](#)

IoT Edge Module Name *

Module Settings Environment Variables **Container Create Options** Module Twin Settings

Create options direct the creation of the IoT Edge module Docker container. [View all options](#)

```

1  {
2      "HostConfig": {
3          "IpcMode": "host",
4          "PidMode": "host"
5      }
6  }

```

Add **Cancel**

11. On the Set modules page, select **Review + Create** and then select **Create**.

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge

ase-myasegpudev1-iohub

Modules **Routes** **Review + create**

Validation passed.

Deployment

The text box below displays the deployment to be submitted.

```

1  {
2      "modulesContent": {
3          "$edgeAgent": {
4              "properties.desired": {
5                  "modules": {
6                      "cuda-sample1": {
7                          "settings": {
8                              "image": "nvcr.io/nvidia/k8s/cuda-sample:nbody",
9                              "createOptions": "{\"HostConfig\":{\"IpcMode\":\"host\",\"PidMode\":\"host\"}}"
10                         },
11                         "type": "docker",
12                         "version": "1.0",
13                         "env": {
14                             "NVIDIA_VISIBLE_DEVICES": {
15                                 "value": "0"
16                             }
17                         },
18                         "imagePullPolicy": "on-create",
19                         "status": "running",
20                         "restartPolicy": "always"
21                     },
22                     "cuda-sample2": {
23                         "settings": {
24                             "image": "nvcr.io/nvidia/k8s/cuda-sample:nbody",
25                             "createOptions": "{\"HostConfig\":{\"IpcMode\":\"host\",\"PidMode\":\"host\"}}"
26                         },
27                     }
28                 }
29             }
30         }
31     }

```

Create **< Previous** **Next >**

12. The **Runtime status** of both the modules should now show as **Running**.

Name	Type	Specified in Deployment	Reported by Device	Runtime	Exit C...
\$EdgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$EdgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
cuda-sample1	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
cuda-sample2	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

Monitor workload deployment

1. Open a new PowerShell session.
2. List the pods running in the `iotedge` namespace. Run the following command:

```
kubectl get pods -n iotedge
```

Here is an example output:

```
PS C:\WINDOWS\system32> kubectl get pods -n iotedge --kubeconfig C:\GPU-sharing\kubeconfigs\configiotuser1
NAME          READY   STATUS    RESTARTS   AGE
cuda-sample1-869989578c-ssng8  2/2     Running   0          5s
cuda-sample2-6db6d98689-d74kb  2/2     Running   0          4s
edgeagent-79f988968b-7p2tv    2/2     Running   0          6d21h
edgehub-d6c764847-18v4m       2/2     Running   0          24h
iotedged-55fdb7b5c6-19zn8    1/1     Running   1          6d21h
PS C:\WINDOWS\system32>
```

There are two pods, `cuda-sample1-97c494d7f-1nmns` and `cuda-sample2-d9f6c4688-2rlld9` running on your device.

3. While both the containers are running the n-body simulation, view the GPU utilization from the Nvidia smi output. Go to the PowerShell interface of the device and run `Get-HcsGpuNvidiaSmi`.

Here is an example output when both the containers are running the n-body simulation:

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Fri Mar 5 13:31:16 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2 |
|-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A | Volatile Uncorr. ECC | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
| |          |          |             |            |          MIG M. |
|-----+-----+-----+-----+
| 0  Tesla T4           On     | 00002C74:00:00.0 Off   |                0 | | | |
| N/A  52C   P0    69W / 70W | 221MiB / 15109MiB | 100%       Default |
| |          |          |             |            |          N/A |
+-----+-----+-----+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory |
| ID   ID
|-----+-----+-----+-----+-----+-----+
| 0  N/A N/A 188342 C    /tmp/nbody               109MiB |
| 0  N/A N/A 188413 C    /tmp/nbody               109MiB |
+-----+
[10.100.10.10]: PS>
```

As you can see, there are two containers running with n-body simulation on GPU 0. You can also view their corresponding memory usage.

- Once the simulation has completed, the Nvidia smi output will show that there are no processes running on the device.

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Fri Mar 5 13:54:48 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2 |
|-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A | Volatile Uncorr. ECC | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
| |          |          |             |            |          MIG M. |
|-----+-----+-----+-----+
| 0  Tesla T4           On     | 00002C74:00:00.0 Off   |                0 | | | |
| N/A  34C   P8    9W / 70W | 0MiB / 15109MiB | 0%       Default |
| |          |          |             |            |          N/A |
+-----+-----+-----+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory |
| ID   ID
|-----+-----+-----+-----+-----+-----+
| No running processes found
+-----+
[10.100.10.10]: PS>
```

- After the n-body simulation has completed, view the logs to understand the details of the deployment and the time required for the simulation to complete.

Here is an example output from the first container:

```
PS C:\WINDOWS\system32> kubectl -n iotedge --kubeconfig C:\GPU-sharing\kubeconfigs\configiotuser1 logs cuda-sample1-869989578c-ssng8 cuda-sample1
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// snipped //=====// snipped //=====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 170171.531 ms
= 98.590 billion interactions per second
= 1971.801 single-precision GFLOP/s at 20 flops per interaction
no-op
PS C:\WINDOWS\system32>
```

Here is an example output from the second container:

```
PS C:\WINDOWS\system32> kubectl -n iotedge --kubeconfig C:\GPU-sharing\kubeconfigs\configiotuser1 logs cuda-sample2-6db6d98689-d74kb cuda-sample2
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// snipped //=====// snipped //=====
> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 170054.969 ms
= 98.658 billion interactions per second
= 1973.152 single-precision GFLOP/s at 20 flops per interaction
no-op
PS C:\WINDOWS\system32>
```

6. Stop the module deployment. In the IoT Hub resource for your device:

- Go to **Automatic Device Deployment > IoT Edge**. Select the IoT Edge device corresponding to your device.
- Go to **Set modules** and select a module.

Home > ase-myasegpudev1-iohub >
myasegpudev1-edge ✎ ...
 ase-myasegpudev1-iohub

Device ID	myasegpudev1-edge	<input type="button" value=""/>	<input type="button" value=""/>
Primary Key	<input type="button" value=""/>	<input type="button" value=""/>
Secondary Key	<input type="button" value=""/>	<input type="button" value=""/>
Primary Connection String	<input type="button" value=""/>	<input type="button" value=""/>
Secondary Connection String	<input type="button" value=""/>	<input type="button" value=""/>
IoT Edge Runtime Response	200 -- OK	<input type="button" value=""/>	<input type="button" value=""/>
Enable connection to IoT Hub	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Parent device	No parent device	<input type="button" value=""/>	<input type="button" value=""/>

Modules IoT Edge hub connections Deployments and Configurations

Name	Type	Specified in Deployment	Reported by ...	Runni...	Exit C...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
cuda-sample1	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
cuda-sample2	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

c. On the **Modules** tab, select a module.

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >
Set modules on device: myasegpudev1-edge ✎ ...
 ase-myasegpudev1-iohub

Container Registry Credentials

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
<input type="text" value="Name"/>	<input type="text" value="Address"/>	<input type="text" value="User name"/>	<input type="text" value="Password"/>

IoT Edge Modules

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub. [Learn more](#)

NAME	DESIRED STATUS	<input type="button" value=""/>
<input type="text" value="cuda-sample1"/>	running	<input type="button" value=""/>
<input type="text" value="cuda-sample2"/>	running	<input type="button" value=""/>

Send usage data to Microsoft to help improve our products and services. Read our [privacy statement](#) to learn more. See [details](#) of what data is collected.

d. On the **Module settings** tab, set **Desired status** to stopped. Select **Update**.

Home > ase-myasegpudev1-iohub > myasegpudev1-edge >

Set modules on device: myasegpudev1-edge

ase-myasegpudev1-iohub

Update IoT Edge Module

Specify the settings for an IoT Edge custom module.

[Learn more](#)

IoT Edge Module Name *

Module Settings Environment Variables Container Create Options Module Twin Settings

Image URI *

Restart Policy

Desired Status

Image Pull Policy

Startup Order

Send more...

- e. Repeat the steps to stop the second module deployed on the device. Select **Review + create** and then select **Create**. This should update the deployment.

Set modules on device: myasegpudev1-edge

X

ase-myasegpudev1-iohub

[Modules](#) [Routes](#) [Review + create](#)

Container Registry Credentials

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
<input type="text" value="Name"/>	<input type="text" value="Address"/>	<input type="text" value="User name"/>	<input type="password" value="Password"/>

IoT Edge Modules

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub. [Learn more](#)

[+](#) Add ▾ [Runtime Settings](#)

NAME	DESIRED STATUS	
cuda-sample1	stopped	
cuda-sample2	stopped	



Send usage data to Microsoft to help improve our products and services. Read our [privacy statement](#) to learn more. See [details](#) of what data is collected.

[Review + create](#)[< Previous](#)[Next: Routes >](#)

- f. Refresh Set modules page multiple times. until the module Runtime status shows as Stopped.

Device ID: myasegpudev1-edge

Primary Key: (redacted)

Secondary Key: (redacted)

Primary Connection String: (redacted)

Secondary Connection String: (redacted)

IoT Edge Runtime Response: 200 -- OK

Enable connection to IoT Hub: Enable Disable

Parent device: No parent device

Modules

Name	Type	Specified in Deployment	Reported by ...	Runni...	Exit C...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
cuda-sample1	IoT Edge Custom Module	✓ Yes	⊖ No	--	--
cuda-sample2	IoT Edge Custom Module	✓ Yes	⊖ No	--	--

Deploy with context-sharing

You can now deploy the n-body simulation on two CUDA containers when MPS is running on your device. First, you'll enable MPS on the device.

1. Connect to the PowerShell interface of your device.
2. To enable MPS on your device, run the `Start-HcsGpuMPS` command.

```
[10.100.10.10]: PS>Start-HcsGpuMPS
K8S-1HXQG13CL-1HXQG13:
Set compute mode to EXCLUSIVE_PROCESS for GPU 0000191E:00:00.0.
All done.
Created nvidia-mps.service
[10.100.10.10]: PS>
```

3. Get the Nvidia smi output from the PowerShell interface of the device. You can see the `nvidia-cuda-mps-server` process or the MPS service is running on the device.

Here is an example output:

```
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Thu Mar  4 12:37:39 2021
+-----+
| NVIDIA-SMI 460.32.03    Driver Version: 460.32.03    CUDA Version: 11.2    |
+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A  | Volatile Uncorr. ECC  | | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M.  |
| |          |          |             |          |          |          MIG M. |
+-----+
|  0  Tesla T4           On     | 00002C74:00:00.0 Off    |          0 | | | | |
| N/A   36C   P8    9W / 70W |    28MiB / 15109MiB |     0%  E. Process |
| |          |          |             |          |          |          N/A |
+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory  |
| ID   ID
+-----+
|  0  N/A N/A  122792      C  nvidia-cuda-mps-server  25MiB  |
+-----+
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
```

4. Deploy the modules that you stopped earlier. Set the **Desired status** to running via **Set modules**.

Here is the example output:

```
PS C:\WINDOWS\system32> kubectl get pods -n iotedge --kubeconfig C:\GPU-
sharing\kubeconfigs\configiotuser1
NAME          READY   STATUS    RESTARTS   AGE
cuda-sample1-869989578c-2zxh6   2/2     Running   0          44s
cuda-sample2-6db6d98689-fn7mx   2/2     Running   0          44s
edgeagent-79f988968b-7p2tv     2/2     Running   0          5d20h
edgehub-d6c764847-18v4m        2/2     Running   0          27m
iotedged-55fdb7b5c6-19zn8     1/1     Running   1          5d20h
PS C:\WINDOWS\system32>
```

You can see that the modules are deployed and running on your device.

5. When the modules are deployed, the n-body simulation also starts running on both the containers. Here is the example output when the simulation has completed on the first container:

```
PS C:\WINDOWS\system32> kubectl -n iotedge logs cuda-sample1-869989578c-2zxh6 cuda-sample1
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// snipped //=====// snipped //=====

> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 155256.062 ms
= 108.062 billion interactions per second
= 2161.232 single-precision GFLOP/s at 20 flops per interaction
no-op
PS C:\WINDOWS\system32>
```

Here is the example output when the simulation has completed on the second container:

```

PS C:\WINDOWS\system32> kubectl -n iotedge --kubeconfig C:\GPU-sharing\kubeconfigs\configiotuser1
logs cuda-sample2-6db6d98689-fn7mx cuda-sample2
Run "nbody -benchmark [-numbodies=<numBodies>]" to measure performance.
=====// snipped //=====// snipped //=====

> Windowed mode
> Simulation data stored in video memory
> Single precision floating point simulation
> 1 Devices used for simulation
GPU Device 0: "Turing" with compute capability 7.5

> Compute 7.5 CUDA device: [Tesla T4]
40960 bodies, total time for 10000 iterations: 155366.359 ms
= 107.985 billion interactions per second
= 2159.697 single-precision GFLOP/s at 20 flops per interaction
no-op
PS C:\WINDOWS\system32>

```

- Get the Nvidia smi output from the PowerShell interface of the device when both the containers are running the n-body simulation. Here is an example output. There are three processes, the `nvidia-cuda-mps-server` process (type C) corresponds to the MPS service and the `/tmp/nbody` processes (type M + C) correspond to the n-body workloads deployed by the modules.

```

[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi
K8S-1HXQG13CL-1HXQG13:

Thu Mar  4 12:59:44 2021
+-----+
| NVIDIA-SMI 460.32.03     Driver Version: 460.32.03    CUDA Version: 11.2 |
+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A  | Volatile Uncorr. ECC | | | | |
| Fan  Temp  Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
| |          |          |             |           |          |          MIG M. |
+-----+
|  0  Tesla T4          On   | 00002C74:00:00.0 Off  |            0 | | | |
| N/A   54C   P0    69W /  70W |    242MiB / 15109MiB |    100%   E. Process |
| |          |          |             |           |          N/A |
+-----+
+-----+
| Processes:
| GPU  GI  CI      PID  Type  Process name          GPU Memory |
| ID   ID
+-----+
|  0  N/A N/A    56832  M+C   /tmp/nbody          107MiB |
|  0  N/A N/A    56900  M+C   /tmp/nbody          107MiB |
|  0  N/A N/A   122792    C   nvidia-cuda-mps-server  25MiB |
+-----+
[10.100.10.10]: PS>Get-HcsGpuNvidiaSmi

```

Next steps

- Deploy a shared GPU Kubernetes workload on your Azure Stack Edge Pro.

Develop a C# IoT Edge module to move files on Azure Stack Edge Pro

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article steps you through how to create an IoT Edge module for deployment with your Azure Stack Edge Pro device. Azure Stack Edge Pro is a storage solution that allows you to process data and send it over network to Azure.

You can use Azure IoT Edge modules with your Azure Stack Edge Pro to transform the data as it moved to Azure. The module used in this article implements the logic to copy a file from a local share to a cloud share on your Azure Stack Edge Pro device.

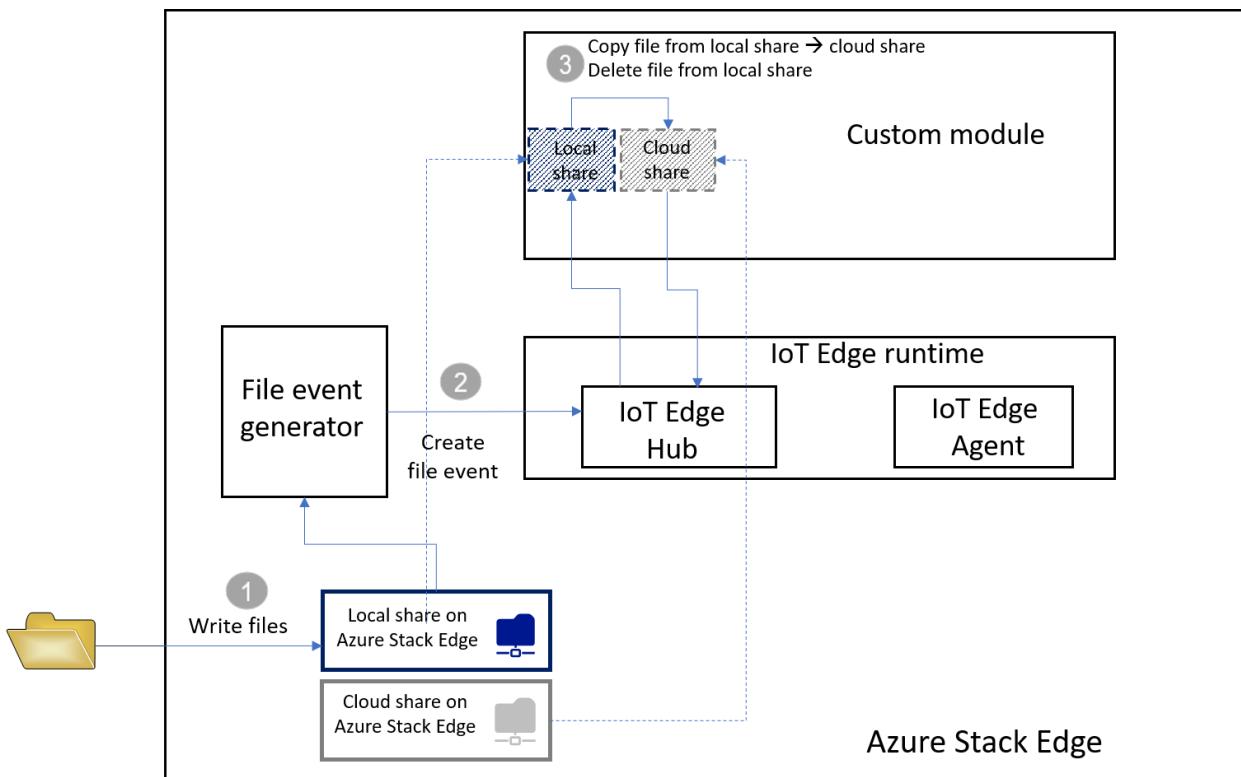
In this article, you learn how to:

- Create a container registry to store and manage your modules (Docker images).
- Create an IoT Edge module to deploy on your Azure Stack Edge Pro device.

About the IoT Edge module

Your Azure Stack Edge Pro device can deploy and run IoT Edge modules. Edge modules are essentially Docker containers that perform a specific task, such as ingest a message from a device, transform a message, or send a message to an IoT Hub. In this article, you will create a module that copies files from a local share to a cloud share on your Azure Stack Edge Pro device.

1. Files are written to the local share on your Azure Stack Edge Pro device.
2. The file event generator creates a file event for each file written to the local share. The file events are also generated when a file is modified. The file events are then sent to IoT Edge Hub (in IoT Edge runtime).
3. The IoT Edge custom module processes the file event to create a file event object that also contains a relative path for the file. The module generates an absolute path using the relative file path and copies the file from the local share to the cloud share. The module then deletes the file from the local share.



Once the file is in the cloud share, it automatically gets uploaded to your Azure Storage account.

Prerequisites

Before you begin, make sure you have:

- An Azure Stack Edge Pro device that is running.
 - The device also has an associated IoT Hub resource.
 - The device has Edge compute role configured. For more information, go to [Configure compute](#) for your Azure Stack Edge Pro.
- The following development resources:
 - [Visual Studio Code](#).
 - [C# for Visual Studio Code \(powered by OmniSharp\) extension](#).
 - [Azure IoT Edge extension for Visual Studio Code](#).
 - [.NET Core 2.1 SDK](#).
 - Docker CE. You may have to create an account to download and install the software.

Create a container registry

An Azure container registry is a private Docker registry in Azure where you can store and manage your private Docker container images. The two popular Docker registry services available in the cloud are Azure Container Registry and Docker Hub. This article uses the Container Registry.

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. Select **Create a resource > Containers > Container Registry**. Click **Create**.
3. Provide:
 - a. A unique **Registry name** within Azure that contains 5 to 50 alphanumeric characters.
 - b. Choose a **Subscription**.

- c. Create new or choose an existing **Resource group**.
- d. Select a **Location**. We recommend that this location be the same as that is associated with the Azure Stack Edge resource.
- e. Toggle **Admin user** to **Enable**.
- f. Set the **SKU** to **Basic**.

The screenshot shows the 'Create container registry' wizard step 1: Set details. The form includes the following fields:

- * Registry name: mycontreg2.azurecr.io
- * Subscription: Internal Consumption
- * Resource group: mycontregrg (with 'Create new' link)
- * Location: West US
- * Admin user: Enable (selected)
- * SKU: Basic

At the bottom, there are two buttons: a red 'Create' button and a blue 'Automation options' link.

- 4. Select **Create**.
- 5. After your container registry is created, browse to it, and select **Access keys**.

The screenshot shows the 'mycontreg2 - Access keys' page in the Azure portal. The left sidebar has a 'Search (Ctrl+ /)' bar and links for Overview, Activity log, Access control (IAM), Tags, Quick start, Events, Settings, Access keys (which is selected and highlighted with a red box), Locks, Automation script, Services, Repositories, Webhooks, and Replications. The main area shows the Registry name as 'mycontreg2', the Login server as 'mycontreg2.azurecr.io', and the Admin user status as 'Enable'. It also displays the Username 'mycontreg2' and two password entries: 'password' and 'password2', each with a copy icon.

6. Copy the values for **Login server**, **Username**, and **Password**. You use these values later to publish the Docker image to your registry and to add the registry credentials to the Azure IoT Edge runtime.

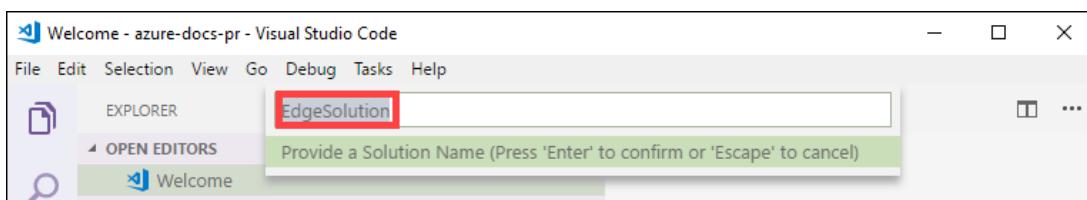
Create an IoT Edge module project

The following steps create an IoT Edge module project based on the .NET Core 2.1 SDK. The project uses Visual Studio Code and the Azure IoT Edge extension.

Create a new solution

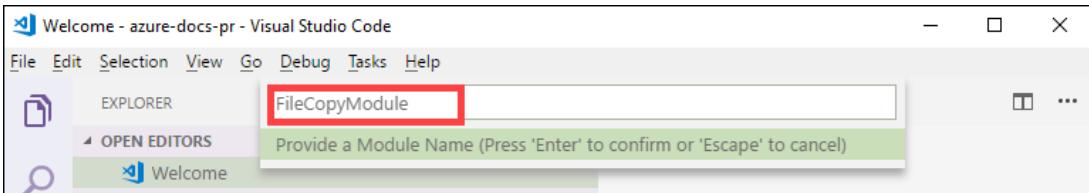
Create a C# solution template that you can customize with your own code.

1. In Visual Studio Code, select **View > Command Palette** to open the VS Code command palette.
2. In the command palette, enter and run the command **Azure: Sign in** and follow the instructions to sign in your Azure account. If you're already signed in, you can skip this step.
3. In the command palette, enter and run the command **Azure IoT Edge: New IoT Edge solution**. In the command palette, provide the following information to create your solution:
 - a. Select the folder where you want to create the solution.
 - b. Provide a name for your solution or accept the default **EdgeSolution**.



- c. Choose **C# Module** as the module template.
- d. Replace the default module name with the name you want to assign, in this case, it is

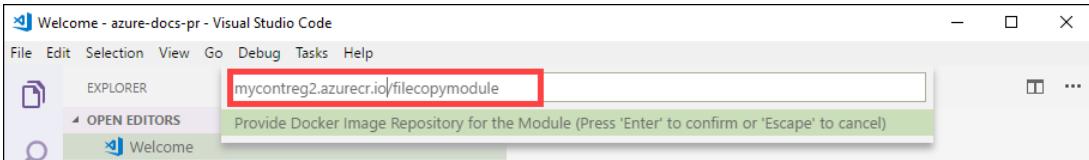
FileCopyModule.



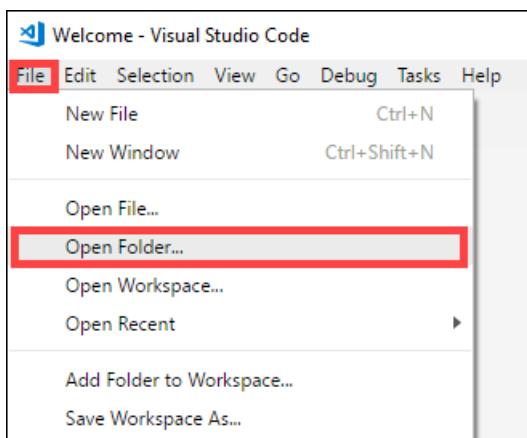
- e. Specify the container registry that you created in the previous section as the image repository for your first module. Replace **localhost:5000** with the login server value that you copied.

The final string looks like <Login server name>/<Module name>. In this example, the string is:

`mycontreg2.azurecr.io/filecopymodule`.

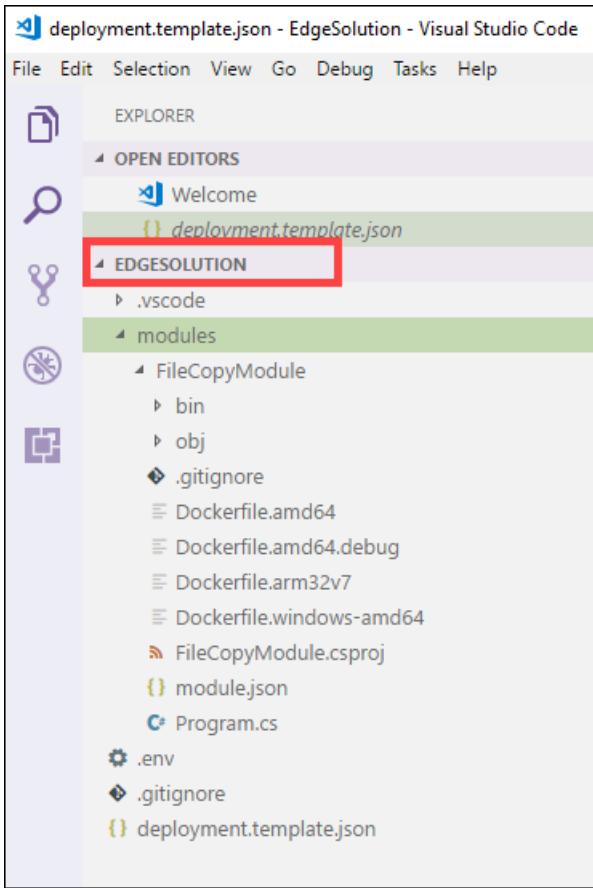


4. Go to **File > Open Folder**.



5. Browse and point to the **EdgeSolution** folder that you created earlier. The VS Code window loads your IoT Edge solution workspace with its five top-level components. You won't edit the `.vscode` folder, `.gitignore` file, `.env` file, and the `deployment.template.json**` in this article.

The only component that you modify is the modules folder. This folder has the C# code for your module and Docker files to build your module as a container image.



Update the module with custom code

1. In the VS Code explorer, open **modules > FileCopyModule > Program.cs**.
2. At the top of the **FileCopyModule namespace**, add the following using statements for types that are used later. **Microsoft.Azure.Devices.Client.Transport.Mqtt** is a protocol to send messages to IoT Edge Hub.

```
namespace FileCopyModule
{
    using Microsoft.Azure.Devices.Client.Transport.Mqtt;
    using Newtonsoft.Json;
```

3. Add the **InputFolderPath** and **OutputFolderPath** variable to the Program class.

```
class Program
{
    static int counter;
    private const string InputFolderPath = "/home/input";
    private const string OutputFolderPath = "/home/output";
```

4. Immediately after the previous step, add the **FileEvent** class to define the message body.

```

/// <summary>
/// The FileEvent class defines the body of incoming messages.
/// </summary>
private class FileEvent
{
    public string ChangeType { get; set; }

    public string ShareRelativeFilePath { get; set; }

    public string ShareName { get; set; }
}

```

5. In the **Init** method, the code creates and configures a **ModuleClient** object. This object allows the module to connect to the local Azure IoT Edge runtime using MQTT protocol to send and receive messages. The connection string that's used in the **Init** method is supplied to the module by the IoT Edge runtime. The code registers a **FileCopy** callback to receive messages from an IoT Edge hub via the **input1** endpoint. Replace the **Init** method with the following code.

```

/// <summary>
/// Initializes the ModuleClient and sets up the callback to receive
/// messages containing file event information
/// </summary>
static async Task Init()
{
    MqttTransportSettings mqttSetting = new MqttTransportSettings(TransportType.Mqtt_Tcp_Only);
    ITransportSettings[] settings = { mqttSetting };

    // Open a connection to the IoT Edge runtime
    ModuleClient ioTHubModuleClient = await ModuleClient.CreateFromEnvironmentAsync(settings);
    await ioTHubModuleClient.OpenAsync();
    Console.WriteLine("IoT Hub module client initialized.");

    // Register callback to be called when a message is received by the module
    await ioTHubModuleClient.SetInputMessageHandlerAsync("input1", FileCopy, ioTHubModuleClient);
}

```

6. Remove the code for **PipeMessage** method and in its place, insert the code for **FileCopy**.

```

/// <summary>
/// This method is called whenever the module is sent a message from the IoT Edge Hub.
/// This method deserializes the file event, extracts the corresponding relative file path, and
creates the absolute input file path using the relative file path and the InputFolderPath.
/// This method also forms the absolute output file path using the relative file path and the
OutputFolderPath. It then copies the input file to output file and deletes the input file after the
copy is complete.
/// </summary>
static async Task<MessageResponse> FileCopy(Message message, object userContext)
{
    int counterValue = Interlocked.Increment(ref counter);

    try
    {
        byte[] messageBytes = message.GetBytes();
        string messageString = Encoding.UTF8.GetString(messageBytes);
        Console.WriteLine($"Received message: {counterValue}, Body: [{messageString}]");

        if (!string.IsNullOrEmpty(messageString))
        {
            var fileEvent = JsonConvert.DeserializeObject<FileEvent>(messageString);

            string relativeFileName = fileEvent.ShareRelativeFilePath.Replace("\\", "/");
            string inputFilePath = InputFolderPath + relativeFileName;
            string outputPath = OutputFolderPath + relativeFileName;

            if (File.Exists(inputFilePath))
            {
                Console.WriteLine($"Moving input file: {inputFilePath} to output file:
{outputPath}");
                var outputDir = Path.GetDirectoryName(outputPath);
                if (!Directory.Exists(outputDir))
                {
                    Directory.CreateDirectory(outputDir);
                }

                File.Copy(inputFilePath, outputPath, true);
                Console.WriteLine($"Copied input file: {inputFilePath} to output file:
{outputPath}");
                File.Delete(inputFilePath);
                Console.WriteLine($"Deleted input file: {inputFilePath}");
            }
            else
            {
                Console.WriteLine($"Skipping this event as input file doesn't exist:
{inputFilePath}");
            }
        }
        catch (Exception ex)
        {
            Console.WriteLine("Caught exception: {0}", ex.Message);
            Console.WriteLine(ex.StackTrace);
        }

        Console.WriteLine($"Processed event.");
        return MessageResponse.Completed;
    }
}

```

7. Save this file.

8. You can also [download an existing code sample](#) for this project. You can then validate the file that you saved against the `program.cs` file in this sample.

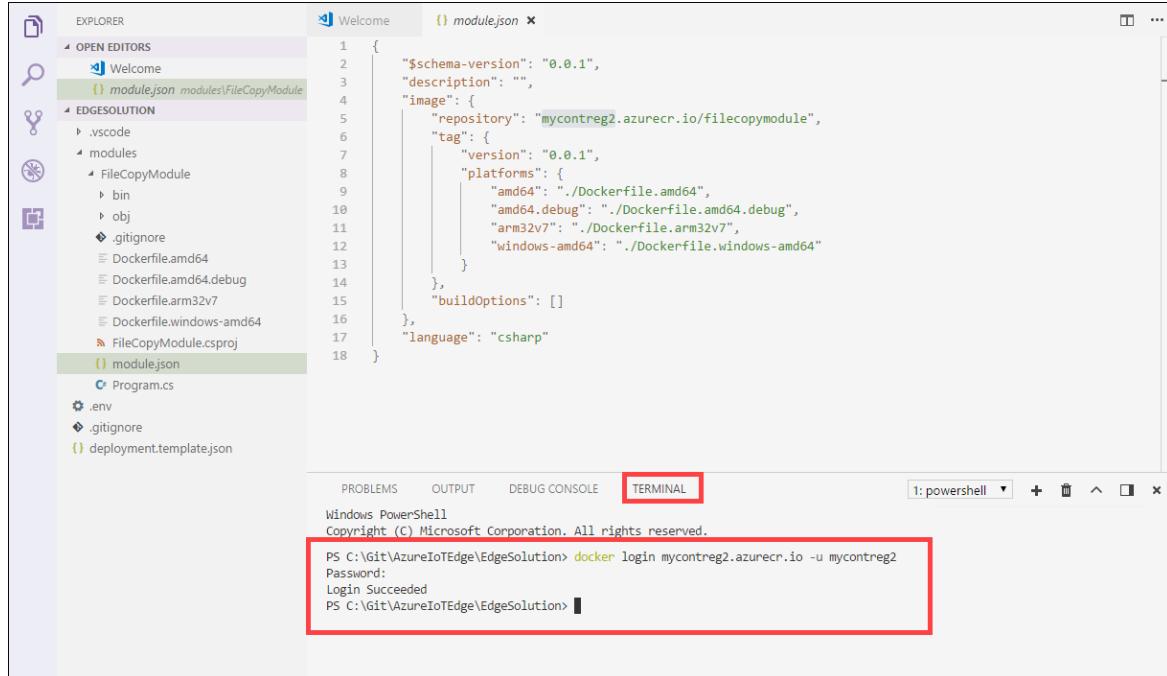
Build your IoT Edge solution

In the previous section, you created an IoT Edge solution and added code to the FileCopyModule to copy files from local share to the cloud share. Now you need to build the solution as a container image and push it to your container registry.

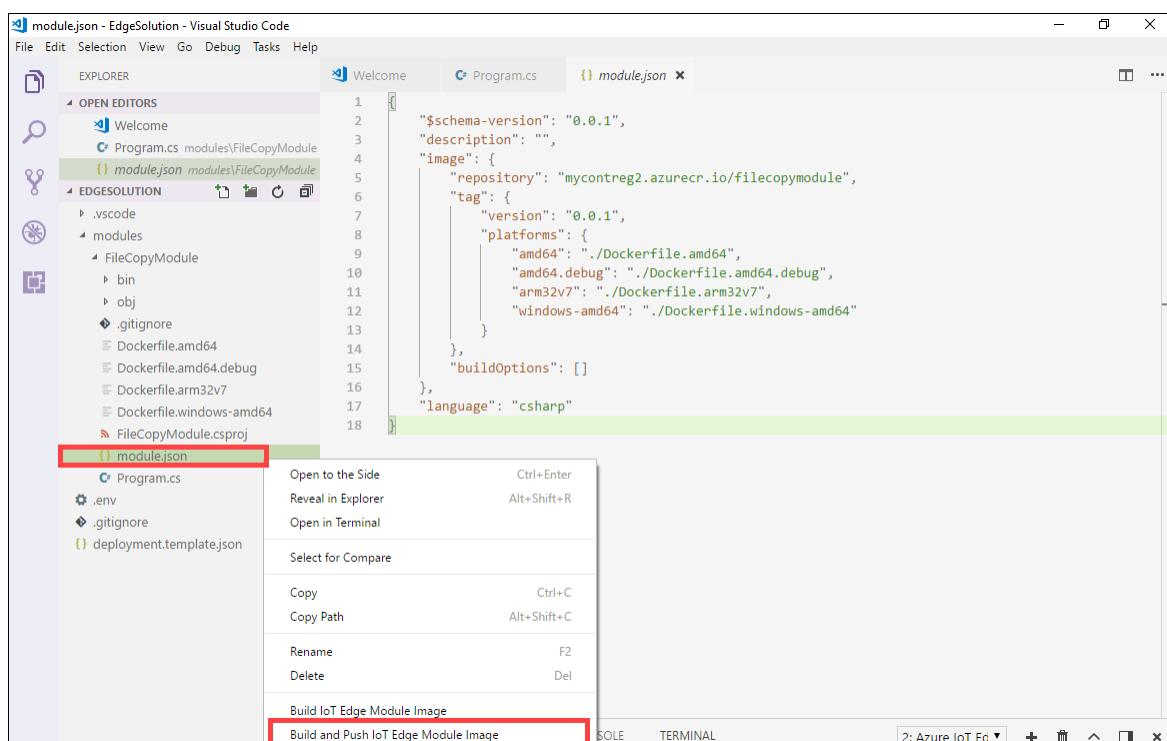
1. In VSCode, go to Terminal > New Terminal to open a new Visual Studio Code integrated terminal.
2. Sign in to Docker by entering the following command in the integrated terminal.

```
docker login <ACR login server> -u <ACR username>
```

Use the login server and username that you copied from your container registry.

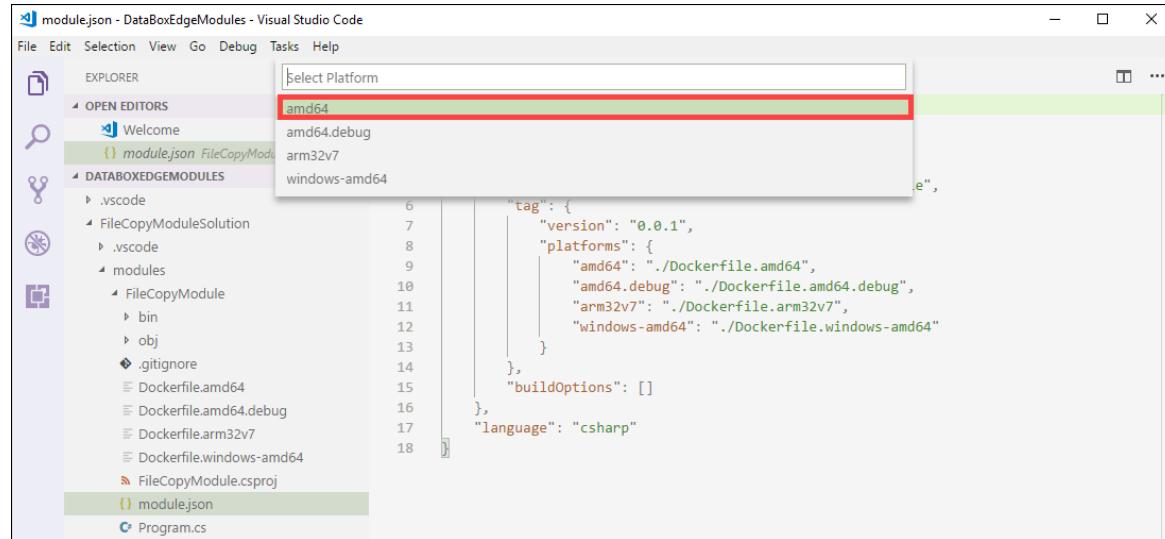


3. When prompted for password, supply the password. You can also retrieve the values for login server, username, and password from the **Access Keys** in your container registry in the Azure portal.
4. Once the credentials are supplied, you can push your module image to your Azure container registry. In the VS Code Explorer, right-click the **module.json** file and select **Build and Push IoT Edge solution**.



When you tell Visual Studio Code to build your solution, it runs two commands in the integrated terminal: docker build and docker push. These two commands build your code, containerize the CSharpModule.dll, and then push the code to the container registry that you specified when you initialized the solution.

You will be prompted to choose the module platform. Select *amd64* corresponding to Linux.



IMPORTANT

Only the Linux modules are supported.

You may see the following warning that you can ignore:

Program.cs(77,44): warning CS1998: This async method lacks 'await' operators and will run synchronously. Consider using the 'await' operator to await non-blocking API calls, or 'await Task.Run(...)' to do CPU-bound work on a background thread.

5. You can see the full container image address with tag in the VS Code integrated terminal. The image address is built from information that's in the module.json file with the format

<repository>:<version>-<platform> . For this article, it should look like

mycontreg2.azurecr.io/filecopymodule:0.0.1-amd64 .

Next steps

To deploy and run this module on Azure Stack Edge Pro, see the steps in [Add a module](#).

Enable Azure Arc on Kubernetes cluster on your Azure Stack Edge Pro GPU device

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article shows you how to enable Azure Arc on an existing Kubernetes cluster on your Azure Stack Edge Pro device.

This procedure is intended for those who have reviewed the [Kubernetes workloads on Azure Stack Edge Pro device](#) and are familiar with the concepts of [What is Azure Arc-enabled Kubernetes \(Preview\)?](#).

Prerequisites

Before you can enable Azure Arc on Kubernetes cluster, make sure that you have completed the following prerequisites on your Azure Stack Edge Pro device and the client that you will use to access the device:

For device

1. You have sign-in credentials to a 1-node Azure Stack Edge Pro device.
 - a. The device is activated. See [Activate the device](#).
 - b. The device has the compute role configured via Azure portal and has a Kubernetes cluster. See [Configure compute](#).
2. You've owner access to the subscription. You would need this access during the role assignment step for your service principal.

For client accessing the device

1. You have a Windows client system that will be used to access the Azure Stack Edge Pro device.
 - The client is running Windows PowerShell 5.0 or later. To download the latest version of Windows PowerShell, go to [Install Windows PowerShell](#).
 - You can have any other client with a [Supported operating system](#) as well. This article describes the procedure when using a Windows client.
2. You have completed the procedure described in [Access the Kubernetes cluster on Azure Stack Edge Pro device](#). You have:
 - Installed `kubectl` on the client.
 - Make sure that the `kubectl` client version is skewed no more than one version from the Kubernetes master version running on your Azure Stack Edge Pro device.
 - Use `kubectl version` to check the version of kubectl running on the client. Make a note of the full version.
 - In the local UI of your Azure Stack Edge Pro device, go to **Software update** and note the Kubernetes server version number.

The screenshot shows the Azure Stack Edge Pro (1 GPU) configuration interface. On the left, there's a sidebar with various settings like Overview, Configuration, Maintenance, and Power. The main pane is titled "Software update" and displays device software and Kubernetes versions. A specific line of text, "Kubernetes server version: v1.17.3", is highlighted with a red box.

- Verify these two versions are compatible.

Register Kubernetes resource providers

Before you enable Azure Arc on the Kubernetes cluster, you will need to enable and register

`Microsoft.Kubernetes` and `Microsoft.KubernetesConfiguration` against your subscription.

- To enable a resource provider, in the Azure portal, go to the subscription that you are planning to use for the deployment. Go to **Resource Providers**.
- In the right-pane, search for the providers you want to add. In this example, `Microsoft.Kubernetes` and `Microsoft.KubernetesConfiguration`.

Provider	Status
Microsoft.Kubernetes	NotRegistered
Microsoft.KubernetesConfiguration	NotRegistered

- Select a resource provider and from the top of the command bar, select **Register**. Registration takes several minutes.

Provider	Status
Microsoft.Kubernetes	NotRegistered
Microsoft.KubernetesConfiguration	NotRegistered

4. Refresh the UI until you see that the resource provider is registered. Repeat the process for both resource providers.

The screenshot shows the 'SMS Automation | Resource providers' page in the Azure portal. The left sidebar has a 'Resource providers' item highlighted with a red box. The main area shows a search bar with 'Microsoft.Kubernetes' and a table with two rows. Both rows have a green checkmark and the word 'Registered' next to them. The table columns are 'Provider' and 'Status'.

Provider	Status
Microsoft.Kubernetes	Registered
Microsoft.KubernetesConfiguration	Registered

You can also register resource providers via the `az cli`. For more information, see [Register the two providers for Azure Arc-enabled Kubernetes](#).

Create service principal, assign role

1. Make sure that you have `Subscription ID` and the name of the resource group you used for the resource deployment for your Azure Stack Edge service. To get the subscription ID, go to your Azure Stack Edge resource in the Azure portal. Navigate to **Overview > Essentials**.

The screenshot shows the 'myasegpures1' resource group details in the Azure portal. The 'Overview' tab is selected and highlighted with a red box. The 'Essentials' section is expanded, showing device information like model, location, and software version. The 'Subscription ID' field is highlighted with a red box and contains the placeholder '<Your-subscription-ID>'.

To get the resource group name, go to **Properties**.

The screenshot shows the 'myasegpures1' resource group properties in the Azure portal. The 'Properties' tab is selected and highlighted with a red box. The 'Resource group' field is highlighted with a red box and contains the value 'myaserg1'.

2. To create a service principal, use the following command via the `az cli`.

```
az ad sp create-for-rbac --name "<Informative name for service principal>"
```

For information on how to log into the [az cli](#), [Start Cloud Shell in Azure portal](#). If using [az cli](#) on a local client to create the service principal, make sure that you are running version 2.25 or later.

Here is an example.

```
PS /home/user> az ad sp create-for-rbac --name "https://azure-arc-for-ase-k8s"
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-arc-for-ase-k8s",
  "name": "https://azure-arc-for-ase-k8s",
  "password": "<password>",
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
PS /home/user>
```

3. Make a note of the `appId`, `name`, `password`, and `tenantID` as you will use this as input in the next command.
4. After creating the new service principal, assign the `Kubernetes Cluster - Azure Arc Onboarding` role to the newly created principal. This is a built-in Azure role (use the role ID in the command) with limited permissions. Use the following command:

```
az role assignment create --role 34e09817-6cbe-4d01-b1a2-e0eac5743d41 --assignee <appId-from-service-principal> --scope /subscriptions/<SubscriptionID>/resourceGroups/<Resource-group-name>
```

Here is an example.

```
PS /home/user> az role assignment create --role 34e09817-6cbe-4d01-b1a2-e0eac5743d41 --assignee
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx --scope /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/myaserg1
{
  "canDelegate": null,
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/myaserg1/providers/Microsoft.Authorization/roleAssignments/59272f92-e5ce-
4aeb-9c0c-62532d8caf25",
  "name": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "principalId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "principalType": "ServicePrincipal",
  "resourceGroup": "myaserg1",
  "roleDefinitionId": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Authorization/roleDefinitions/34e09817-6cbe-4d01-b1a2-e0eac5743d41",
  "scope": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/myaserg1",
  "type": "Microsoft.Authorization/roleAssignments"
}
PS /home/user>
```

Enable Arc on Kubernetes cluster

Follow these steps to configure the Kubernetes cluster for Azure Arc management:

1. [Connect to the PowerShell interface](#) of your device.
2. Type:

```
Set-HcsKubernetesAzureArcAgent -SubscriptionId "<Your Azure Subscription Id>" -ResourceGroupName "
<Resource Group Name>" -ResourceName "<Azure Arc resource name (shouldn't exist already)>" -Location "
<Region associated with resource group>" -TenantId "<Tenant Id of service principal>" -ClientId "<App id of service principal>"
```

When this command is run, there is a followup prompt to enter the `ClientSecret`. Provide the service

principal password.

Add the `CloudEnvironment` parameter if you are using a cloud other than Azure public. You can set this parameter to `AZUREPUBLICCLOUD`, `AZURECHINACLOUD`, `AZUREGERMANCLOUD`, and `AZUREUSGOVERNMENTCLOUD`.

NOTE

- To deploy Azure Arc on your device, make sure that you are using a [Supported region for Azure Arc](#).
- Use the `az account list-locations` command to figure out the exact location name to pass in the `Set-HcsKubernetesAzureArcAgent` cmdlet. Location names are typically formatted without any spaces.
- `ClientId` and `ClientSecret` are required.

Here is an example:

```
[10.100.10.10]: PS>Set-HcsKubernetesAzureArcAgent -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -ResourceGroupName "myaserg1" -ResourceName "myasetestresarc" -Location "westeurope" -TenantId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -ClientId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

WARNING: A script or application on the remote computer 10.126.76.0 is sending a prompt request. When
you are prompted,
enter sensitive information, such as credentials or passwords, only if you trust the remote computer
and the
application or script that is requesting the data.

cmdlet Set-HcsKubernetesAzureArcAgent at command pipeline position 1

Supply values for the following parameters:
ClientSecret: ****
[10.100.10.10]: PS>
```

In the Azure portal, a resource should be created with the name you provided in the preceding command.

Name	Type	Resource group	Location	Subscription
myasetestresarc	Azure Arc enabled Kube...	myaserg1	West Europe	SMS Automation

3. To verify that Azure Arc is enabled successfully, run the following command from PowerShell interface:

```
kubectl get deployments,pods -n azure-arc
```

Here is a sample output that shows the Azure Arc agents that were deployed on your Kubernetes cluster in the `azure-arc` namespace.

```
[10.128.44.240]: PS>kubectl get deployments,pods -n azure-arc
NAME                                READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/cluster-metadata-operator   1/1     1           1           13d
deployment.apps/clusterconnect-agent       1/1     1           1           13d
deployment.apps/clusteridentityoperator    1/1     1           1           13d
deployment.apps/config-agent              1/1     1           1           13d
deployment.apps/controller-manager        1/1     1           1           13d
deployment.apps/extension-manager         1/1     1           1           13d
deployment.apps/flux-logs-agent          1/1     1           1           13d
deployment.apps/kube-aad-proxy           1/1     1           1           13d
deployment.apps/metrics-agent            1/1     1           1           13d
deployment.apps/resource-sync-agent      1/1     1           1           13d

NAME                               READY   STATUS    RESTARTS   AGE
pod/cluster-metadata-operator-9568b899c-2stjn 2/2     Running   0          13d
pod/clusterconnect-agent-576758886d-vggmv   3/3     Running   0          13d
pod/clusteridentityoperator-6f59466c87-mm96j 2/2     Running   0          13d
pod/config-agent-7cbd6cb89f-9fdnt        2/2     Running   0          13d
pod/controller-manager-df6d56db5-kxmfj      2/2     Running   0          13d
pod/extension-manager-58c94c5b89-c6q72     2/2     Running   0          13d
pod/flux-logs-agent-6db9687fcb-rmxww     1/1     Running   0          13d
pod/kube-aad-proxy-67b87b9f55-bthqv      2/2     Running   0          13d
pod/metrics-agent-575c565fd9-k5j2t        2/2     Running   0          13d
pod/resource-sync-agent-6bbd8bcd86-x5bk5   2/2     Running   0          13d

[10.128.44.240]: PS>
```

A conceptual overview of these agents is available [here](#).

Remove Arc from the Kubernetes cluster

To remove the Azure Arc management, follow these steps:

1. a. [Connect to the PowerShell interface](#) of your device.
2. Type:

```
Remove-HcsKubernetesAzureArcAgent
```

NOTE

By default, when resource `yamls` are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster. You need to set `--sync-garbage-collection` in Arc OperatorParams to allow the deletion of resources when deleted from git repository. For more information, see [Delete a configuration](#)

Next steps

To understand how to run an Azure Arc deployment, see [Deploy a stateless PHP Guestbook application with Redis via GitOps on an Azure Stack Edge Pro device](#)

Deploy a PHP `guestbook` stateless application with Redis on Azure Arc-enabled Kubernetes cluster on Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article shows you how to build and deploy a simple, multi-tier web application using Kubernetes and Azure Arc. This example consists of the following components:

- A single-instance Redis master to store `guestbook` entries
- Multiple replicated Redis instances to serve reads
- Multiple web frontend instances

The deployment is done using GitOps on the Azure Arc-enabled Kubernetes cluster on your Azure Stack Edge Pro device.

This procedure is intended for people who have reviewed the [Kubernetes workloads on Azure Stack Edge Pro device](#) and are familiar with the concepts of [What is Azure Arc-enabled Kubernetes \(Preview\)](#).

NOTE

This article contains references to the term *slave*, a term that Microsoft no longer uses. When the term is removed from the software, we'll remove it from this article.

Prerequisites

Before you can deploy the stateless application, make sure that you have completed the following prerequisites on your device and the client that you will use to access the device:

For device

1. You have sign-in credentials to a 1-node Azure Stack Edge Pro device.
 - a. The device is activated. See [Activate the device](#).
 - b. The device has the compute role configured via Azure portal and has a Kubernetes cluster. See [Configure compute](#).
2. You have enabled Azure Arc on the existing Kubernetes cluster on your device and you have a corresponding Azure Arc resource in the Azure portal. For detailed steps, see [Enable Azure Arc on Azure Stack Edge Pro device](#).

For client accessing the device

1. You have a Windows client system that will be used to access the Azure Stack Edge Pro device.
 - The client is running Windows PowerShell 5.0 or later. To download the latest version of Windows PowerShell, go to [Install Windows PowerShell](#).
 - You can have any other client with a [Supported operating system](#) as well. This article describes the procedure when using a Windows client.

2. You have completed the procedure described in [Access the Kubernetes cluster on Azure Stack Edge Pro device](#). You have:

- Installed `kubectl` on the client.
- Make sure that the `kubectl` client version is skewed no more than one version from the Kubernetes master version running on your Azure Stack Edge Pro device.
 - Use `kubectl version` to check the version of kubectl running on the client. Make a note of the full version.
 - In the local UI of your Azure Stack Edge Pro device, go to **Overview** and note the Kubernetes software number.
 - Verify these two versions for compatibility from the mapping provided in the Supported Kubernetes version.

3. You have a [GitOps configuration that you can use to run an Azure Arc deployment](#). In this example, you will use the following `yaml` files to deploy on your Azure Stack Edge Pro device.

- `frontend-deployment.yaml`
- `frontend-service.yaml`
- `redis-master-deployment.yaml`
- `redis-master-service.yaml`
- `redis-slave-deployment.yaml`
- `redis-slave-service.yaml`

Deploy configuration

Follow these steps to configure the Azure Arc resource to deploy a GitOps configuration via the Azure portal:

1. In your Azure portal, go to the Azure Arc resource that you have created when you enabled Azure Arc on the Kubernetes cluster on your device.

Name	Type	Resource group	Location	Subscription
myasetestresarc	Azure Arc enabled Kube...	myaserg1	West Europe	SMS Automation

2. Go to **Configurations** and select **+ Add configuration**.

The screenshot shows the 'Configurations' section of the Azure Arc enabled Kubernetes interface. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Settings, Policies, Properties, Locks, and Export template. The 'Configurations' link is also highlighted with a red box. The main area has a search bar, a 'Refresh' button, and a table header with columns: Name, Operator instance, Operator namespace, Operator scope, Operator state, and Last applied. A message 'No results.' is displayed below the table.

3. In **Add configuration**, enter the appropriate values for the fields, and then select **Apply**.

PARAMETER	DESCRIPTION
Configuration name	Name for the configuration resource.
Operator instance name	Instance name of the operator to identify a specific configuration. Name is a string of maximum 253 characters that must be lowercase, alphanumeric, hyphen, and period only.
Operator namespace	Set to demotestguestbook to match the namespace specified in the deployment <code>yaml</code> . The field defines the namespace where the operator is installed. Name is a string of maximum 253 characters that must be lowercase, alphanumeric, hyphen, and period only.
Repository URL	Path to the git repository in <code>http://github.com/username/repo</code> or <code>git://github.com/username/repo</code> format where your GitOps configuration is located.
Operator scope	Select Namespace . This parameter defines the scope at which the operator is installed. Select Namespace to install your operator in the namespace specified in the deployment yaml files.
Operator type	Leave at default. This parameter specifies the type of the operator - by default, set as flux.
Operator params	Leave this blank. This parameter contains parameters to pass to the flux operator.
Helm	Set this parameter to Disabled . Enable this option if you will do chart-based deployments.

New Configuration

X

Configuration name * ⓘ

myazurearc1



Operator instance name * ⓘ

aseoperator1



Operator namespace * ⓘ

demotestguestbook



Repository URL * ⓘ

https://github.com/kagoyal/dbehaikudemo



Operator scope ⓘ

namespace cluster

Operator type ⓘ

Flux

Operator params ⓘ

Helm ⓘ

Enabled Disabled

Add

Cancel

4. The configuration deployment starts and the **Operator state** shows as **Pending**.

The screenshot shows the 'Configurations' section of the 'myasetestresarc' resource. The configuration table has one row highlighted with a red border:

Name	Operator instance	Operator namespace	Operator scope	Operator state	Last applied
myazurearc1	aseoperator1	demotestguestbook	namespace	Pending	--

The 'Configurations' link in the left sidebar is also highlighted with a red border.

5. The deployment takes a couple minutes. When the deployment completes, the **Operator state** shows as **Installed**.

The screenshot shows the 'Configurations' section of the Azure Arc enabled Kubernetes interface. On the left, there's a sidebar with links for Overview, Activity log, Access control (IAM), Tags, Settings, and Configurations (which is highlighted with a red box). The main area has a search bar, an 'Add configuration' button, and a 'Refresh' button. A table lists configurations with columns: Name, Operator instance, Operator namespace, Operator scope, Operator state, and Last applied. One row is selected, showing 'myazurearc1', 'aseoperator1', 'demotestguestbook', 'namespace', 'Installed', and '8/24/2020, 11:15'.

Verify deployment

The deployment via the GitOps configuration creates a `demotestguestbook` namespace as specified in the deployment `.yaml` files located in the git repo.

1. After you have applied the GitOps configuration, [Connect to the PowerShell interface of the device](#).
2. Run the following command to list the pods running in the `demotestguestbook` namespace corresponding to the deployment.

```
kubectl get pods -n <your-namespace>
```

Here is a sample output.

```
[10.128.44.240]: PS>kubectl get pods -n demotestguestbook
NAME           READY   STATUS    RESTARTS   AGE
aseoperator1-5569658644-cqtb5  1/1     Running   0          91m
frontend-6cb7f8bd65-4xb4f      1/1     Running   0          91m
frontend-6cb7f8bd65-q9cxj      1/1     Running   0          91m
frontend-6cb7f8bd65-xpzs6      1/1     Running   0          91m
memcached-86bdf9f56b-512fq     1/1     Running   0          91m
redis-master-7db7f6579f-2z29w  1/1     Running   0          91m
redis-slave-7664787fbc-lgr2n   1/1     Running   0          91m
redis-slave-7664787fbc-vlvzn   1/1     Running   0          91m
[10.128.44.240]: PS>
```

3. In this example, the frontend service was deployed as type:LoadBalancer. You will need to find the IP address of this service to view the `guestbook`. Run the following command.

```
kubectl get service -n <your-namespace>
```

```
[10.128.44.240]: PS>kubectl get service -n demotestguestbook
NAME        TYPE        CLUSTER-IP      EXTERNAL-IP      PORT(S)        AGE
frontend    LoadBalancer 10.96.79.38    10.128.44.245   80:31238/TCP  85m
memcached   ClusterIP   10.102.47.75   <none>          11211/TCP    85m
redis-master ClusterIP  10.104.32.99   <none>          6379/TCP    85m
redis-slave  ClusterIP   10.104.215.146  <none>          6379/TCP    85m
[10.128.44.240]: PS>
```

4. The frontend service of `type:LoadBalancer` has an external IP address. This IP is from the IP address range that you specified for external services when configuring the Compute network settings on the device. Use this IP address to view the `guestbook` at URL: `https://<external-IP-address>`.

Leaving one more message!

Submit

Leaving a message!

Delete deployment

To delete the deployment, you can delete the configuration from the Azure portal. Deleting the configuration will delete the objects that were created, including deployments and services.

1. In the Azure portal, go the Azure Arc resource > Configurations.
2. Locate the configuration you want to delete. Select the ... to invoke the context menu and select **Delete**.

Home > myasetestresarc | Configurations

Azure Arc enabled Kubernetes

Search (Ctrl+ /) Add configuration Refresh

Name	Operator instance	Operator namespace	Operator scope	Operator state	Last applied
myazurearc1	aseoperator1	demotestguestbook	namespace	Installed	07/11/2020 11:15 PM PDT

Details

Delete

It may take up several minutes for the configuration to be deleted.

Next steps

Learn how to [Use Kubernetes Dashboard to monitor deployments on your Azure Stack Edge Pro device](#)

Deploy Azure Data Services on your Azure Stack Edge Pro GPU device

9/21/2022 • 10 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the process of creating an Azure Arc Data Controller and then deploying Azure Data Services on your Azure Stack Edge Pro GPU device.

Azure Arc Data Controller is the local control plane that enables Azure Data Services in customer-managed environments. Once you have created the Azure Arc Data Controller on the Kubernetes cluster that runs on your Azure Stack Edge Pro GPU device, you can deploy Azure Data Services such as SQL Managed Instance on that data controller.

The procedure to create Data Controller and then deploy an SQL Managed Instance involves the use of PowerShell and `kubectl` - a native tool that provides command-line access to the Kubernetes cluster on the device.

Prerequisites

Before you begin, make sure that:

1. You've access to an Azure Stack Edge Pro GPU device and you've activated your device as described in [Activate Azure Stack Edge Pro](#).
2. You've enabled the compute role on the device. A Kubernetes cluster was also created on the device when you configured compute on the device as per the instructions in [Configure compute on your Azure Stack Edge Pro GPU device](#).
3. You have the Kubernetes API endpoint from the **Device** page of your local web UI. For more information, see the instructions in [Get Kubernetes API endpoint](#).
4. You've access to a client that will connect to your device.
 - a. This article uses a Windows client system running PowerShell 5.0 or later to access the device. You can use any other client with a [Supported operating system](#).
 - b. Install `kubectl` on your client. For the client version:
 - a. Identify the Kubernetes server version installed on the device. In the local UI of the device, go to [Software updates](#) page. Note the **Kubernetes server version** in this page.
 - b. Download a client that is skewed no more than one minor version from the master. The client version but may lead the master by up to one minor version. For example, a v1.3 master should work with v1.1, v1.2, and v1.3 nodes, and should work with v1.2, v1.3, and v1.4 clients. For more information on Kubernetes client version, see [Kubernetes version and version skew support policy](#).
5. Optionally, [Install client tools for deploying and managing Azure Arc-enabled data services](#). These tools are not required but recommended.
6. Make sure you have enough resources available on your device to provision a data controller and one SQL Managed Instance. For data controller and one SQL Managed Instance, you will need a minimum of 16 GB of RAM and 4 CPU cores. For detailed guidance, go to [Minimum requirements for Azure Arc](#).

enabled data services deployment.

Configure Kubernetes external service IPs

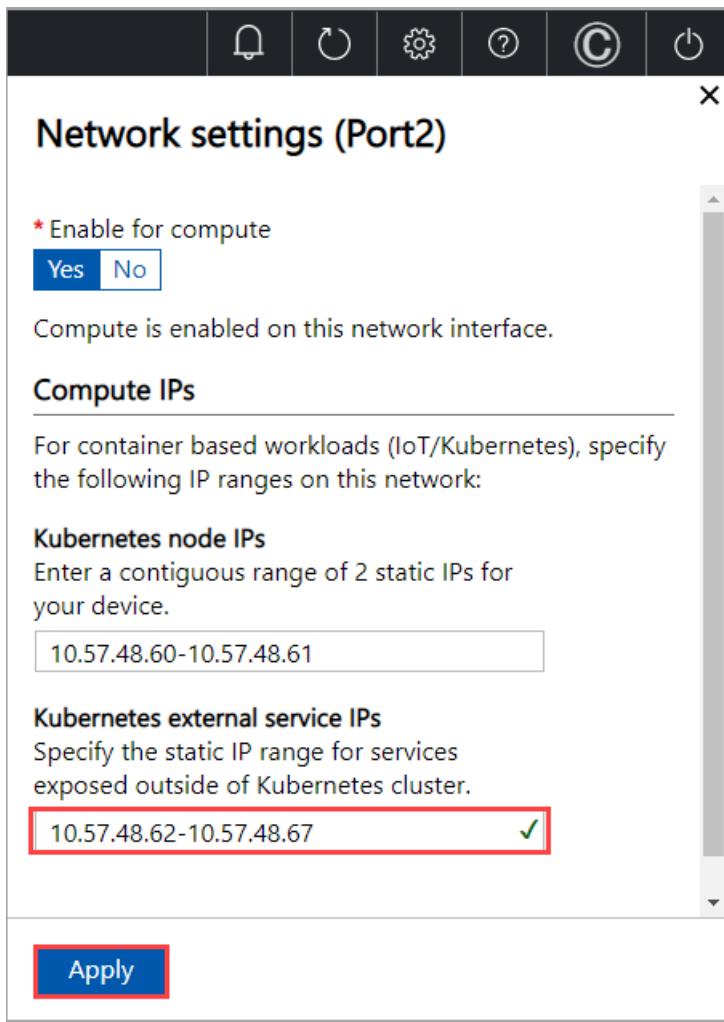
1. Go the local web UI of the device and then go to Compute.
2. Select the network enabled for compute.

The screenshot shows the Azure Stack Edge Pro (1 GPU) local web UI. The top bar displays the device name "Azure Stack Edge Pro (1 GPU)" and various system icons. The left sidebar is titled "CONFIGURATION" and contains the following items: Overview, Get started, Network, **Compute** (highlighted with a red box), Web proxy, Device, Update server, Time, Certificates, and Cloud details. The main content area is titled "Compute" and shows the user "myasepgudev". It instructs to "Configure one network interface on your device for compute. Use this network interface to connect to any compute modules running on your device." Below this is a table with columns "Name", "Network", and "Enabled for compute". The table rows are:

Name	Network	Enabled for compute
Port 1	192.168.100.0	No
Port 2	10.57.48.0	Yes
Port 3	192.168.0.0	No
Port 4	192.168.0.0	No
Port 5	192.168.0.0	No
Port 6	192.168.0.0	No

At the bottom of the page are two buttons: "< Back to Overview" and "Next: Web proxy >".

3. Make sure that you provide three additional Kubernetes external service IPs (in addition to the IPs you have already configured for other external services or containers). The data controller will use two service IPs and the third IP is used when you create a SQL Managed Instance. You will need one IP for each additional Data Service you will deploy.



4. Apply the settings and these new IPs will immediately take effect on an already existing Kubernetes cluster.

Deploy Azure Arc Data Controller

Before you deploy a data controller, you'll need to create a namespace.

Create namespace

Create a new, dedicated namespace where you will deploy the Data Controller. You'll also create a user and then grant user the access to the namespace that you created.

NOTE

For both namespace and user names, the [DNS subdomain naming conventions](#) apply.

1. [Connect to the PowerShell interface](#).

2. Create a namespace. Type:

```
New-HcsKubernetesNamespace -Namespace <Name of namespace>
```

3. Create a user. Type:

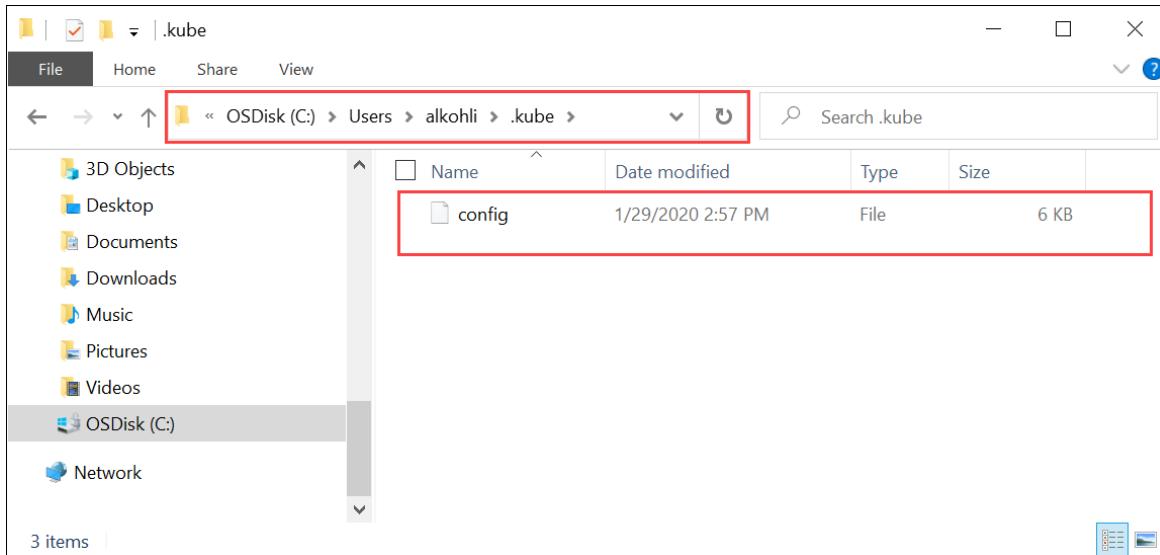
```
New-HcsKubernetesUser -UserName <User name>
```

4. A config file is displayed in plain text. Copy this file and save it as a *config* file.

IMPORTANT

Do not save the config file as `.txt` file, save the file without any file extension.

- The config file should live in the `.kube` folder of your user profile on the local machine. Copy the file to that folder in your user profile.



- Grant the user access to the namespace that you created. Type:

```
Grant-HcsKubernetesNamespaceAccess -Namespace <Name of namespace> -UserName <User name>
```

Here is a sample output of the preceding commands. In this example, we create a `myadstest` namespace, a `myadsuser` user and granted the user access to the namespace.

```
[10.100.10.10]: PS>New-HcsKubernetesNamespace -Namespace myadstest
[10.100.10.10]: PS>New-HcsKubernetesUser -UserName myadsuser
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data: LS0tLS1CRUdJTiBD=====/snipped//=====VSVE1GSUNBVETLS0tLQo=
  server: https://compute.myasegpudev.wdshcscsso.com:6443
  name: kubernetes
contexts:
- context:
  cluster: kubernetes
  user: myadsuser
  name: myadsuser@kubernetes
current-context: myadsuser@kubernetes
kind: Config
preferences: {}
users:
- name: myadsuser
  user:
    client-certificate-data: LS0tLS1CRUdJTiBDRV=====/snipped//=====EE9PQotLS0kFURSBLRVktLS0tLQo=

[10.100.10.10]: PS>Grant-HcsKubernetesNamespaceAccess -Namespace myadstest -UserName myadsuser
[10.100.10.10]: PS>Set-HcsKubernetesAzureArcDataController -SubscriptionId db4e2fdb-6d80-4e6e-b7cd-736098270664 -ResourceGroupName myasegpurg -Location "EastUS" -UserName myadsuser -Password "Password1" -DataControllerName "arctestcontroller" -Namespace myadstest
[10.100.10.10]: PS>
```

- Add a DNS entry to the hosts file on your system.

- Run Notepad as administrator and open the `hosts` file located at

```
C:\windows\system32\drivers\etc\hosts .
```

- b. Use the information that you saved from the **Device** page in the local UI (prerequisite) to create the entry in the hosts file.

For example, copy this endpoint `https://compute.myasegpudev.microsoftdatabox.com/[10.100.10.10]` to create the following entry with device IP address and DNS domain:

```
10.100.10.10 compute.myasegpudev.microsoftdatabox.com
```

8. To verify that you can connect to the Kubernetes pods, start a cmd prompt or a PowerShell session. Type:

```
PS C:\WINDOWS\system32> kubectl get pods -n "myadstest"
No resources found.
PS C:\WINDOWS\system32>
```

You can now deploy your data controller and data services applications in the namespace, then view the applications and their logs.

Create data controller

The data controller is a collection of pods that are deployed to your Kubernetes cluster to provide an API, the controller service, the bootstrapper, and the monitoring databases and dashboards. Follow these steps to create a data controller on the Kubernetes cluster that exists on your Azure Stack Edge device in the namespace that you created earlier.

1. Gather the following information that you'll need to create a data controller:

COLUMN1	COLUMN2
Data controller name	A descriptive name for your data controller. For example, <code>arctestdatacontroller</code> .
Data controller username	Any username for the data controller administrator user. The data controller username and password are used to authenticate to the data controller API to perform administrative functions.
Data controller password	A password for the data controller administrator user. Choose a secure password and share it with only those that need to have cluster administrator privileges.
Name of your Kubernetes namespace	The name of the Kubernetes namespace that you want to create the data controller in.
Azure subscription ID	The Azure subscription GUID for where you want the data controller resource in Azure to be created.
Azure resource group name	The name of the resource group where you want the data controller resource in Azure to be created.
Azure location	The Azure location where the data controller resource metadata will be stored in Azure. For a list of available regions, see Azure global infrastructure / Products by region .

2. Connect to the PowerShell interface. To create the data controller, type:

```
Set-HcsKubernetesAzureArcDataController -SubscriptionId <Subscription ID> -ResourceGroupName  
<Resource group name> -Location <Location without spaces> -UserName <User you created> -Password  
<Password to authenticate to Data Controller> -DataControllerName <Data Controller Name> -Namespace  
<Namespace you created>
```

Here is a sample output of the preceding commands.

```
[10.100.10.10]: PS>Set-HcsKubernetesAzureArcDataController -SubscriptionId db4e2fdb-6d80-4e6e-b7cd-  
736098270664 -ResourceGroupName myasegpurg -Location "EastUS" -UserName myadsuser -Password  
"Password1" -DataControllerName "arctestcontroller" -Namespace myadstest  
[10.100.10.10]: PS>
```

The deployment may take approximately 5 minutes to complete.

NOTE

The data controller created on Kubernetes cluster on your Azure Stack Edge Pro GPU device works only in the disconnected mode in the current release. The disconnected mode is for the Data Controller and not for your device.

Monitor data creation status

1. Open another PowerShell window.
2. Use the following `kubectl` command to monitor the creation status of the data controller.

```
kubectl get datacontroller/<Data controller name> --namespace <Name of your namespace>
```

When the controller is created, the status should be `Ready`. Here is a sample output of the preceding command:

```
PS C:\WINDOWS\system32> kubectl get datacontroller/arctestcontroller --namespace myadstest  
NAME          STATE  
arctestcontroller  Ready  
PS C:\WINDOWS\system32>
```

3. To identify the IPs assigned to the external services running on the data controller, use the `kubectl get svc -n <namespace>` command. Here is a sample output:

```

PS C:\WINDOWS\system32> kubectl get svc -n myadstest
NAME           TYPE      CLUSTER-IP   EXTERNAL-IP     PORT(S)
AGE
controldb-svc ClusterIP  172.28.157.130 <none>        1433/TCP,8311/TCP,8411/TCP
3d21h
controller-svc ClusterIP  172.28.123.251 <none>        443/TCP,8311/TCP,8301/TCP,8411/TCP,8401/TCP
3d21h
controller-svc-external LoadBalancer 172.28.154.30  10.57.48.63  30080:31090/TCP
3d21h
logsdb-svc    ClusterIP  172.28.52.196 <none>        9200/TCP,8300/TCP,8400/TCP
3d20h
logsgui-svc   ClusterIP  172.28.85.97  <none>        5601/TCP,8300/TCP,8400/TCP
3d20h
metricsdb-svc ClusterIP  172.28.255.103 <none>        8086/TCP,8300/TCP,8400/TCP
3d20h
metricsdc-svc ClusterIP  172.28.208.191 <none>        8300/TCP,8400/TCP
3d20h
metricsui-svc  ClusterIP  172.28.158.163 <none>        3000/TCP,8300/TCP,8400/TCP
3d20h
mgmtproxy-svc ClusterIP  172.28.228.229 <none>
443/TCP,8300/TCP,8311/TCP,8400/TCP,8411/TCP
3d20h
mgmtproxy-svc-external LoadBalancer 172.28.166.214 10.57.48.64  30777:30621/TCP
3d20h
sqlex-svc     ClusterIP  None          <none>        1433/TCP
3d20h
PS C:\WINDOWS\system32>

```

Deploy SQL managed instance

After you have successfully created the data controller, you can use a template to deploy a SQL Managed Instance on the data controller.

Deployment template

Use the following deployment template to deploy a SQL Managed Instance on the data controller on your device.

```
apiVersion: v1
data:
  password: UGFzc3dvcmQx
  username: bXlhZHN1c2Vy
kind: Secret
metadata:
  name: sqlex-login-secret
type: Opaque
---
apiVersion: sql.arcdata.microsoft.com/v1alpha1
kind: sqlmanagedinstance
metadata:
  name: sqlex
spec:
  limits:
    memory: 4Gi
    vcores: "4"
  requests:
    memory: 2Gi
    vcores: "1"
  service:
    type: LoadBalancer
  storage:
    backups:
      className: ase-node-local
      size: 5Gi
    data:
      className: ase-node-local
      size: 5Gi
    datalogs:
      className: ase-node-local
      size: 5Gi
    logs:
      className: ase-node-local
      size: 1Gi
```

Metadata name

The metadata name is the name of the SQL Managed Instance. The associated pod in the preceding `deployment.yaml` will be named as `sqlex-n` (`n` is the number of pods associated with the application).

Password and username data

The data controller username and password are used to authenticate to the data controller API to perform administrative functions. The Kubernetes secret for the data controller username and password in the deployment template are base64 encoded strings.

You can use an online tool to base64 encode your desired username and password or you can use built in CLI tools depending on your platform. When using an online Base64 encode tool, provide the user name and password strings (that you entered while creating the data controller) in the tool and the tool will generate the corresponding Base64 encoded strings.

Service type

Service type should be set to `LoadBalancer`.

Storage class name

You can identify the storage class on your Azure Stack Edge device that the deployment will use for data, backups, data logs and logs. Use the `kubectl get storageclass` command to get the storage class deployed on your device.

```
PS C:\WINDOWS\system32> kubectl get storageclass
NAME          PROVISIONER      RECLAIMPOLICY  VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ase-node-local  rancher.io/local-path  Delete    WaitForFirstConsumer  false                  5d23h
PS C:\WINDOWS\system32>
```

In the preceding sample output, the storage class `ase-node-local` on your device should be specified in the template.

Spec

To create an SQL Managed Instance on your Azure Stack Edge device, you can specify your memory and CPU requirements in the spec section of the `deployment.yaml`. Each SQL managed instance must request a minimum of 2-GB memory and 1 CPU core as shown in the following example.

```
spec:
  limits:
    memory: 4Gi
    vcores: "4"
  requests:
    memory: 2Gi
    vcores: "1"
```

For detailed sizing guidance for data controller and 1 SQL Managed Instance, review [SQL managed instance sizing details](#).

Run deployment template

Run the `deployment.yaml` using the following command:

```
kubectl create -n <Name of namespace that you created> -f <Path to the deployment yaml>
```

Here is a sample output of the following command:

```
PS C:\WINDOWS\system32> kubectl get pods -n "myadstest"
No resources found.
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> kubectl create -n myadstest -f C:\azure-arc-data-services\sqllex.yaml secret/sqllex-login-secret created
sqlmanagedinstance.sql.arcdata.microsoft.com/sqllex created
PS C:\WINDOWS\system32> kubectl get pods --namespace myadstest
NAME        READY   STATUS    RESTARTS   AGE
bootstrapper-mv2cd  1/1     Running   0          83m
control-w9s9l   2/2     Running   0          78m
controldb-0    2/2     Running   0          78m
controlwd-4bmc5  1/1     Running   0          64m
logsdb-0       1/1     Running   0          64m
logsui-wpmw2   1/1     Running   0          64m
metricsdb-0    1/1     Running   0          64m
metricsdc-fb5r5  1/1     Running   0          64m
metricsui-56qzs 1/1     Running   0          64m
mgmtproxy-2ck17 2/2     Running   0          64m
sqllex-0        3/3     Running   0          13m
PS C:\WINDOWS\system32>
```

The `sqllex-0` pod in the sample output indicates the status of the SQL Managed Instance.

Remove data controller

To remove the data controller, delete the dedicated namespace in which you deployed it.

```
kubectl delete ns <Name of your namespace>
```

Next steps

- [Deploy a stateless application on your Azure Stack Edge Pro.](#)

Configure load balancing with MetalLB on your Azure Stack Edge

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to configure load balancing on your Azure Stack Edge device using MetalLB via Border Gateway Protocol (BGP).

About MetalLB and load balancing

MetalLB is a load-balancer implementation for bare metal Kubernetes clusters. MetalLB serves two functions: it assigns IP addresses to the Kubernetes load balancer services from a configured pool of IP addresses and then announces the IP to the external network. MetalLB achieves these functions through standard routing protocols such as Address Resolution Protocol (ARP), Neighbor Discovery Protocol (NDP), or Border Gateway Protocol (BGP).

For more information, see [BGP mode for MetalLB](#).

MetalLB on Azure Stack Edge

There are multiple networking components such as Calico, MetalLB, and Core DNS installed on your Azure Stack Edge device. MetalLB hooks into the Kubernetes cluster running on your Azure Stack Edge device, and allows you to create Kubernetes services of type `LoadBalancer` in the cluster.

In BGP mode, all machines in the cluster establish BGP peering sessions with nearby routers that you control, and tell those routers how to forward traffic to the service IPs. MetalLB with the Border Gateway Protocol (BGP) is not the default networking mode for the Kubernetes cluster running on your device. To configure MetalLB via BGP, you designate the top-of-rack (ToR) switch as the load balancer and set up peer sessions.

MetalLB in BGP mode can be configured to achieve low failover times if you are using 2-node devices. This configuration is more involved than the standard configuration as you may not have access to the top-of-rack switch.

Configure MetalLB

You can configure MetalLB in BGP mode by connecting to the PowerShell interface of the device and then running specific cmdlets.

Prerequisites

Before you begin, make sure that:

- Compute is enabled on one port of the device. This creates a virtual switch on that port.
 - To enable compute, in the local UI for your device, go to [Advanced networking](#) page and select a port on which you want to enable compute.
 - In the [Network settings](#) page, enable the port for compute. **Apply** the settings.
- You have available IPs in the same subnet the port that you enabled for compute on your device.

Configuration

For a basic configuration for MetalLB using BGP session, you need the following information:

- The peer IP address that MetalLB should connect to.
- The peer's Autonomous System Number (ASN). BGP requires that routes are announced with an ASN for peer sessions.
- The ASN MetalLB should use. ASNs are 16-bit numbers between 1 and 65534 and 32-bit numbers between 131072 and 4294967294.

IMPORTANT

For MetalLB to work in BGP mode, peers must be specified. If no BGP peers are specified, MetalLB will work in default layer 2 mode. For more information, see [Layer 2 mode in MetalLB](#).

Follow these steps to configure MetalLB in BGP mode:

1. [Connect to the PowerShell interface](#) of the device.
2. Run the `Get-HcsExternalVirtualSwitch` cmdlet to get the name of the external virtual switch that you'll use for BGP mode. This virtual switch is created when you enabled the port for compute.

```
Get-HcsExternalVirtualSwitch
```

3. Run the `Set-HcsBGPPeer` cmdlet to establish a BGP peer session.

```
Set-HcsBGPPeer -PeerAddress <IP address of the port that you enabled for compute> -PeerAsn <ASN for the peer> -SelfAsn <Your ASN> -SwitchName <Name of virtual switch on the port enabled for compute> -HoldTimeInSeconds <Optional hold time in seconds>
```

4. Once you have established the session, run the `Get-HcsBGPPeers` cmdlet to get the peer sessions that exist on a virtual switch.

```
Get-HcsBGPPeers -SwitchName <Name of virtual switch that you enabled for compute>
```

5. Run the `Remove-HcsBGPPeer` cmdlet to remove the peer session.

```
Remove-HcsBGPPeer -PeerAddress <IP address of the port that you enabled for compute> -SwitchName <Name of virtual switch on the port enabled for compute>
```

6. Run the `Get-HcsBGPPeers` to verify that the peer session is removed.

Here is an example output:

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> $Name = "dbe-1csphq2.microsoftdatabox.com"
PS C:\WINDOWS\system32> Set-Item WSMan:\localhost\Client\TrustedHosts $Name -Concatenate -Force
PS C:\WINDOWS\system32> $sessOptions = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName
Minishell -UseSSL -SessionOption $sessOptions
WARNING: The Windows PowerShell interface of your device is intended to
be used only for the initial network configuration. Please
engage Microsoft Support if you need to access this interface
to troubleshoot any potential issues you may be experiencing.
Changes made through this interface without involving Microsoft
Support could result in an unsupported configuration.
[dbe-1csphq2.microsoftdatabox.com]: PS>Get-HcsExternalVirtualSwitch

Name          : vSwitch1
InterfaceAlias : {Port2}
EnableIov      : False
MacAddressPools :
IPAddressPools : {}
BGPPeers       :
ConfigurationSource : Dsc
EnabledForCompute : False
EnabledForStorage : False
EnabledForMgmt   : True
SupportsAcceleratedNetworking : False
DbeDhcpHostVnicName : 3cb2d0ae-6a7b-44cc-8a5d-8eac2d1c0436
VirtualNetworks : {}
EnableEmbeddedTeaming : True
Vnics          : {}
Type           : External

Name          : vSwitch2
InterfaceAlias : {Port3, Port4}
EnableIov      : False
MacAddressPools :
IPAddressPools : {}
BGPPeers       :
ConfigurationSource : Dsc
EnabledForCompute : False
EnabledForStorage : True
EnabledForMgmt   : False
SupportsAcceleratedNetworking : False
DbeDhcpHostVnicName : 8dd480c0-8f22-42b1-8621-d2a43f70690d
VirtualNetworks : {}
EnableEmbeddedTeaming : True
Vnics          : {}
Type           : External

[dbe-1csphq2.microsoftdatabox.com]: PS>Set-HcsBGPPeer -PeerAddress 10.126.77.125 -PeerAsn 64512 -SelfAsn
64513 -SwitchName vSwitch1 -HoldTimeInSeconds 15
[dbe-1csphq2.microsoftdatabox.com]: PS>Get-HcsBGPPeers -SwitchName vSwitch1

PeerAddress  PeerAsn SelfAsn HoldTime
-----  -----  -----
10.126.77.125 64512  64513    15

[dbe-1csphq2.microsoftdatabox.com]: PS>Remove-HcsBGPPeer -PeerAddress 10.126.77.125 -SwitchName vSwitch1
[dbe-1csphq2.microsoftdatabox.com]: PS>Get-HcsBGPPeers -SwitchName vSwitch1
[dbe-1csphq2.microsoftdatabox.com]: PS>

```

Next steps

- Learn more about [Networking on Kubernetes cluster on your Azure Stack Edge device](#).

Deploy IoT Edge on an Ubuntu VM on Azure Stack Edge

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to deploy an IoT Edge runtime on an Ubuntu VM running on your Azure Stack Edge device. For new development work, use the self-serve deployment method described in this article as it uses the latest software version.

High-level flow

The high-level flow is as follows:

1. Create or identify the IoT Hub or [Azure IoT Hub Device Provisioning Service \(DPS\)](#) instance.
2. Use Azure CLI to acquire the Ubuntu 20.04 LTS VM image.
3. Upload the Ubuntu image onto the Azure Stack Edge VM image library.
4. Deploy the Ubuntu image as a VM using the following steps:
 - a. Provide the name of the VM, the username, and the password. Creating another disk is optional.
 - b. Set up the network configuration.
 - c. Provide a prepared *cloud-init* script on the *Advanced* tab.

Prerequisites

Before you begin, make sure you have:

- An Azure Stack Edge device that you've activated. For detailed steps, see [Activate Azure Stack Edge Pro GPU](#).
- Access to the latest Ubuntu 20.04 VM image, either the image from Azure Marketplace or a custom image that you're bringing:

```
$urn = Canonical:0001-com-ubuntu-server-focal:20_04-lts:20.04.202007160
```

Use steps in [Search for Azure Marketplace images](#) to acquire the VM image.

Prepare the cloud-init script

To deploy the IoT Edge runtime onto the Ubuntu VM, use a *cloud-init* script during the VM deployment.

Use steps in one of the following sections:

- [Prepare the cloud-init script with symmetric key provisioning](#).
- [Prepare the cloud-init script with IoT Hub DPS](#).

Use symmetric key provisioning

To connect your device to IoT Hub without DPS, use the steps in this section to prepare a *cloud-init* script for the VM creation *Advanced* page to deploy the IoT Edge runtime and Nvidia's container runtime.

1. Use an existing IoT Hub or create a new Hub. Use these steps to [create an IoT Hub](#).

2. Use these steps to [register your Azure Stack Edge device in IoT Hub](#).
3. Retrieve the Primary Connection String from IoT Hub for your device, and then paste it into the location below for *DeviceConnectionString*.

Cloud-init script for symmetric key provisioning

```
#cloud-config

runcmd:
- dcs=<DeviceConnectionString>
- |
  set -x
(
  # Wait for docker daemon to start

  while [ $(ps -ef | grep -v grep | grep docker | wc -l) -le 0 ]; do
    sleep 3
  done

  if [ $(lspci | grep NVIDIA | wc -l) -gt 0 ]; then

    #install Nvidia drivers

    apt install -y ubuntu-drivers-common
    ubuntu-drivers devices
    ubuntu-drivers autoinstall

    # Install NVIDIA Container Runtime

    curl -s -L https://nvidia.github.io/nvidia-container-runtime/gpgkey | apt-key add -
    distribution=$(./etc/os-release;echo $ID$VERSION_ID)
    curl -s -L https://nvidia.github.io/nvidia-container-runtime/$distribution/nvidia-container-
    runtime.list | tee /etc/apt/sources.list.d/nvidia-container-runtime.list
    apt update
    apt install -y nvidia-container-runtime
  fi

  # Restart Docker

  systemctl daemon-reload
  systemctl restart docker

  # Install IoT Edge

  apt install -y aziot-edge

  if [ ! -z $dcs ]; then
    iotedge config mp --connection-string $dcs
    iotedge config apply
  fi
  if [ $(lspci | grep NVIDIA | wc -l) -gt 0 ]; then
    reboot
  fi      ) &

apt:
  preserve_sources_list: true
  sources:
    msft.list:
      source: "deb https://packages.microsoft.com/ubuntu/20.04/prod focal main"
      key: |
        -----BEGIN PGP PUBLIC KEY BLOCK-----
        Version: GnuPG v1.4.7 (GNU/Linux)

        mQENBFYxWIwBCADAKoZhZlJxGNGWzqV+1OG1xiQeoowKhssGAKvd+buXCGISZJwT

```

```

LXZqIcIiLP7pqdcZWtE9bSc7yBY2MalDp9Liu0KekywQ6VVX1T72NPf5Ev6x6DLV
7aVwsCzUAF+eb7DC9fPuFLEdxmOEYoPjznQ7cCnSV4JQxAqhU4T60jbvRazG13ag
OeizPXmR1jMtUUttHQZnRhtlzkmwIrUivbfPD+fEoHJ1+uIdfOzZX8/oKHKLe2j
H632kvsNzJF1ROVvGLYAk2WRcLu+Rjjggixhwib+Mu/A8Tf4V6b+Ypps44q8EvVr
M+QvY7LNSOFFoS6S1sy9oisGTdfE39nC7pVRABEBAAG0N01pY3Jvc29mdCAoUmVs
ZWFZZSBzaWduaW5nKSA8Z3Bnc2VjdXJpdH1AbW1jcm9zb2Z0LmNvbT6JATUEwEC
AB8FA1YxWIwCGwMGCwkIBwMCBBUCCAMDFgIBAh4BAheAAAoJEos+lK2+EiPGpsH
/32vKy29Hg51H9dffJmx0/a/F+5vKeCeVqimvyTM04C+XENNusbYZ3eRPHGHFLqe
MNGxsfb7C7zxEeW7J/vSzRgHxm7ZvESisUYRFq2sgkJ+HFERNrqfcia5bdhmrUsy
7SWw9ybxsdFOkuQoyKD3tBm1GFONQM1BaOMWdAsic965rvJsd5zYaZZFI1UwTkFXV
KJt3bp3Ngn1vEYXwijGta+FXz6GLHueJwF0I7ug34DgUKAFvAs8Hacr2DRYXL5RJ
XdNgj4Jd2/g6T9InmWT0hAS1jur+dJnzNiNCkbn9KbX7J/qK1IbR8y560yRmFsU+
NdCFTw7wY0Fb1fwJ+/KtsC4=
=J6gs
-----END PGP PUBLIC KEY BLOCK-----
packages:
- moby-cli
- moby-engine
write_files:
- path: /etc/systemd/system/docker.service.d/override.conf
  permissions: "0644"
  content: |
    [Service]
    ExecStart=
    ExecStart=/usr/bin/dockerd --host=fd:// --add-runtime=nvidia=/usr/bin/nvidia-container-runtime --log-
    driver local

```

Use DPS

Use steps in this section to connect your device to DPS and IoT Central. You'll prepare a *script.sh* file to deploy the IoT Edge runtime as you create the VM.

1. Use the existing IoT Hub and DPS, or create a new IoT Hub.
 - Use these steps to [create an IoT Hub](#).
 - Use these steps to [create the DPS, and then link the IoT Hub to the DPS scope](#).
2. Go to the DPS resource and create an individual enrollment.
 - a. Go to **Device Provisioning Service > Manage enrollments > Add individual enrollment**.
 - b. Make sure that the selection for **Symmetric Key for attestation type** and **IoT Edge device** is **True**. The default selection is **False**.
 - c. Retrieve the following information from the DPS resource page:
 - **Registration ID**. We recommend that you use the same ID as the **Device ID** for your IoT Hub.
 - **ID Scope** which is available in the [Overview menu](#).
 - **Primary SAS Key** from the Individual Enrollment menu.
3. Copy and paste values from IoT Hub (IDScope) and DPS (RegistrationID, Symmetric Key) into the script arguments.

Cloud-init script for IoT Hub DPS

```

#cloud-config

runcmd:
  - dps_idscope=<DPS IDScope>
  - registration_device_id=<RegistrationID>
  - key=<Symmetric Key>
  - |
    set -x
    (
      wget https://github.com/Azure/iot-edge-config/releases/latest/download/azure-iot-edge-installer.sh -O azure-iot-edge-installer.sh \
      && chmod +x azure-iot-edge-installer.sh \
      && sudo -H ./azure-iot-edge-installer.sh -s $dps_idscope -r $registration_device_id -k $key \
      && rm -rf azure-iot-edge-installer.sh

    # Wait for docker daemon to start

    while [ $(ps -ef | grep -v grep | grep docker | wc -l) -le 0 ]; do
      sleep 3
    done

    systemctl stop aziot-edge

    if [ $(lspci | grep NVIDIA | wc -l) -gt 0 ]; then

      #install Nvidia drivers

      apt install -y ubuntu-drivers-common
      ubuntu-drivers devices
      ubuntu-drivers autoinstall

      # Install NVIDIA Container Runtime

      curl -s -L https://nvidia.github.io/nvidia-container-runtime/gpgkey | apt-key add -
      distribution=$(lsb_release -c -s; echo $ID$VERSION_ID)
      curl -s -L https://nvidia.github.io/nvidia-container-runtime/$distribution/nvidia-container-
      runtime.list | tee /etc/apt/sources.list.d/nvidia-container-runtime.list
      apt update
      apt install -y nvidia-container-runtime
    fi

    # Restart Docker

    systemctl daemon-reload
    systemctl restart docker

    systemctl start aziot-edge
    if [ $(lspci | grep NVIDIA | wc -l) -gt 0 ]; then
      reboot
    fi
  ) &
write_files:
  - path: /etc/systemd/system/docker.service.d/override.conf
    permissions: "0644"
    content: |
      [Service]
      ExecStart=
      ExecStart=/usr/bin/dockerd --host=fd:// --add-runtime=nvidia=/usr/bin/nvidia-container-runtime --log-
      driver local

```

Deploy IoT Edge runtime

Deploying the IoT Edge runtime is part of VM creation, using the *cloud-init* script mentioned above.

Here are the high-level steps to deploy the VM and IoT Edge runtime:

1. Acquire the Ubuntu VM image from Azure Marketplace. For detailed steps, follow the instructions in [Use Azure Marketplace image to create VM image for your Azure Stack Edge](#).

- a. In the [Azure portal](#), go to Azure Marketplace.

- b. Connect to the Azure Cloud Shell or a client with Azure CLI installed. For detailed steps, see [Quickstart for Bash in Azure Cloud Shell](#).

NOTE

Closing the shell session will delete all variables created during the shell session. Reopening the session will require recreating the variables.

- c. Run the following command to set the subscription.

```
az account set --subscription <subscription id>
```

2. Use steps in [Search for Azure Marketplace images](#) to search the Azure Marketplace for an Ubuntu 20.04 LTS image.

Example of an Ubuntu 20.04 LTS image:

```
$urn = Canonical:0001-com-ubuntu-server-focal:20_04-lts:20.04.202007160
```

3. Create a new managed disk from the Marketplace image. For detailed steps, see [Use Azure Marketplace image to create VM image for your Azure Stack Edge](#).

4. Export a VHD from the managed disk to an Azure Storage account. For detailed steps, see [Export a VHD from the managed disk to Azure Storage](#).

5. Follow these steps to create an Ubuntu VM using the VM image.

- a. Specify the *cloud-init* script on the **Advanced** tab. To create a VM, see [Deploy GPU VM via Azure portal](#) or [Deploy VM via Azure portal](#).

The screenshot shows the 'Add a virtual machine' wizard in the Microsoft Azure portal. The 'Advanced' tab is selected. In the 'Custom data and cloud init' section, a red box highlights the 'Custom data' input field. Inside the field, a cloud-init script is shown:

```
#cloud-config
runcmd:
- dcs=<device connection string>
- |
  set -x
(
```

A tooltip below the input field states: 'Custom data on the selected image will be processed by cloud-init. [Learn more about custom data and cloud init](#)'.

At the bottom, there are 'Review + create', 'Previous', and 'Next: Review + create' buttons.

- b. Specify the appropriate device connection strings in the *cloud-init* to connect to the IoT Hub or DPS device. For detailed steps, see [Provision with symmetric keys](#) or [Provision with IoT Hub DPS](#).

The screenshot shows the 'Custom data and cloud init' configuration screen. A red box highlights the '- dcs=<device connection string>' line in the 'runcmd' section of the cloud-init script.

If you didn't specify the *cloud-init* during VM creation, you'll have to manually deploy the IoT Edge runtime after the VM is created:

1. Connect to the VM via SSH.
2. Install the container engine on the VM. For detailed steps, see [Create and provision an IoT Edge device on Linux using symmetric keys](#) or [Quickstart - Set up IoT Hub DPS with the Azure portal](#).

Verify the IoT Edge runtime

Use these steps to verify that your IoT Edge runtime is running.

1. Go to IoT Hub resource in the Azure portal.
2. Select the IoT Edge device.
3. Verify that the IoT Edge runtime is running.

Home > All resources > ase-wonASE-IOHub

myiotedgegedevice

ase-wonASE-IOHub

Save Set modules Manage child devices Troubleshoot Device twin Manage keys Refresh

Primary Connection String eye copy

Secondary Connection String eye copy

IoT Edge Runtime Response eye copy

417 -- The device's deployment configuration is not set

Enable connection to IoT Hub eye

Enable
 Disable

Parent device eye
No parent device gear

Distributed Tracing (preview) eye
Learn more Not configured gear

Modules IoT Edge hub connections Deployments and Configurations

Name	Type	Specified in Deployment	Reported by ...	Runti...	Exit C...
\$edgeAgent	IoT Edge System Module	<input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes	running	0
\$edgeHub	Module Identity	NA	NA	NA	NA

To troubleshoot your IoT Edge device configuration, see [Troubleshoot your IoT Edge device](#).

Update the IoT Edge runtime

To update the VM, follow the instructions in [Update IoT Edge](#). To find the latest version of Azure IoT Edge, see [Azure IoT Edge releases](#).

Next steps

To deploy and run an IoT Edge module on your Ubuntu VM, see the steps in [Deploy IoT Edge modules](#).

To deploy Nvidia's DeepStream module, see [Deploy the Nvidia DeepStream module on Ubuntu VM on Azure Stack Edge Pro with GPU](#).

To deploy NVIDIA DIGITS, see [Enable a GPU in a prefabricated NVIDIA module](#).

Deploy the Nvidia DeepStream module on Ubuntu VM on Azure Stack Edge Pro with GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

This article walks you through deploying Nvidia's DeepStream module on an Ubuntu VM running on your Azure Stack Edge device. The DeepStream module is supported only on GPU devices.

Prerequisites

Before you begin, make sure you have:

- Deployed an IoT Edge runtime on a GPU VM running on an Azure Stack Edge device. For detailed steps, see [Deploy IoT Edge on an Ubuntu VM on Azure Stack Edge](#).

Get module from IoT Edge Module Marketplace

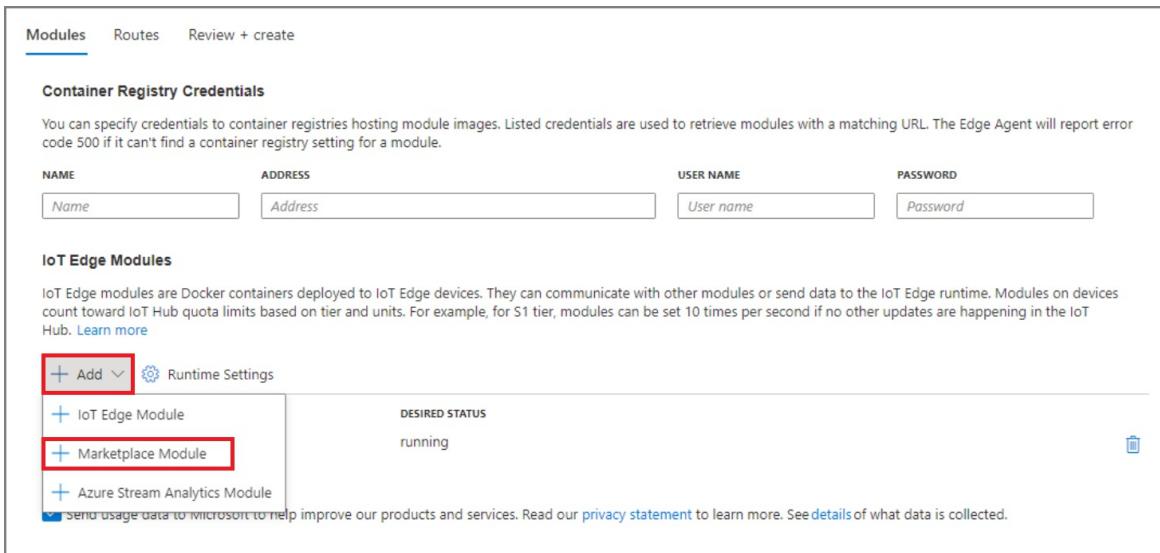
1. In the [Azure portal](#), go to **Device management > IoT Edge**.
2. Select the IoT Hub device that you configured while deploying the IoT Edge runtime.

The screenshot shows the Azure portal interface for managing IoT Edge devices. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Devices' section. The main area is titled 'ase-wonASE-IOTHub | IoT Edge'. On the left, there's a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Events', 'Pricing and scale', 'Device management', 'Devices' (which is highlighted with a red box), 'IoT Edge' (which is also highlighted with a red box), and 'Configurations'. The main content area is titled 'IoT Edge Devices' and contains a sub-section 'IoT Edge Deployments'. It has a 'Device name' input field with 'enter device ID' placeholder text and a 'Find devices' button. Below is a table with columns: Device ID, Runtime Response, Module Count, Connected Client Count, and Deployment Count. Two rows are listed: 'ubuntu' and 'winger'. The 'winger' row is highlighted with a red box. The 'ubuntu' row shows '406 -- The device is offline or not...' under 'Runtime Response'.

3. Select **Set modules**.

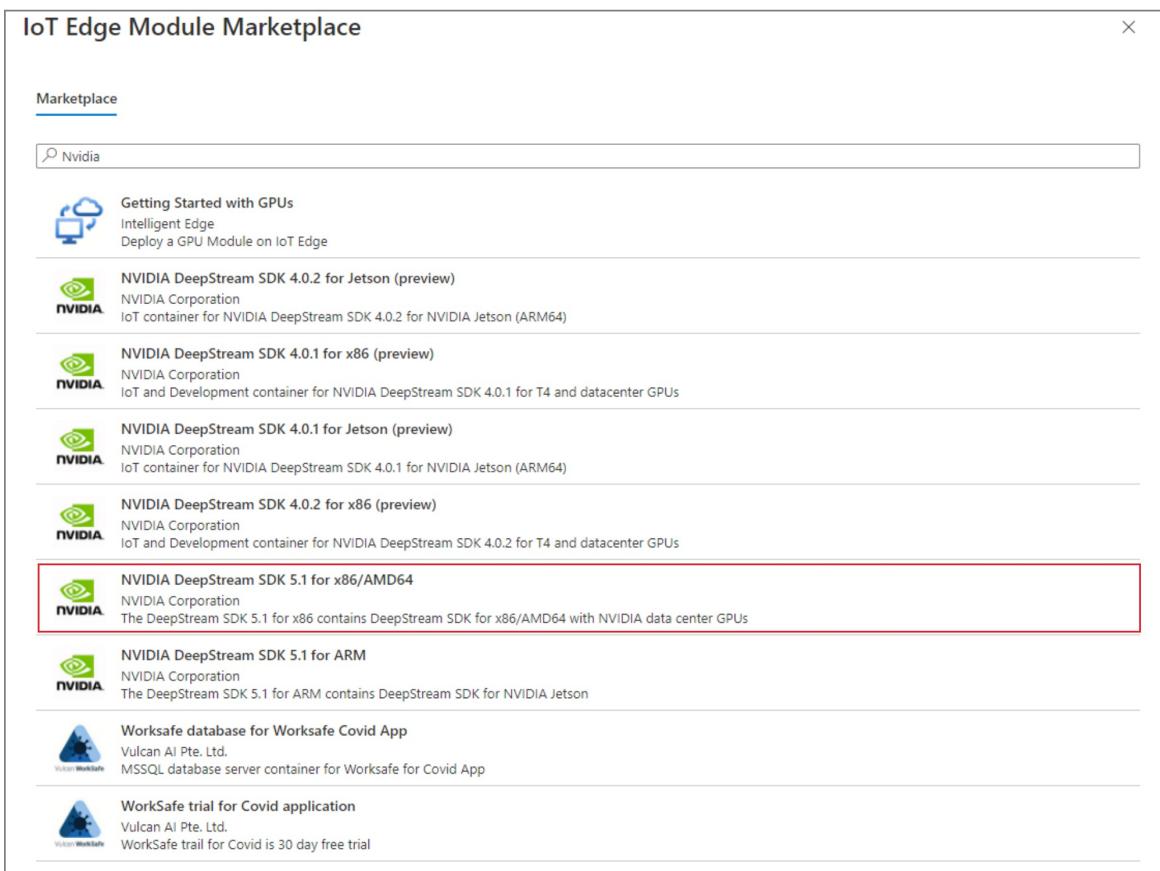
The screenshot shows the 'Set modules' configuration page for the 'iotedgegpu' device. The top navigation bar includes 'Save', 'Set modules' (which is highlighted with a red box), 'Manage child devices', 'Troubleshoot', 'Device twin', 'Manage keys', and 'Refresh'. The main form fields include 'Device ID' (set to 'iotedgegpu'), 'Primary Key' (redacted), 'Secondary Key' (redacted), 'Primary Connection String' (redacted), 'Secondary Connection String' (redacted), 'IoT Edge Runtime Response' (set to '200 - OK'), 'Enable connection to IoT Hub' (radio button set to 'Enable'), 'Parent device' (set to 'No parent device'), and 'Distributed Tracing (preview)' (set to 'Not configured'). At the bottom, there are tabs for 'Modules', 'IoT Edge hub connections', and 'Deployments and Configurations'. The 'Modules' tab is active, showing a table with columns: Name, Type, Specified in Deployment, Reported by Device, Runtime Status, and Exit Code. Two entries are listed: 'SedgeAgent' (Type: IoT Edge System Module, Status: running, Exit Code: 0) and 'SedgeHub' (Type: IoT Edge System Module, Status: running, Exit Code: 0).

4. Select Add > Marketplace Module.



The screenshot shows the 'IoT Edge Modules' configuration page. At the top, there are tabs for 'Modules', 'Routes', and 'Review + create'. Below this, a section titled 'Container Registry Credentials' contains fields for 'NAME', 'ADDRESS', 'USER NAME', and 'PASSWORD'. A note states: 'You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.' Below this, a section titled 'IoT Edge Modules' lists three modules: 'IoT Edge Module', 'Marketplace Module' (which is selected and highlighted with a red box), and 'Azure Stream Analytics Module'. The 'Marketplace Module' row shows 'DESIRED STATUS' as 'running'. At the bottom, there is a note about sending usage data to Microsoft and links to the privacy statement and data collection details.

5. Search for NVIDIA DeepStream SDK 5.1 for x86/AMD64 and then select it.



The screenshot shows the 'IoT Edge Module Marketplace' search results for 'Nvidia'. The 'Marketplace' tab is selected. A search bar contains the text 'Nvidia'. The results list several items:

- Getting Started with GPUs
- NVIDIA DeepStream SDK 4.0.2 for Jetson (preview)
- NVIDIA DeepStream SDK 4.0.1 for x86 (preview)
- NVIDIA DeepStream SDK 4.0.1 for Jetson (preview)
- NVIDIA DeepStream SDK 4.0.2 for x86 (preview)
- NVIDIA DeepStream SDK 5.1 for x86/AMD64 (selected)
- NVIDIA DeepStream SDK 5.1 for ARM
- Worksafe database for Worksafe Covid App
- WorkSafe trial for Covid application

6. Select Review + Create, and then select Create module.

Verify module runtime status

1. Verify that the module is running.

IoT Edge hub connections					
Name	Type	Specified in Deployment	Reported by Device	Runtime Status	Exit Code
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
SimulatedTemperatureSensor	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
NVIDIADeepStreamSDK	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

2. Verify that the module provides the following output in the troubleshooting page of the IoT Edge device on IoT Hub:

Troubleshoot ...

ase-chawonASEGPU-IOTHub

Restart NVIDIADeepStreamSDK Refresh Download

NVIDIADeepStreamSDK Time range: Since 15 minutes Find: Not specified

```
"version": "4.0",
"id": 1382,
"@timestamp": "2022-05-10T23:45:38.321Z",
"sensorid": "HWY_20_AND_LOCUST_EBA_4_11_2018_4_59_59_508_AM_UTC-07_00",
"objects": [
  "1264|1043.2|472.5|1120|510|Vehicle#||||||0",
  "1268|1212.8|476.25|1308.8|513.75|Vehicle#||||||0",
  "1248|685.6|476.25|636.8|521.25|Vehicle#||||||0",
  "1253|1520|495|1657.6|536.25|Vehicle#||||||0",
  "1265|1632|498.75|1865.6|585|Vehicle#||||||0",
  "1180|630.4|483.75|774.4|596.25|Vehicle#||||||0",
  "1251|1276.8|491.25|1571.2|622.5|Vehicle#||||||0",
  "1155|406.4|480|428.8|547.5|Person",
  "1121|441.6|483.75|464|551.25|Person"
]
}
Message sent: {
  "version": "4.0",
  "id": 1377,
  "@timestamp": "2022-05-10T23:45:38.496Z",
  "sensorid": "HWY_20_AND_LOCUST_WBA_4_11_2018_4_59_59_379_AM_UTC-07_00",
  "objects": [
    "1247|646.4|457.5|684.8|480|Vehicle#||||||0",
    "1249|1024|468.75|1056|491.25|Vehicle#||||||0",
    "1248|1072|472.5|1142.4|506.25|Vehicle#||||||0",
    "1221|582.4|472.5|630.4|513.75|Vehicle#||||||0",
    "1245|1283.2|483.75|1382.4|525|Vehicle#||||||0",
    "1235|1574.4|498.75|1715.2|543.75|Vehicle#||||||0",
    "1166|624|483.75|755.2|588.75|Vehicle#||||||0",
    "1233|1129.6|483.75|1360|588.75|Vehicle#||||||0",
    "1250|1817.6|510|1913.6|585|Vehicle#||||||0",
    "1113|441.6|476.25|464|551.25|Person",
    "1154|406.4|476.25|428.8|547.5|Person"
  ]
}
Message sent: {
  "version": "4.0",
  "id": 1381,
  "@timestamp": "2022-05-10T23:45:38.398Z",
  "sensorid": "HWY_20_AND_LOCUST_EBA_4_11_2018_4_59_59_508_AM_UTC-07_00",
  "objects": [
    "1247|646.4|457.5|694.4|483.75|Vehicle#||||||0",
    "1253|1011.2|468.75|1046.4|487.5|Vehicle#||||||0",
    "1248|1049.6|472.5|1123.2|506.25|Vehicle#||||||0",
    "1254|553.6|472.5|582.4|495|Vehicle#||||||0",
    "1221|585.6|476.25|633.6|521.25|Vehicle#||||||0",
    "1235|1529.6|4951|673.6|540|Vehicle#||||||0".
  ]
}
Showing last 1500 line(s)
```

After a certain period of time, the module runtime will complete and quit, causing the module status to return an error. This error condition is expected behavior.

IoT Edge hub connections					
Name	Type	Specified in Deployment	Reported by Device	Runtime Status	Exit Code
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
SimulatedTemperatureSensor	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0
NVIDIADeepStreamSDK	IoT Edge Custom Module	✓ Yes	✓ Yes	● Error	0

Next steps

[Troubleshoot IoT Edge issues.](#)

Configure and run a module on GPU on Azure Stack Edge Pro device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

Your Azure Stack Edge Pro device contains one or more Graphics Processing Unit (GPU). GPUs are a popular choice for AI computations as they offer parallel processing capabilities and are faster at image rendering than Central Processing Units (CPUs). For more information on the GPU contained in your Azure Stack Edge Pro device, go to [Azure Stack Edge Pro device technical specifications](#).

This article describes how to configure and run a module on the GPU on your Azure Stack Edge Pro device. In this article, you will use a publicly available container module **Digits** written for Nvidia T4 GPUs. This procedure can be used to configure any other modules published by Nvidia for these GPUs.

Prerequisites

Before you begin, make sure that:

1. You've access to a GPU enabled 1-node Azure Stack Edge Pro device. This device is activated with a resource in Azure.

Configure module to use GPU

To configure a module to use the GPU on your Azure Stack Edge Pro device to run a module, follow these steps.

1. In the Azure portal, go to the resource associated with your device.
2. In **Overview**, select **IoT Edge**.

The screenshot shows the Azure portal interface for managing an Azure Stack Edge Pro device named "myasetest". The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring (Device events, Alerts, Metrics). The main content area is titled "Overview" and displays the message "Your device is running fine!". It includes sections for "Deployed edge services" (No deployed services) and "Edge services". Under "Edge services", there are three cards: "Virtual machines" (New), "IoT Edge" (selected and highlighted with a red border), and "Cloud storage gateway". Each card has a "How to get started?" link.

3. In **Enable IoT Edge service**, select **Add**.

4. In **Create IoT Edge service**, enter settings for your IoT Hub resource:

FIELD	VALUE
Subscription	Subscription used by the Azure Stack Edge resource.
Resource group	Resource group used by the Azure Stack Edge resource.
IoT Hub	Choose from Create new or Use existing . By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.
Name	If you don't want to use the default name provided for a new IoT Hub resource, enter a different name.

When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Create IoT Edge service

Azure Stack Edge Pro - 1 GPU

X

[Basics](#) [Review + Create](#)

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription * ⓘ

Edge Gateway Test

Resource group * ⓘ

myaserg

IoT Hub * ⓘ

 Create new Use existing

myasetest-iothub

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

IoT Edge device: myasetest-edge

IoT Gateway device: myasetest-storagegateway

Only Linux container image types are supported.

[Review + Create](#)[Previous](#)[Next: Review + Create](#)

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

Home > myasetest >

IoT Edge | Overview

Azure Stack Edge Pro - 1 GPU

[Search \(Ctrl+\)](#) << [Add module](#) [Add trigger](#) [Refresh configuration](#) [Remove](#) | [Refresh](#)

[Overview](#) **IoT Edge service is running fine!** Start processing the data using IoT Edge modules. [Learn more](#)

[Modules](#) [Triggers](#) [Properties](#)

Modules

IoT Edge modules are containers that run Azure services, third-party services, or your own code.
To read data from Edge local shares for processing and uploading it to cloud, add a Module. If multiple containers are deployed, which are chained together for pipeline processing, go to [Azure IoT Hub](#).

[Add module](#)

Triggers

Add triggers to start processing at a repeated interval or on file events such as creation of a file, modification of a file on a share.

[Add trigger](#)

Edge Shares
For container to store or transfer files and folders to Azure Storage account (other than temp data). create a share.

[Configure Shares](#)

Edge Storage account
For container to transfer unstructured data like binary, audio, or video streaming data to Azure Storage account, create a storage account.

[Configure Storage account](#)

Network bandwidth usage
If containers uploads data to cloud using shares configure network bandwidth usage across multiple time-of-day schedules.

[Configure Bandwidth schedule](#)

5. To confirm the Edge compute role has been configured, select **Properties**.

IoT Hub	myasetest-iohub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

6. In **Properties**, select the link for **IoT Edge device**.

Device ID	Runtime Response	IoT Edge Module Count	Connected Client Count	Deployment Count
myasegpu1-edge	417 - The device's deploy...	1	0	0

In the right pane, you see the IoT Edge device associated with your Azure Stack Edge Pro device. This device corresponds to the IoT Edge device you created when creating the IoT Hub resource.

7. Select this IoT Edge device.

<input checked="" type="checkbox"/> Device ID	Runtime Response	IoT Edge Module Count	Connected Client Count	Deployment Count
<input checked="" type="checkbox"/> myasegpu1-edge	417 - The device's deploy...	1	0	0

8. Select Set modules.

Home > All resources > myasegpuiothub1 | IoT Edge > myasegpu1-edge

myasegpu1-edge
myasegpuiothub1

Save **Set Modules** Manage Child Devices Device Twin Manage keys Refresh

Device ID: myasegpu1-edge
Primary Key:
Secondary Key:
Primary Connection String:
Secondary Connection String:
IoT Edge Runtime Response: 417 -- The device's deployment configuration is not set
Enable connection to IoT Hub: Enable Disable

Modules IoT Edge Hub connections Deployments

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CODE
\$edgeAgent	IoT Edge System Module	<input type="radio"/> No	<input checked="" type="radio"/> Yes	running	0
\$edgeHub	Module Identity	NA	NA	NA	NA

9. Select + Add and then select + IoT Edge module.

Home > All resources > myasegpuiothub1 | IoT Edge > myasegpu1-edge > Set modules on device: myasegpu1-edge

Set modules on device: myasegpu1-edge
myasegpuiothub1

Modules Routes Review + create

Container Registry Credentials
You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
Name	Address	User name	Password

IoT Edge Modules
An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub.
[Learn more](#)

+ Add **Runtime Settings**

NAME **RED STATUS**

- + IoT Edge Module
- + Marketplace Module
- + Azure Stream Analytics Module

Review + create < Previous Next: Routes >

10. In the Add IoT Edge Module tab:

- Provide the **Image URI**. You will use the publicly available Nvidia module **Digits** here.
- Set **Restart policy** to **always**.

c. Set Desired state to running.

Set modules on device: myasegpu1-edge

IoT Edge Module Name *

Module name

Image URI *

nvidia/digits:6.0

Restart Policy

always

Desired Status

running

Add Cancel

11. In the **Environment variables** tab, provide the Name of the variable and the corresponding value.

- To have the current module use one GPU on this device, use the NVIDIA_VISIBLE_DEVICES.
- Set the value to 0 or 1. A value of 0 or 1 ensures that at least one GPU is used by the device for this module. When you set the value to 0, 1, that implies that both the GPUs on your device are being used by this module.

Set modules on device: myasegpu1-edge

IoT Edge Module Name *

Module name

Environment variables

NAME VALUE

NVIDIA_VISIBLE_DEVICES 0

Variable name Variable value

Add Cancel

For more information on environment variables that you can use with the Nvidia GPU, go to

nVidia container runtime.

NOTE

A module can use one, both or no GPUs.

12. Enter a name for your module. At this point you can choose to provide container create option and modify module twin settings or if done, select **Add**.

The screenshot shows the Azure portal interface for managing IoT Edge modules. The top navigation bar includes 'Home', 'All resources', 'myasegpuiohub1 | IoT Edge', 'myasegpu1-edge', and 'Set modules on device: myasegpu1-edge'. The main title is 'Set modules on device: myasegpu1-edge'. A sub-section titled 'Add IoT Edge Module' is displayed. The 'NAME' field contains 'digits1'. Under 'Environment Variables', there is a row with 'NAME' 'NVIDIA_VISIBLE_DEVICES' and 'VALUE' '0'. At the bottom, there are 'Add' and 'Cancel' buttons, with 'Add' being highlighted by a red box.

13. Make sure that the module is running and select **Review + Create**.

Home > All resources > myasegpuiohub1 | IoT Edge > myasegpu1-edge > Set modules on device: myasegpu1-edge

Set modules on device: myasegpu1-edge

myasegpuiohub1

Modules Routes Review + create

Container Registry Credentials

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error code 500 if it can't find a container registry setting for a module.

NAME	ADDRESS	USER NAME	PASSWORD
Name	Address	User name	Password

IoT Edge Modules

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub.

[Learn more](#)

+ Add  Runtime Settings

NAME	DESIRED STATUS
digits1	running



[Review + create](#) < Previous [Next: Routes >](#)



14. In the **Review + Create** tab, the deployment options that you selected are displayed. Review the options and select **Create**.

Home > All resources > myasegpuiothub1 | IoT Edge > myasegpu1-edge > Set modules on device: myasegpu1-edge

Set modules on device: myasegpu1-edge

myasegpuiothub1

Modules Routes Review + create

✓ Validation passed.

Deployment

The text box below displays the deployment to be submitted.

```

1  {
2      "modulesContent": {
3          "$edgeAgent": {
4              "properties.desired": {
5                  "modules": {
6                      "digits1": {
7                          "settings": {
8                              "image": "nvidia/digits:6.0",
9                              "createOptions": ""
10                         },
11                         "type": "docker",
12                         "env": {
13                             "NVIDIA_VISIBLE_DEVICES": {
14                                 "value": "0"
15                             }
16                         },
17                         "status": "running",
18                         "restartPolicy": "always",
19                         "version": "1.0"
20                     }
21                 }
22             }
23         }
24     }

```

The configuration for the 'digits1' module is highlighted with a red box.

Create < Previous Next >

15. Make a note of the **runtime status** of the module.

Home > All resources > myasegpuiothub1 | IoT Edge > myasegpu1-edge

myasegpu1-edge

myasegpuiothub1

Save Set Modules Manage Child Devices Device Twin Manage keys Refresh

Device ID	myasegpu1-edge	Edit
Primary Key	View Edit
Secondary Key	View Edit
Primary Connection String	View Edit
Secondary Connection String	View Edit
IoT Edge Runtime Response	417 -- The device's deployment configuration is not set	Edit
Enable connection to IoT Hub	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

Modules IoT Edge Hub connections Deployments

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTI...	EXIT CO...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✗ No	--	--
digits1	IoT Edge Custom Module	✓ Yes	✗ No	--	--

It takes a couple minutes for the module to be deployed. Select **Refresh** and you should see the runtime status update to **running**.

The screenshot shows the Azure IoT Edge device configuration interface for the device **myasegpu1-edge**. The top navigation bar includes links for Home, All resources, myasegpu1othub1 | IoT Edge, and myasegpu1-edge. The main content area displays various configuration settings and a list of modules.

Configuration Settings:

- Device ID: myasegpu1-edge
- Primary Key: (redacted)
- Secondary Key: (redacted)
- Primary Connection String: (redacted)
- Secondary Connection String: (redacted)
- IoT Edge Runtime Response: 200 -- OK
- Enable connection to IoT Hub: Enable Disable

Modules Tab:

The **Modules** tab is selected, showing the following table:

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CODE
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
digits1	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

Next steps

- Learn more about [Environment variables that you can use with the Nvidia GPU](#).

Deploy a GPU enabled IoT module on Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R

This article describes how to deploy a GPU enabled IoT Edge module on your Azure Stack Edge Pro GPU device.

In this article, you learn how to:

- Prepare Azure Stack Edge Pro to run a GPU module.
- Download and install sample code from a Git repository.
- Build the solution and generate a deployment manifest.
- Deploy the solution to Azure Stack Edge Pro device.
- Monitor the module output.

About sample module

The GPU sample module in this article includes PyTorch and TensorFlow benchmarking sample code for CPU against GPU.

Prerequisites

Before you begin, make sure you have:

- You've access to a GPU enabled 1-node Azure Stack Edge Pro device. This device is activated with a resource in Azure. See [Activate the device](#).
- You've configured compute on this device. Follow the steps in [Tutorial: Configure compute on your Azure Stack Edge Pro device](#).
- An Azure Container Registry (ACR). Go to the **Access keys** blade and make a note of the ACR login server, username, and password. For more information, go to [Quickstart: Create a private container registry using the Azure portal](#).
- The following development resources on a Windows client:
 - [Azure CLI 2.0 or later](#)
 - Docker CE. You may have to create an account to download and install the software.
 - [Visual Studio Code](#)
 - [Azure IoT Edge extension for Visual Studio Code](#).
 - [Python extension for Visual Studio Code](#)
 - [Python 3](#)
 - Pip for installing Python packages (typically included with your Python installation)

Get the sample code

1. Go to the [Azure Intelligent Edge Patterns in Azure samples](#). Clone or download the zip file for code.

Azure-Samples / azure-intelligent-edge-patterns

Code Issues Pull requests Actions Projects Wiki Security Insights

master

GusPoland Merge pull request #141 from Azure...
 .github Initial commit
 AKSe-on-AzStackHub Update README.m...
 GpuReferenceModules Merge branch 'mas...
 Research Merge pull request

Clone with HTTPS Use SSH
<https://github.com/Azure-Samples/azure>

About Samples for Intelligent Edge Patterns
 Readme MIT License

Releases 74 Azure Intelligent Ed... Latest

Download ZIP

Extract the files from the zip. You can also clone the samples.

```
git clone https://github.com/Azure-Samples/azure-intelligent-edge-patterns.git
```

Build and deploy module

1. Open the **GpuReferenceModules** folder in Visual Studio Code.

Open Folder

git > azure-intelligent-edge-patterns-master

Organize New folder

Name	Date modified	Type
.github	7/23/2020 9:56 AM	File folder
AKSe-on-AzStackHub	7/23/2020 9:56 AM	File folder
edge-ai-void-detection	7/23/2020 9:56 AM	File folder
edge-training	7/23/2020 9:56 AM	File folder
factory-ai-vision	7/23/2020 9:56 AM	File folder
fhir-server-edge	7/23/2020 9:56 AM	File folder
footfall-analysis	7/23/2020 9:57 AM	File folder
GpuReferenceModules	7/23/2020 2:09 PM	File folder
hybrid-devops	7/23/2020 9:57 AM	File folder
hybrid-relay	7/23/2020 9:57 AM	File folder
migration-patterns-and-practices	7/23/2020 9:57 AM	File folder
mongodb-hadr	7/23/2020 9:57 AM	File folder

OSDisk (C:)

Folder: GpuReferenceModules

Select Folder Cancel

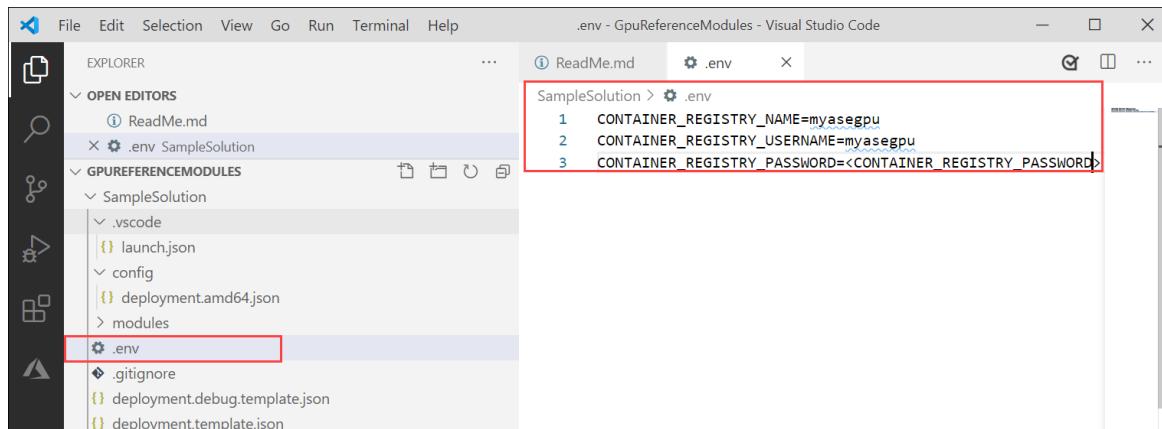
2. Open the *deployment.template.json* and identify the parameters it references for the container registry. In the following file, CONTAINER_REGISTRY_USERNAME, CONTAINER_REGISTRY_PASSWORD, and CONTAINER_REGISTRY_NAME are used.

```
{
"$schema-template": "2.0.0",
"modulesContent": {
"$edgeAgent": {
"properties.desired": {
"schemaVersion": "1.0",
"runtime": {
"type": "docker",
"settings": {
"minDockerVersion": "v1.25",
"loggingOptions": "",
"registryCredentials": {
"${CONTAINER_REGISTRY_NAME}": {
"username": "$CONTAINER_REGISTRY_USERNAME",
"password": "$CONTAINER_REGISTRY_PASSWORD",
"address": "${CONTAINER_REGISTRY_NAME}.azurecr.io"
}
}
}
}
},
}
},
},
```

3. Create a new file. Fill out the values for your container registry parameters (use the ones identified in the earlier step) as follows:

```
CONTAINER_REGISTRY_NAME=<YourContainerRegistryName>
CONTAINER_REGISTRY_USERNAME=<YourContainerRegistryUserName>
CONTAINER_REGISTRY_PASSWORD=<YourContainerRegistryPassword>
```

A sample `.env` file is shown below:



4. Save the file as `.env` in the **SampleSolution** folder.
5. To sign into Docker, enter the following command in the Visual Studio Code integrated terminal.

```
docker login -u <CONTAINER_REGISTRY_USERNAME> -p <CONTAINER_REGISTRY_PASSWORD>
<CONTAINER_REGISTRY_NAME>
```

Go to the **Access keys** section of your container registry in the Azure portal. Copy and use the registry name, password, and login server.

Home >
myasegpu | Access keys
Container registry

Search (Ctrl+ /) <<

Overview
Activity log
Access control (IAM)
Tags
Quick start
Events

Settings

Access keys (highlighted)
Encryption
Identity
Networking
Security
Locks
Export template

Services

Registry name: myasegpu
Login server: myasegpu.azurecr.io
Admin user: (Enable) (Disable)
Username: myasegpu
Name Password
password: <Password> (copy) (refresh)
password2: <Password> (copy) (refresh)

After the credentials are supplied, the sign in succeeds.

.env - GpuReferenceModules - Visual Studio Code

File Edit Selection View Go Run Terminal Help

EXPLORER OPEN EDITORS README.md .env deployment.template.json

GPUREFERENCEMODULES SampleSolution .vscode config deployment.debug.template.json deployment.template.json

OUTLINE

AZURE IOT HUB myasegpuioth Devices myasegpures1-edge myasegpures1-storagegaga... Endpoints

TERMINAL

```
alkohli@alkohli-slp2 MINGW64 /c/git/azure-intelligent-edge-patterns-master/GpuReferenceModules
$ docker login -u myasegpu -p Bh088a/dKLN1B8uO2oqUunxnafS8gdus myasegpu.azurecr.io
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
Login Succeeded
```

PROBLEMS 4 OUTPUT DEBUG CONSOLE 1: bash

Ln 3, Col 49 Spaces: 4 UTF-8 CRLF Plain Text

- Push your image to your Azure container registry. In the VS Code Explorer, select and right-click the **deployment.template.json** file and then select **Build and Push IoT Edge solution**.

The screenshot shows the Visual Studio Code interface with the following details:

- File Explorer:** On the left, showing files like `ReadMe.md`, `.env`, and `deployment.template.json`.
- Context Menu:** A right-click context menu is open over `deployment.template.json`, listing options such as "Validate this workspace folder", "Open to the Side", "Reveal in File Explorer", "Open in Integrated Terminal", "Select for Compare", "Open Timeline", "Cut", "Copy", "Copy Path", "Copy Relative Path", "Rename", "Delete", and "Build and Push IoT Edge Solution". The "Build and Push IoT Edge Solution" option is highlighted with a red box.
- Code Editor:** The main editor area displays the JSON content of `deployment.template.json`, which includes schema validation errors (red squiggly lines) and some placeholder values.
- Terminal:** At the bottom, the terminal shows command-line output related to building an IoT Edge solution.

If Python and Python extension are not installed, these will be installed when you build and push the solution. However, this would result in longer build times.

Once this step is complete, you see the module in your container registry.

The screenshot shows the Azure Container Registry interface for the user 'myasegpu'. The top navigation bar includes 'Home >' and the user's name 'myasegpu | Repositories'. Below the navigation is a 'Container registry' section with a cloud icon. On the left, a sidebar lists 'Locks', 'Export template', 'Services' (with 'Repositories' highlighted), 'Webhooks', 'Replications', and 'Tasks'. The main content area has a search bar ('Search (Ctrl+ /)') and a refresh button. A secondary search bar ('Search to filter repositories ...') is also present. The 'Repositories' list contains one item, 'gpumodule', which is highlighted with a red box. An ellipsis button is at the end of the repository list.

- To create a deployment manifest, right-click the `deployment.template.json` and then select **Generate IoT Edge Deployment Manifest**.

The notification informs you the path at which the deployment manifest was generated. The manifest is the `deployment.amd64.json` file generated in the `config` folder.

- Select the `deployment.amd64.json` file in `config` folder and then choose **Create Deployment for Single Device**. Do not use the `deployment.template.json` file.

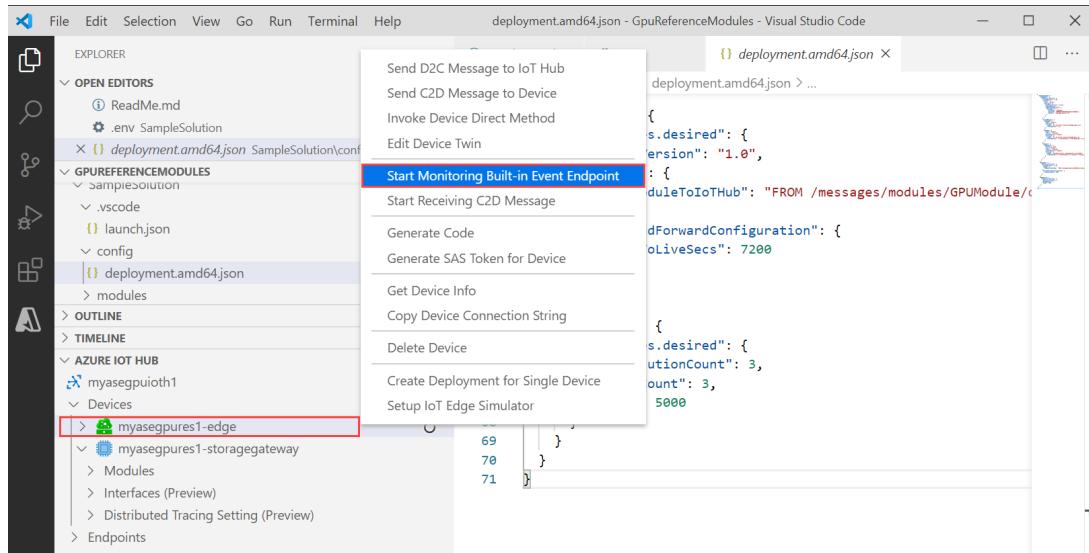
In the **Output** window, you should see a message that deployment succeeded.

```
[Edge] Start deployment to device [myasegpures1-edge]
[Edge] Deployment succeeded.
```

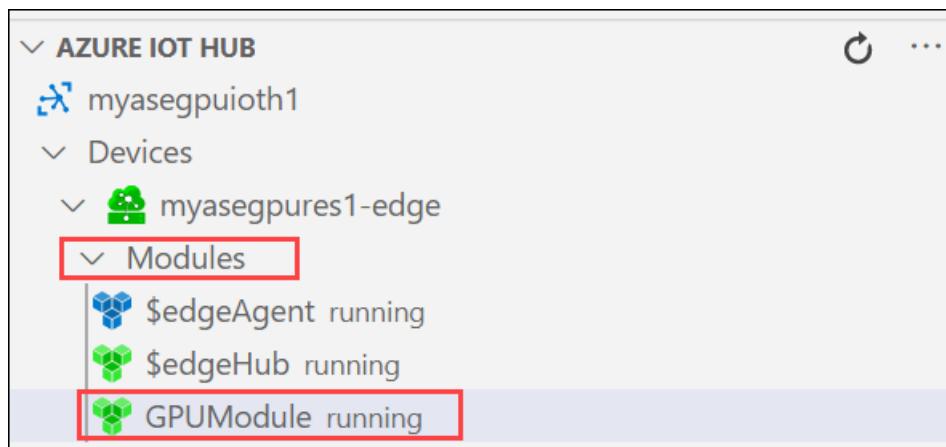
Monitor the module

1. In the VS Code command palette, run **Azure IoT Hub: Select IoT Hub**.
2. Choose the subscription and IoT hub that contain the IoT Edge device that you want to configure. In this case, select the subscription used to deploy the Azure Stack Edge Pro device, and select the IoT Edge device created for your Azure Stack Edge Pro device. This occurs when you configure compute via the Azure portal in the earlier steps.
3. In the VS Code explorer, expand the Azure IoT Hub section. Under **Devices**, you should see the IoT Edge device corresponding to your Azure Stack Edge Pro device.

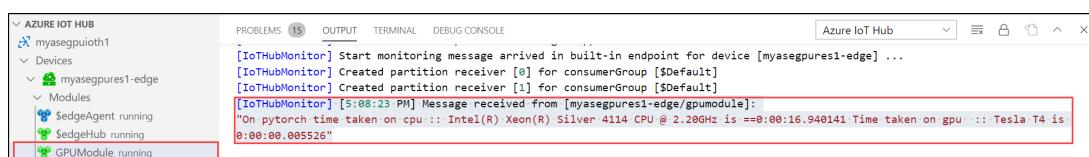
- a. Select that device, right-click and select **Start Monitoring Built-in Event Endpoint**.



- b. Go to **Devices > Modules** and you should see your **GPU module** running.



- c. The VS Code terminal should also show the IoT Hub events as the monitoring output for your Azure Stack Edge Pro device.



You can see that the time taken to execute the same set of operations (5000 iterations of shape transformation) by GPU is lot lesser than it is for CPU.

Next Steps

- Learn more about how to [Configure GPU to use a module](#).

Deploy a GPU enabled IoT module from Azure Marketplace on Azure Stack Edge Pro GPU device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

This article describes how to deploy a Graphics Processing Unit (GPU) enabled IoT Edge module from Azure Marketplace on your Azure Stack Edge Pro device.

In this article, you learn how to:

- Prepare Azure Stack Edge Pro to run a GPU module.
- Download and deploy GPU enabled IoT module from Azure Marketplace.
- Monitor the module output.

About sample module

The GPU sample module in this article includes PyTorch and TensorFlow benchmarking sample code for CPU against GPU.

Prerequisites

Before you begin, make sure you have:

- You've access to a GPU enabled 1-node Azure Stack Edge device. This device is activated with a resource in Azure.
- You've configured compute on this device. Follow the steps in [Tutorial: Configure compute on your Azure Stack Edge device](#).
- The following development resources on a Windows client:
 - [Visual Studio Code](#)
 - [Azure IoT Edge extension for Visual Studio Code](#).

Get module from Azure Marketplace

1. Browse all [Apps in Azure Marketplace](#).

The screenshot shows the Azure Marketplace homepage. On the left, there's a sidebar with categories like 'Get Started', 'Analytics', 'AI + Machine Learning', etc. The main area has search filters for 'Trials', 'Operating System', 'Publisher', 'Pricing Model', and 'Product Type'. Below these are three featured products:

- CloudGuard IaaS - Firewall & Threat Prevention** by Check Point: 5 stars (2 reviews), Price varies, Get it now.
- CIS Microsoft Windows Server 2016 Benchmark L1** by Center For Internet Security, Inc.: 5 stars (1 review), Software plans start at \$0.02/hour, Get it now.
- FortiGate NGFW - Single VM with ARM Template** by Fortinet: 5 stars (3 reviews), Price varies, Test Drive.

2. Search for Getting started with GPUs.

The screenshot shows the Azure Marketplace search results for 'Getting started with GPUs'. The search bar contains the query. A dropdown menu appears with suggestions: 'Search all apps for Getting started with GPUs' and 'Search all consulting services for Getting started with GPUs'. Below the search bar, there's a 'Featured' section with a product card for 'Getting Started with GPUs' by Intelligent Edge.

3. Select Get it now.

The screenshot shows the product page for 'Getting Started with GPUs' by Intelligent Edge. The page includes the product title, a brief description, and a large 'GET IT NOW' button. To the left, there's a sidebar with categories and a 'Categories' section listing 'Analytics', 'Compute', 'Developer Tools', 'Internet of Things', and 'IT & Management Tools'.

4. Select Continue to acknowledge the provider's terms of use and privacy policy.

Create this app in Azure



Getting Started with GPUs

By Intelligent Edge

Software plan

Getting Started with GPUs

Details: IoT Edge module to get started with GPUs

I agree to the Microsoft Standard Contract [terms of use](#) and provider's [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate [terms](#).

Continue

5. Choose the subscription that you used to deploy your Azure Stack Edge Pro device.

Home >

Target Devices for IoT Edge Module

Microsoft

Subscription * ⓘ

AI Infra Build

⚠ An IoT Hub supporting Edge capabilities (Free or Standard SKU Tier) is required to proceed.

Create a new IoT Hub

By deploying this module, I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate terms.

Create

6. Enter the name of the IoT Hub service that you created when you configured your Azure Stack Edge Pro device. To find this IoT Hub service name, go to the Azure Stack Edge resource associated with your device in Azure portal.

- a. In the left pane menu options, go to **Edge services > IoT Edge**.

Home >

myasegpuudev Azure Stack Edge

Search (Ctrl+)

Update device Reset device password Return device Feedback Delete Refresh

View Cost JSON View

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings Locks Properties Order details

Edge services

New

Your device is running fine!

Deployed edge services

Name	Status
IoT Edge	Running

Edge services

New

Virtual machines Bring your workloads to the edge that aren't yet containerized.

How to get started?

IoT Edge Manage containerized application at edge and integrate with IoT Hub.

How to get started?

Cloud storage gateway Seamlessly send your data to Azure Storage account.

How to get started?

- b. Go to **Properties**.

- a. Make a note of the IoT Hub service that was created when you configured compute on your Azure Stack Edge Pro device.
- b. Note the name of the IoT Edge device that was created when you configured compute. You will use this name in the subsequent step.

Edge compute configuration

myasegpures1

The device is configured for compute capabilities. For example, an Azure function can be used to transform the data on an Edge local share and then move it to cloud. [Learn more](#)

IoT Hub ⓘ	myasegpuioth1.azure-devices.net
IoT Edge device ⓘ	myasegpures1-edge
IoT device ⓘ	myasegpures1-storagegateway
Platform ⓘ	Linux

7. Choose **Deploy to a device**.
8. Enter the name of the IoT Edge device or select **Find Device** to browse among the devices registered with the hub.

Select IoT Edge Device

Available IoT Edge Devices

myasegpures1-edge

Load More

Select

9. Select **Create** to continue the standard process of configuring a deployment manifest including adding other modules if desired. Details for the new module such as image URI, create options, and desired properties are predefined but can be changed.

Home >

Target Devices for IoT Edge Module

Microsoft

Subscription * ⓘ

SMS Automation

IoT Hub * ⓘ

myasegpuioth1

Deploy to a device Deploy at Scale

IoT Edge Device Name * ⓘ

myasegpures1-edge

Find Device

By deploying this module, I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate terms.

Create

10. Verify that the module is deployed in your IoT Hub in the Azure portal. Select your device, select **Set Modules** and the module should be listed in the **IoT Edge Modules** section.

Home > myasegpuioth1 | IoT Edge >

myasegpures1-edge ⌘

myasegpuioth1

Save **Set Modules** Manage Child Devices Device Twin Manage keys Refresh

Device ID ⓘ myasegpures1-edge

Primary Key ⓘ ⌚ ⌚

Secondary Key ⓘ ⌚ ⌚

Primary Connection String ⓘ ⌚ ⌚

Secondary Connection String ⓘ ⌚ ⌚

IoT Edge Runtime Response ⓘ 200 -- OK ⌚ ⌚

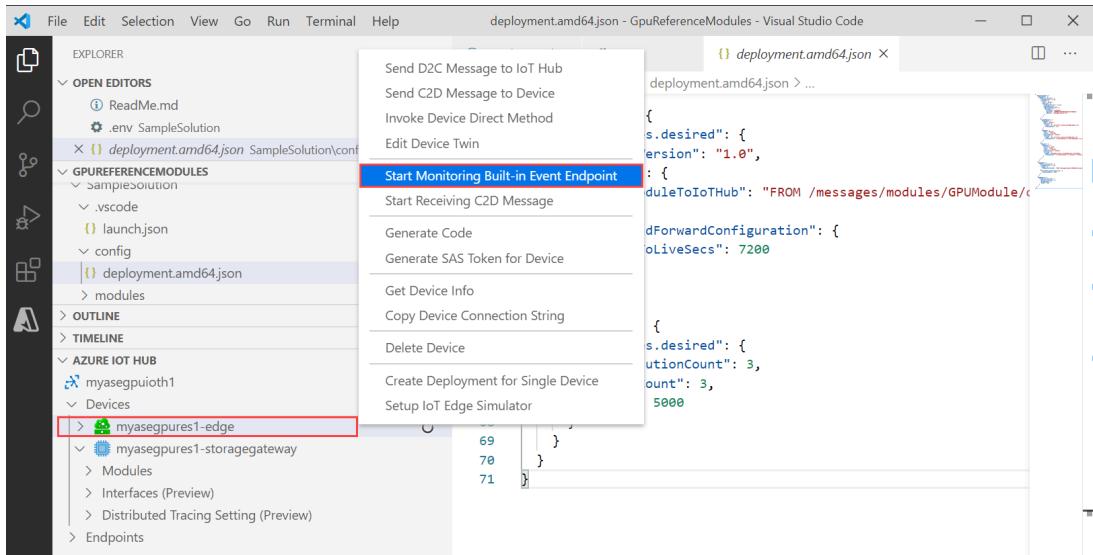
Enable connection to IoT Hub ⓘ Enable Disable

Modules IoT Edge Hub connections Deployments

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CO...
\$edgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
GettingStartedwithGPUs	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

Monitor the module

- In the VS Code command palette, run **Azure IoT Hub: Select IoT Hub**.
- Choose the subscription and IoT hub that contain the IoT Edge device that you want to configure. In this case, select the subscription used to deploy the Azure Stack Edge Pro device, and select the IoT Edge device created for your Azure Stack Edge Pro device. This occurs when you configure compute via the Azure portal in the earlier steps.
- In the VS Code explorer, expand the Azure IoT Hub section. Under **Devices**, you should see the IoT Edge device corresponding to your Azure Stack Edge Pro device.
 - Select that device, right-click and select **Start Monitoring Built-in Event Endpoint**.



- b. Go to **Devices > Modules** and you should see your **GPU module** running.
- c. The VS Code terminal should also show the IoT Hub events as the monitoring output for your Azure Stack Edge Pro device.

```
[IoTHubMonitor] Start monitoring message arrived in built-in endpoint for device [myasegpures1-edge] ...
[IoTHubMonitor] Created partition receiver [0] for consumerGroup [$Default]
[IoTHubMonitor] Created partition receiver [1] for consumerGroup [$Default]
[IoTHubMonitor] [5:08:23 PM] Message received from [myasegpures1-edge/gpumodule]:
"On pytorch time taken on cpu :: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz is ==:00:16.940141 Time taken on gpu :: Tesla T4 is
0:00:00.005526"
```

You can see that the time taken to execute the same set of operations (5000 iterations of shape transformation) by GPU is lot lesser than it is for CPU.

Next Steps

- Learn more about how to [Configure GPU to use a module](#).

Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

This article details the changes needed for a docker-based IoT Edge module that runs on Azure Stack Edge Pro FPGA so it can run on a Kubernetes-based IoT Edge platform on Azure Stack Edge Pro GPU device.

About IoT Edge implementation

The IoT Edge implementation is different on Azure Stack Edge Pro FPGA devices vs. that on Azure Stack Edge Pro GPU devices. For the GPU devices, Kubernetes is used as a hosting platform for IoT Edge. The IoT Edge on FPGA devices uses a docker-based platform. The IoT Edge docker-based application model is automatically translated to the Kubernetes native application model. However, some changes may still be needed as only a small subset of the Kubernetes application model is supported.

If you are migrating your workloads from an FPGA device to a GPU device, you will need to make changes to the existing IoT Edge modules for those to run successfully on the Kubernetes platform. You may need to specify your storage, networking, resource usage, and web proxy requirements differently.

Storage

Consider the following information when specifying storage for the IoT Edge modules.

- Storage for containers on Kubernetes is specified using volume mounts.
- Deployment on Kubernetes can't have binds for associating persistent storage or host paths.
 - For persistent storage, use `Mounts` with type `volume`.
 - For host paths, use `Mounts` with type `bind`.
- For IoT Edge on Kubernetes, bind through `Mounts` works only for directory, and not for file.

Example - Storage via volume mounts

For IoT Edge on docker, host path bindings are used to map the shares on the device to paths inside the container. Here are the container create options used on FPGA devices:

```
{  
  "HostConfig":  
  {  
    "Binds":  
    [  
      "<Host storage path for Edge local share>:<Module storage path>"  
    ]  
  }  
}
```

For host paths for IoT Edge on Kubernetes, an example of using `Mounts` with type `bind` is shown here:

```
{
  "HostConfig": {
    "Mounts": [
      {
        "Target": "<Module storage path>",
        "Source": "<Host storage path>",
        "Type": "bind"
      }
    ]
  }
}
```

For the GPU devices running IoT Edge on Kubernetes, volume mounts are used to specify storage. To provision storage using shares, the value of `Mounts.Source` would be the name of the SMB or NFS share that was provisioned on your GPU device. The `/home/input` is the path at which the volume is accessible within the container. Here are the container create options used on the GPU devices:

```
{
  "HostConfig": {
    "Mounts": [
      {
        "Target": "/home/input",
        "Source": "<nfs-or-smb-share-name-here>",
        "Type": "volume"
      },
      {
        "Target": "/home/output",
        "Source": "<nfs-or-smb-share-name-here>",
        "Type": "volume"
      }
    ]
  }
}
```

Network

Consider the following information when specifying networking for the IoT Edge modules.

- `HostPort` specification is required to expose a service both inside and outside the cluster.
 - K8sExperimental options to limit exposure of service to cluster only.
- Inter module communication requires `HostPort` specification, and connection using mapped port (and not using the container exposed port).
- Host networking works with `dnsPolicy = ClusterFirstWithHostNet`, with that all containers (especially `edgeHub`) don't have to be on host network as well.
- Adding port mappings for TCP, UDP in same request doesn't work.

Example - External access to modules

For any IoT Edge modules that specify port bindings, an IP address is assigned using the Kubernetes external service IP range that was specified in the local UI of the device. There are no changes to the container create options between IoT Edge on docker vs IoT Edge on Kubernetes as shown in the following example.

```
{
  "HostConfig": {
    "PortBindings": {
      "5000/tcp": [
        {
          "HostPort": "5000"
        }
      ]
    }
  }
}
```

However, to query the IP address assigned to your module, you can use the Kubernetes dashboard as described in [Get IP address for services or modules](#).

Alternatively, you can [Connect to the PowerShell interface of the device](#) and use the `iotedge` list command to list all the modules running on your device. The [Command output](#) will also indicate the external IPs associated with the module.

Resource usage

With the Kubernetes-based IoT Edge setups on GPU devices, the resources such as hardware acceleration, memory, and CPU requirements are specified differently than on the FPGA devices.

Compute acceleration usage

To deploy modules on FPGA, use the container create options as shown in the following config:

```
{
  "HostConfig": {
    "Privileged": true,
    "PortBindings": {
      "50051/tcp": [
        {
          "HostPort": "50051"
        }
      ]
    }
  },
  "k8s-experimental": {
    "resources": {
      "limits": {
        "microsoft.com/fpga_catapult": 2
      },
      "requests": {
        "microsoft.com/fpga_catapult": 2
      }
    }
  },
  "Env": [
    "WIRESERVER_ADDRESS=10.139.218.1"
  ]
}
```

For GPU, use resource request specifications instead of Device Bindings as shown in the following minimal configuration. You request nvidia resources instead of catapult, and you needn't specify the `wireserver`.

```
{
    "HostConfig": {
        "Privileged": true,
        "PortBindings": {
            "50051/tcp": [
                {
                    "HostPort": "50051"
                }
            ]
        }
    },
    "k8s-experimental": {
        "resources": {
            "limits": {
                "nvidia.com/gpu": 2
            }
        }
    }
}
```

Memory and CPU usage

To set memory and CPU usage, use processor limits for modules in the `k8s-experimental` section.

```
"k8s-experimental": {
    "resources": {
        "limits": {
            "memory": "128Mi",
            "cpu": "500m",
            "nvidia.com/gpu": 2
        },
        "requests": {
            "nvidia.com/gpu": 2
        }
    }
}
```

The memory and CPU specification are not necessary but generally good practice. If `requests` isn't specified, the values set in `limits` are used as the minimum required.

Using shared memory for modules also requires a different way. For example, you can use the Host IPC mode for shared memory access between Live Video Analytics and Inference solutions as described in [Deploy Live Video Analytics on Azure Stack Edge](#).

Web proxy

Consider the following information when configuring web proxy:

If you have web proxy configured in your network, configure the following environment variables for the `edgeHub` deployment on your docker-based IoT Edge setup on FPGA devices:

- `https_proxy` : <proxy URL>
- `UpstreamProtocol` : `AmqpWs` (unless the web proxy allows `Amqp` traffic)

For the Kubernetes-based IoT Edge setups on GPU devices, you'll need to configure this additional variable during the deployment:

- `no_proxy` : localhost
- IoT Edge proxy on Kubernetes platform uses port 35000 and 35001. Make sure that your module does not run at these ports or it could cause port conflicts.

Other differences

- **Deployment strategy:** You may need to change the deployment behavior for any updates to the module. The default behavior for IoT Edge modules is rolling update. This behavior prevents the updated module from restarting if the module is using resources such as hardware acceleration or network ports. This behavior can have unexpected effects, specially when dealing with persistent volumes on Kubernetes platform for the GPU devices. To override this default behavior, you can specify a `Recreate` in the `k8s-experimental` section in your module.

```
{  
  "k8s-experimental": {  
    "strategy": {  
      "type": "Recreate"  
    }  
  }  
}
```

- **Modules names:** Module names should follow Kubernetes naming conventions. You may need to rename the modules running on IoT Edge with Docker when you move those modules to IoT Edge with Kubernetes. For more information on naming, see [Kubernetes naming conventions](#).
- **Other options:**
 - Certain docker create options that worked on FPGA devices will not work in the Kubernetes environment on your GPU devices. For example: , like – EntryPoint.
 - Environment variables such as `:_` need to be replaced by `_`.
 - **Container Creating** status for a Kubernetes pod leads to **backoff** status for a module on the IoT Hub resource. While there are a number of reasons for the pod to be in this status, a common reason is when a large container image is being pulled over a low network bandwidth connection. When the pod is in this state, the status of the module appears as **backoff** in IOT Hub though the module is just starting up.

Next steps

- Learn more about how to [Configure GPU to use a module](#).

Tutorial: Run a compute workload with IoT Edge module on Azure Stack Edge Pro GPU

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

This tutorial describes how to run a compute workload using an IoT Edge module on your Azure Stack Edge Pro GPU device. After you configure the compute, the device will transform the data before sending it to Azure.

This procedure can take around 10 to 15 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Add shares
- Add a compute module
- Verify data transform and transfer

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro GPU device, make sure that:

- You've activated your Azure Stack Edge Pro device as described in [Activate your Azure Stack Edge Pro](#).
- You have an IoT Edge module that you can run on your data. In this tutorial, we used a `filemove2` module that moves data from Edge local share on your device to Edge share from where the data goes to Azure Storage account.

Configure compute

To configure compute on your Azure Stack Edge Pro, you'll create an IoT Hub resource via the Azure portal.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**, and select **IoT Edge**.

The screenshot shows the Azure Stack Edge Pro Overview page. The left sidebar has sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Properties, Order details, Edge services (Virtual machines, IoT Edge, Cloud storage gateway), Monitoring (Device events, Alerts, Metrics), and Essentials. The main area has tabs for Update device, Reset device password, Return device, Feedback, Delete, and Refresh. A message says "Your device is running fine!". Under "Deployed edge services", there's a table with columns Name and Status, showing "No deployed services". Under "Edge services", there are three cards: "Virtual machines" (New), "IoT Edge" (highlighted with a red box), and "Cloud storage gateway". Each card has a "How to get started?" link.

2. In Enable IoT Edge service, select Add.

The screenshot shows the 'IoT Edge | Overview' page in the Azure Stack Edge portal. At the top, there's a search bar labeled 'Search (Ctrl+ /)' and several navigation links: '+ Add module', '+ Add trigger', 'Refresh configuration', 'Remove', and 'Refresh'. On the left, a sidebar has three items: 'Overview' (which is selected and highlighted with a red box), 'Modules', and 'Triggers'. Below the sidebar, a large central area is titled 'Get started with IoT Edge'. It contains a box with the heading 'Enable IoT Edge service' (also highlighted with a red box). Inside this box, it says 'Enable IoT Edge service to deploy IoT Edge modules locally on your device.' and provides two steps: '1 Set up your on-premises network for Edge computing.' and '2 Configure your Azure subscription for cloud management.'. A blue 'Add' button is located at the bottom of this box. Below this box, there's a link 'Steps to deploy IoT Edge services'. At the bottom of the main area, there's a section titled 'What's next' with the text 'Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services.'

3. On the **Configure Edge compute** blade, input the following information:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.
IoT Hub	Choose from New or Existing . By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.
Name	Accept the default name or enter a name for your IoT Hub resource.

Home > myasetest > IoT Edge >

Create IoT Edge service

Azure Stack Edge

Basics Review + Create

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription *	Edge Gateway Test
Resource group *	myaserg
IoT Hub *	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing myasetest-iothub

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

IoT Edge device: myasetest-edge
 IoT Gateway device: myasetest-storagegateway

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

- When you finish the settings, select **Review + Create**. Review the settings for your IoT Hub resource, and select **Create**.

Resource creation for an IoT Hub resource takes several minutes. After the resource is created, the **Overview** indicates the IoT Edge service is now running.

Home > myasetest >

IoT Edge | Overview

Azure Stack Edge

Overview **Io Edge service is running fine!**
 Start processing the data using IoT Edge modules. [Learn more](#)

Modules
 IoT Edge modules are containers that run Azure services, third-party services, or your own code.
 To read data from Edge local shares for processing and uploading it to cloud, add a Module. If multiple containers are deployed, which are chained together for pipeline processing, go to [Azure IoT Hub](#).

Add module

Triggers
 Add triggers to start processing at a repeated interval or on file events such as creation of a file, modification of a file on a share.

Add trigger

Edge Shares
 For container to store or transfer files and folders to Azure Storage account (other than temp data), create a share.

[Configure Shares](#)

Edge Storage account
 For container to transfer unstructured data like binary, audio, or video streaming data to Azure Storage account, create a storage account.

[Configure Storage account](#)

Network bandwidth usage
 If containers uploads data to cloud using shares configure network bandwidth usage across multiple time-of-day schedules.

[Configure Bandwidth schedule](#)

- To confirm the Edge compute role has been configured, go to **IoT Edge > Properties**.

The screenshot shows the 'IoT Edge | Properties' page for an Azure Stack Edge resource named 'myasetest'. The left sidebar includes links for Overview, Modules, Triggers, and Properties (which is selected and highlighted with a red box). The main content area displays four properties in a table:

IoT Hub	myasetest-iothub
IoT Edge device	myasetest-edge
IoT device for storage gateway	myasetest-storagegateway
Platform	Linux

When the Edge compute role is set up on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

It can take 20-30 minutes to configure compute because, behind the scenes, virtual machines and a Kubernetes cluster are being created.

After you have successfully configured compute in the Azure portal, a Kubernetes cluster and a default user associated with the IoT namespace (a system namespace controlled by Azure Stack Edge) exist.

Add shares

For the simple deployment in this tutorial, you'll need two shares: one Edge share and another Edge local share.

1. To add an Edge share on the device, do the following steps:
 - a. In your Azure Stack Edge resource, go to **Cloud storage gateway > Shares**.
 - b. From the command bar, select **+ Add share**.
 - c. On the **Add share** blade, provide the share name and select the share type.
 - d. To mount the Edge share, select the check box for **Use the share with Edge compute**.
 - e. Select the **Storage account, Storage service**, an existing user, and then select **Create**.

The screenshot shows the 'Cloud storage gateway | Shares' page. On the left, there's a navigation bar with 'Overview', 'Shares' (which is selected and highlighted with a red box), 'Storage accounts', 'Users', and 'Bandwidth'. At the top right, there's a search bar, a 'Search (Ctrl+ /)' button, an 'Add share' button (highlighted with a red box), and a 'Refresh' button. The main area shows a table with columns 'Name', 'Status', and 'Actions'. One row is visible: 'myasesmbedgecloud1' with status 'OK' and an 'OK' button. On the right, the 'Add share' dialog is open. It has sections for 'Share details' (Name: 'myasesmbedgecloud1', Type: 'SMB' selected), 'Configure as Edge local share' (checkbox checked), 'Storage account' ('mynewsal'), 'Storage service' ('Block Blob'), 'Select blob container' ('Create new' selected, 'myasesmbedgecloud1'), 'User details' (allow only read operations unchecked, 'All privilege local user' 'Create new' selected, 'User name': 'myaseuser1', 'Password': '*****', 'Confirm password': '*****'), and a 'Create' button.

NOTE

To mount NFS share to compute, the compute network must be configured on same subnet as NFS Virtual IP address. For details on how to configure compute network, go to [Enable compute network on your Azure Stack Edge Pro](#).

The Edge share is created, and you'll receive a successful creation notification. The share list might be updated, but you must wait for the share creation to be completed.

2. To add an Edge local share on the device, repeat all the steps in the preceding step and select the check box for **Configure as Edge local share**. The data in the local share stays on the device.

This screenshot is similar to the previous one but shows the 'Configure as Edge local share' checkbox checked in the 'Add share' dialog. A tooltip message at the bottom left of the dialog box states: 'Use an Edge local share to process data prior to upload to the cloud. Data in local shares stays on the device.' The rest of the dialog fields are identical to the first screenshot.

If you created a local NFS share, use the following remote sync (`rsync`) command option to copy files onto the share:

```
rsync <source file path> < destination file path>
```

For more information about the `rsync` command, go to [Rsync documentation](#).

3. Go to Cloud storage gateway > Shares to see the updated list of shares.

Name	Status	Type	Used for compute	Storage account	Storage service
myasesmbedgedcloud1	OK	SMB	Enabled	mynewsa1	Block Blob
myasesmbedgelocal1	OK	SMB	Disabled	-	-

Add a module

You could add a custom or a pre-built module. The device does not come with pre-built or custom modules. To learn how to create a custom module, go to [Develop a C# module for your Azure Stack Edge Pro device](#).

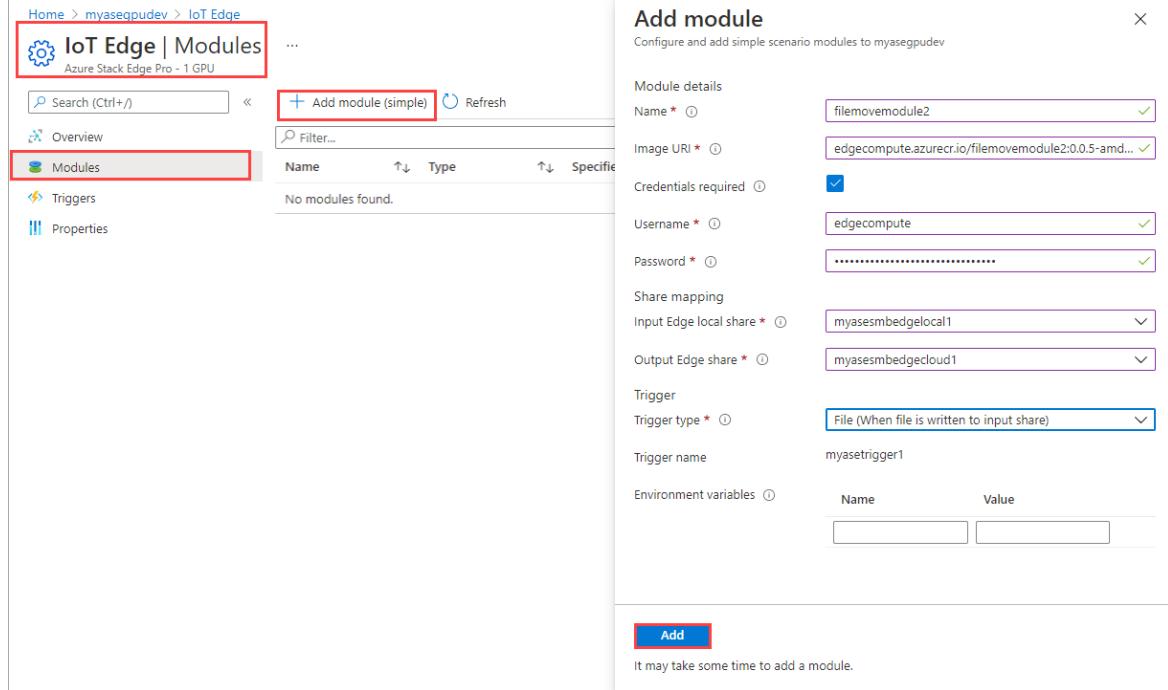
In this section, you add a custom module to the IoT Edge device that you created in [Develop a C# module for your Azure Stack Edge Pro](#). This custom module takes files from an Edge local share on the Edge device and moves them to an Edge (cloud) share on the device. The cloud share then pushes the files to the Azure storage account that's associated with the cloud share.

To add a module, do the following steps:

1. Go to **IoT Edge > Modules**. From the command bar, select **+ Add module**.
2. In the **Add module** blade, input the following values:

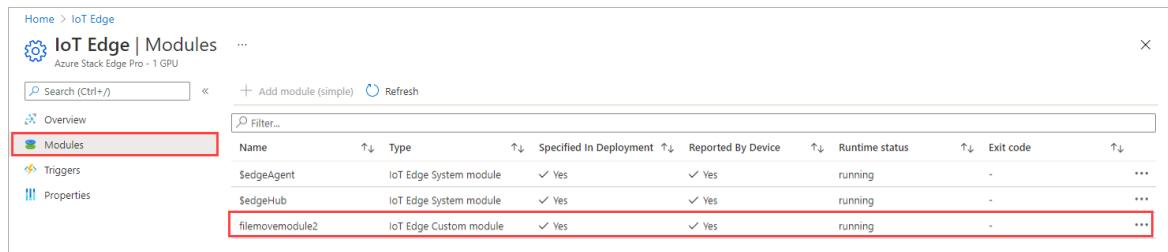
FIELD	VALUE
Name	A unique name for the module. This module is a docker container that you can deploy to the IoT Edge device that's associated with your Azure Stack Edge Pro.
Image URI	The image URI for the corresponding container image for the module.
Credentials required	If checked, username and password are used to retrieve modules with a matching URL.
Input share	Select an input share. The Edge local share is the input share in this case. The module used here moves files from the Edge local share to an Edge share where they are uploaded into the cloud.
Output share	Select an output share. The Edge share is the output share in this case.
Trigger type	Select from File or Schedule . A file trigger fires whenever a file event occurs such as a file is written to the input share. A scheduled trigger fires up based on a schedule defined by you.
Trigger name	A unique name for your trigger.

FIELD	VALUE
Environment variables	Optional information that will help define the environment in which your module will run.



3. Select **Add**. The module gets added. The **IoT Edge > Modules** page updates to indicate that the module is deployed. The runtime status of the module you added should be *running*.

FIELD	VALUE
Environment variables	Optional information that will help define the environment in which your module will run.

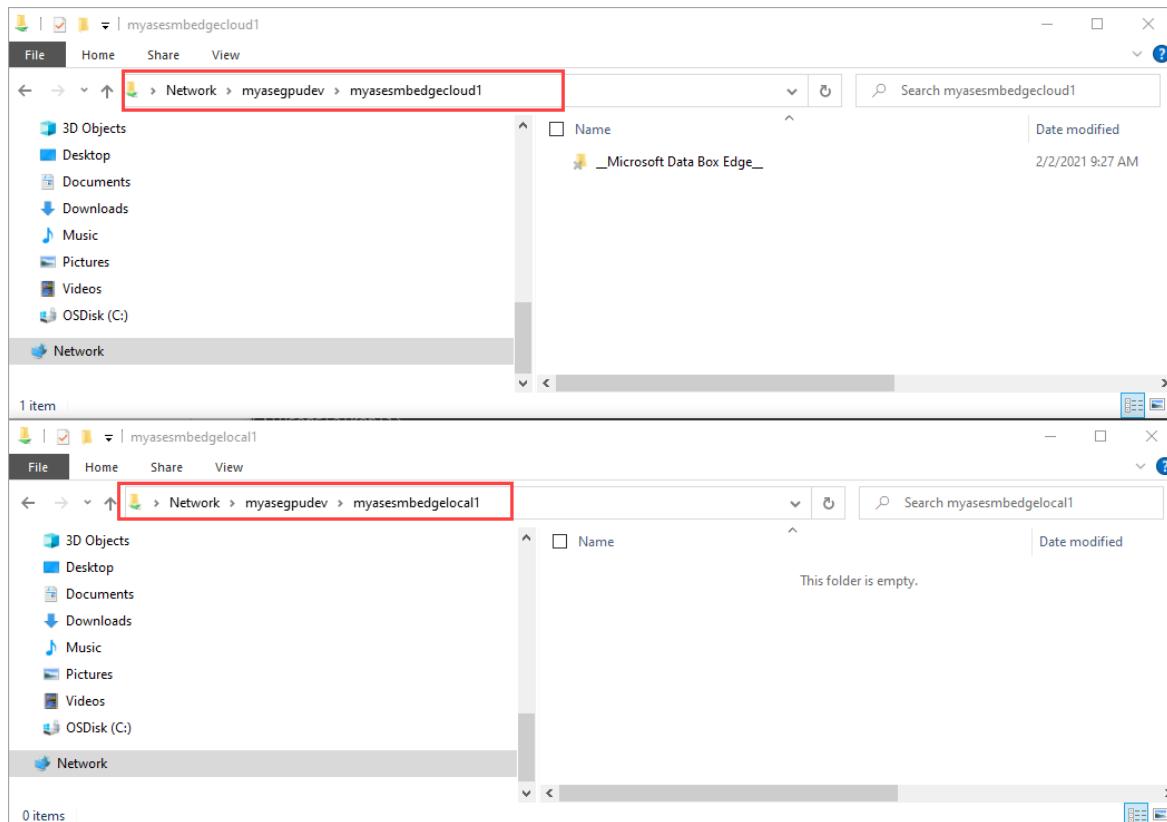


Verify data transform and transfer

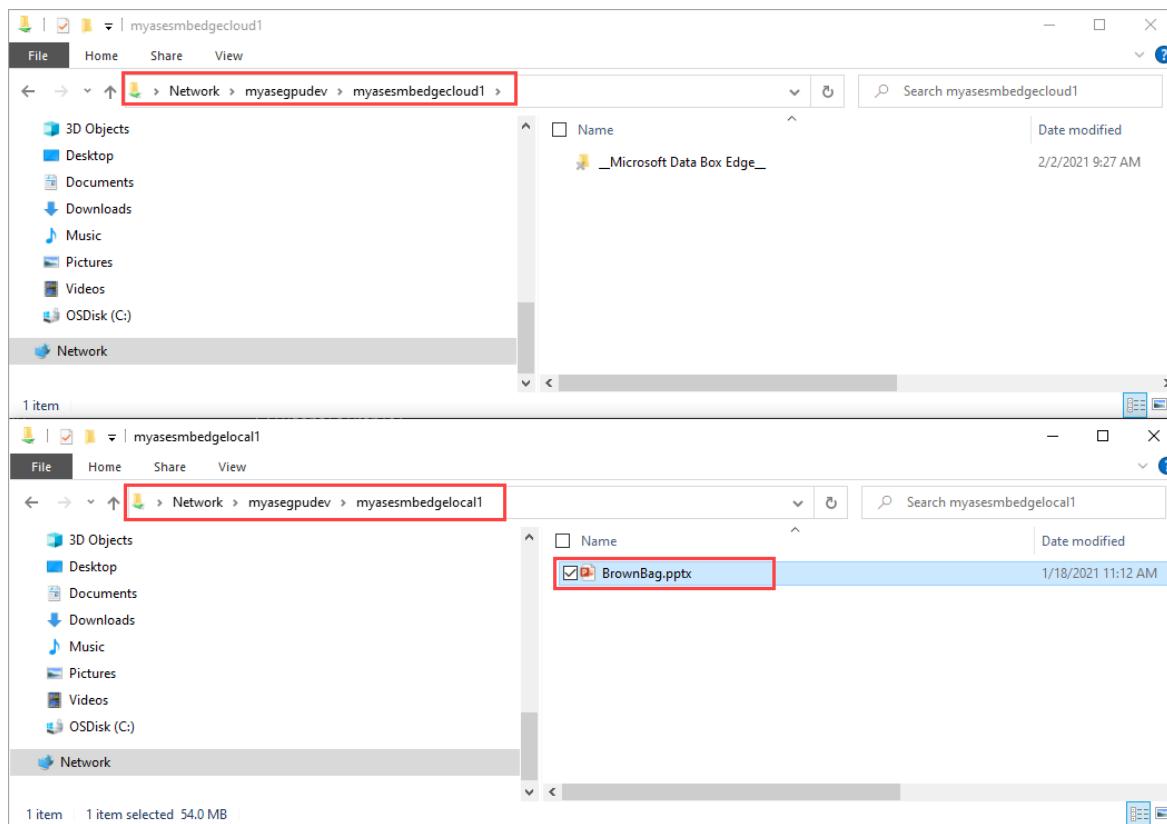
The final step is to ensure that the module is running and processing data as expected. The run-time status of the module should be running for your IoT Edge device in the IoT Hub resource.

To verify that the module is running and processing data as expected, do the following:

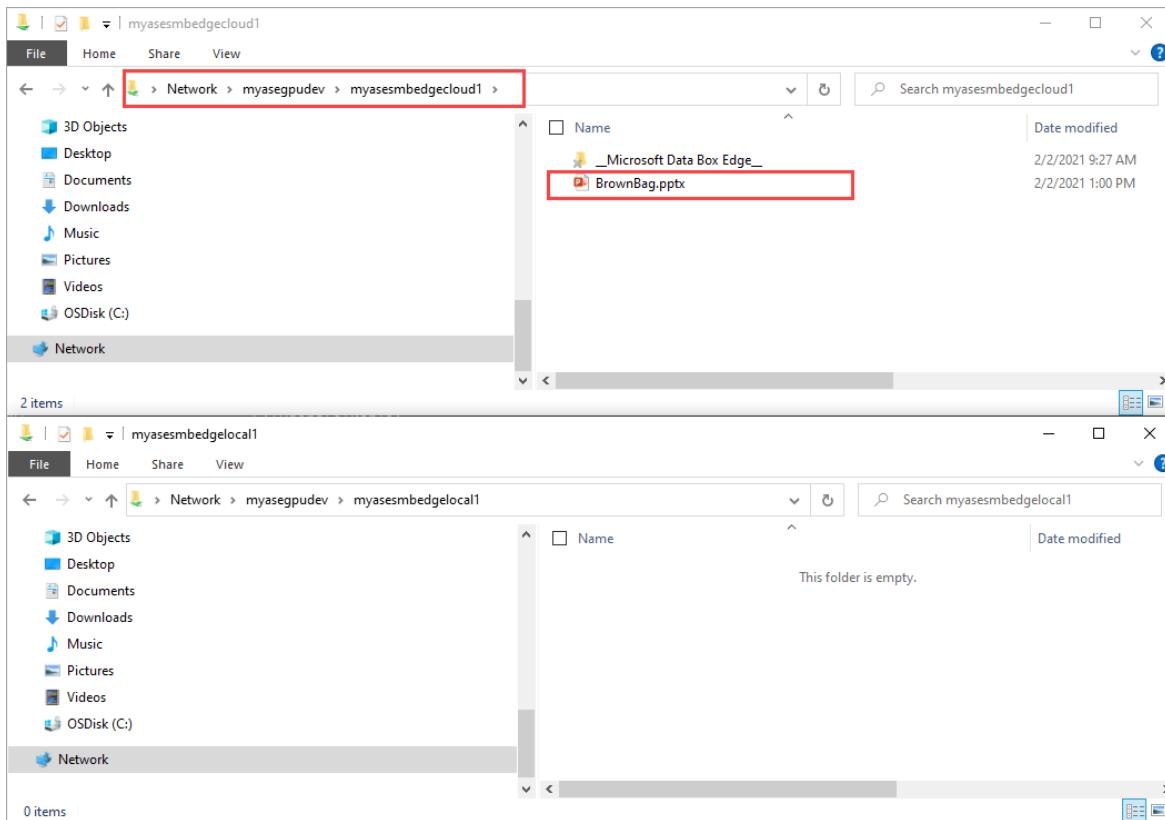
1. In File Explorer, connect to both the Edge local and Edge shares you created previously. See the steps



2. Add data to the local share.



The data gets moved to the cloud share.



The data is then pushed from the cloud share to the storage account. To view the data, you can use Storage Explorer or Azure Storage in portal.

Name	Modified	Access tier	Blob type	Size	Lease state
Microsoft Data Box Edge.pdf	2/2/2021, 9:27 AM	Hot (Inferred)	Block blob	54.02 MiB	Available
BrownBag.pptx	2/2/2021, 1:01:10 PM	Hot (Inferred)	Block blob	54.02 MiB	Available

You have completed the validation process.

Next steps

In this tutorial, you learned how to:

- Configure compute
- Add shares
- Add a compute module
- Verify data transform and transfer

To learn how to administer your Azure Stack Edge Pro device, see:

[Use local web UI to administer an Azure Stack Edge Pro](#)

Troubleshoot IoT Edge issues on your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot compute-related errors on an Azure Stack Edge Pro GPU device by reviewing runtime responses for the IoT Edge agent and errors for the IoT Edge service that's installed on your device.

Review IoT Edge runtime responses

Use the IoT Edge agent runtime responses to troubleshoot compute-related errors. Here is a list of possible responses:

- 200 - OK
- 400 - The deployment configuration is malformed or invalid.
- 417 - The device doesn't have a deployment configuration set.
- 412 - The schema version in the deployment configuration is invalid.
- 406 - The IoT Edge device is offline or not sending status reports.
- 500 - An error occurred in the IoT Edge runtime.

For more information, see [IoT Edge Agent](#).

Troubleshoot IoT Edge service errors

The following errors are related to the IoT Edge service on your Azure Stack Edge Pro GPU device.

Compute modules have Unknown status and can't be used

Error description

All modules on the device show Unknown status and can't be used. The Unknown status persists through a reboot.

Suggested solution

Delete the IoT Edge service, and then redeploy the module(s). For more information, see [Remove IoT Edge service](#).

Modules show as running but aren't working

Error description

The runtime status of the module shows as running, but you don't see the expected outcomes.

This condition may be caused by a module route configuration that's not working, or `edgehub` may not be routing messages as expected. You can check the `edgehub` logs. If you see errors such as failing to connect to the IoT Hub service, then the most common reason is the connectivity issues. The connectivity issues could occur because the AMQP port that the IoT Hub service is using as a default port for communication is blocked or the web proxy server is blocking these messages.

Suggested solution

Take the following steps:

1. To resolve the error, go to the IoT Hub resource for your device and then select your Edge device.
2. Go to **Set modules > Runtime settings**.
3. Add the **Upstream protocol** environment variable and assign it a value of **AMQPWS**. The messages configured in this case are sent over WebSockets via port 443.

Modules show as running but don't have an IP assigned

Error description

The runtime status of the module shows as running, but the containerized app doesn't have an IP address assigned.

This condition happens because the range of IPs you provided for Kubernetes external service IPs isn't sufficient. Extend this range to ensure that each container or VM that you deployed is covered.

Suggested solution

In the local web UI of your device, do the following steps:

1. Go to the **Compute** page. Select the port for which you enabled the compute network.
2. Enter a static, contiguous range of IPs for **Kubernetes external service IPs**. You need one IP for **edgehub** service. Additionally, you need one IP for each IoT Edge module and for each VM you'll deploy.
3. Select **Apply**. The changed IP range should take effect immediately.

For more information, see [Change external service IPs for containers](#).

Configure static IPs for IoT Edge modules

Problem description

Kubernetes assigns dynamic IPs to each IoT Edge module on your Azure Stack Edge Pro GPU device. A method is needed to configure static IPs for the modules.

Suggested solution

You can specify fixed IP addresses for your IoT Edge modules via the K8s-experimental section as described below:

```
{  
  "k8s-experimental": {  
    "serviceOptions" : {  
      "loadBalancerIP" : "100.23.201.78",  
      "type" : "LoadBalancer"  
    }  
  }  
}
```

Expose Kubernetes service as cluster IP service for internal communication

Problem description

By default, the IoT service type is **load balancer**, and the service is assigned externally facing IP addresses. If an application needs Kubernetes pods within the Kubernetes cluster to access other pods in the cluster, you may need to configure the service as a cluster IP service instead of a load balancer service. For more information, see [Kubernetes networking on your Azure Stack Edge Pro GPU device](#).

Suggested solution

You can use the create options via the K8s-experimental section. The following service option should work with port bindings.

```
{  
  "k8s-experimental": {  
    "serviceOptions" : {  
      "type" : "ClusterIP"  
    }  
  }  
}
```

Not able to create or update IoT role

Problem description

When configuring the IoT device during setup, you may see the following error:

(Http status code: 400) Could not create or update IoT role on <YourDeviceName>. An error occurred with the error code {NO_PARAM}. For more information, refer to the error code details (<https://aka.ms/dbe-error-codes>). If the error persists, contact Microsoft Support.

Suggested solution

If your datacenter firewall is restricting or filtering traffic based on source IPs or MAC addresses, make sure that the compute IPs (Kubernetes node IPs) and MAC addresses are on the allowed list. The MAC addresses can be specified by running the `Set-HcsMacAddressPool` cmdlet on the PowerShell interface of the device.

Next steps

- [Debug Kubernetes issues related to IoT Edge.](#)
- [Troubleshoot device issues.](#)

Tutorial: Transfer data via shares with Azure Stack Edge Pro GPU

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This tutorial describes how to add and connect to shares on your Azure Stack Edge Pro device. After you've added the shares, Azure Stack Edge Pro can transfer data to Azure.

This procedure can take around 10 minutes to complete.

In this tutorial, you learn how to:

- Add a share
- Connect to the share

Prerequisites

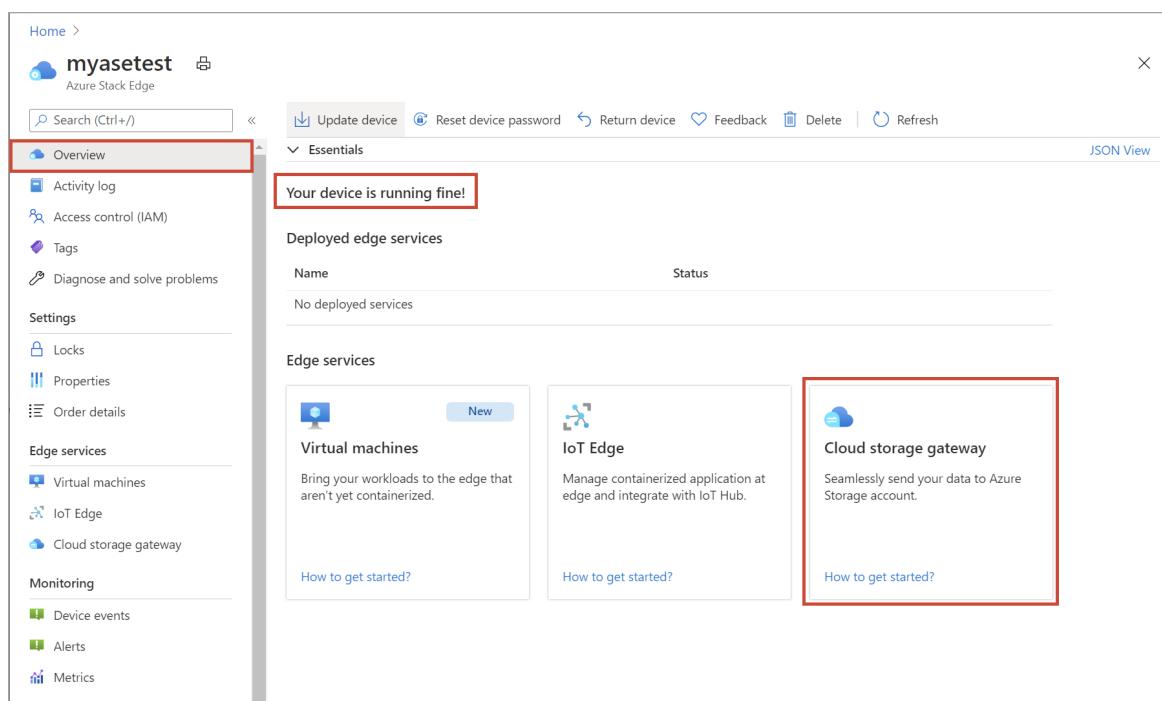
Before you add shares to Azure Stack Edge Pro, make sure that:

- You've installed your physical device as described in [Install Azure Stack Edge Pro](#).
- You've activated the physical device as described in [Activate your Azure Stack Edge Pro](#).

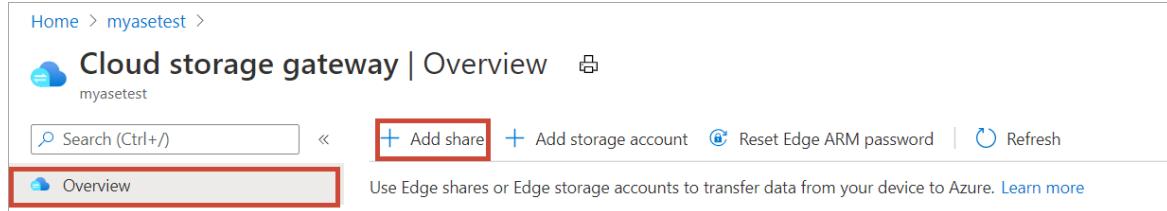
Add a share

To create a share, do the following procedure:

1. In the [Azure portal](#), select your Azure Stack Edge resource and then go to the **Overview**. Your device should be online. Select **Cloud storage gateway**.



2. Select **+ Add share** on the device command bar.



Home > myasetest >

Cloud storage gateway | Overview

myasetest

Search (Ctrl+ /) <> + Add share + Add storage account ⚙ Reset Edge ARM password Refresh

Overview Use Edge shares or Edge storage accounts to transfer data from your device to Azure. [Learn more](#)

3. In the **Add share** pane, follow these steps:

a. In the **Name** box, provide a unique name for your share.

The share name can have only letters, numerals, and hyphens. It must have between 3 to 63 characters and begin with a letter or a numeral. Hyphens must be preceded and followed by a letter or a numeral.

b. Select a **Type** for the share.

The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients.

Depending upon whether you choose SMB or NFS shares, the rest of the options vary slightly.

c. Provide a storage account where the share will reside.

d. In the **Storage service** drop-down list, select **Block Blob, Page Blob, or Files**.

The type of service you select depends on which format you want the data to use in Azure. In this example, because we want to store the data as block blobs in Azure, we select **Block Blob**. If you select **Page Blob**, make sure that your data is 512 bytes aligned. For example, a VHDX is always 512 bytes aligned.

IMPORTANT

Make sure that the Azure Storage account that you use does not have immutability policies or archiving policies set on it if you are using it with a Azure Stack Edge Pro or Data Box Gateway device. If the blob policies are immutable or if the blobs are aggressively archived, you'll experience upload errors when the blob is changed in the share. For more information, see [Set and manage immutability policies for blob storage](#).

e. Create a new blob container or use an existing one from the dropdown list. If creating a blob container, provide a container name. If a container doesn't already exist, it's created in the storage account with the newly created share name.

f. Depending on whether you've created an SMB share or an NFS share, do one of the following steps:

- **SMB share:** Under **All privilege local user**, select **Create new** or **Use existing**. If you create a new local user, enter a username and password, and then confirm the password. This action assigns permissions to the local user. Modification of share-level permissions is currently not supported. If you select the **Allow only read operations** check box for this share data, you can specify read-only users.

Add share

X

myasetest

Share details

Name *

myasesmb1



Type * ⓘ

SMB

NFS

Use the share with Edge compute ⓘ



Configure as Edge local share ⓘ



Storage account * ⓘ



Storage service ⓘ



User details

Allow only read operations ⓘ



All privilege local user ⓘ



Create new



Use existing

User name *

Admin1



Password *

.....



Confirm password *

.....



Create

- **NFS share:** Enter the IP addresses of allowed clients that can access the share.

Add share

myasetest

Share details

Name * mynfsshare

Type * SMB NFS

Use the share with Edge compute (i)

Configure as Edge local share (i)

Storage account * mystorageaccount02

Storage service * Block Blob

Select blob container * Create new Use existing

mynfsshare

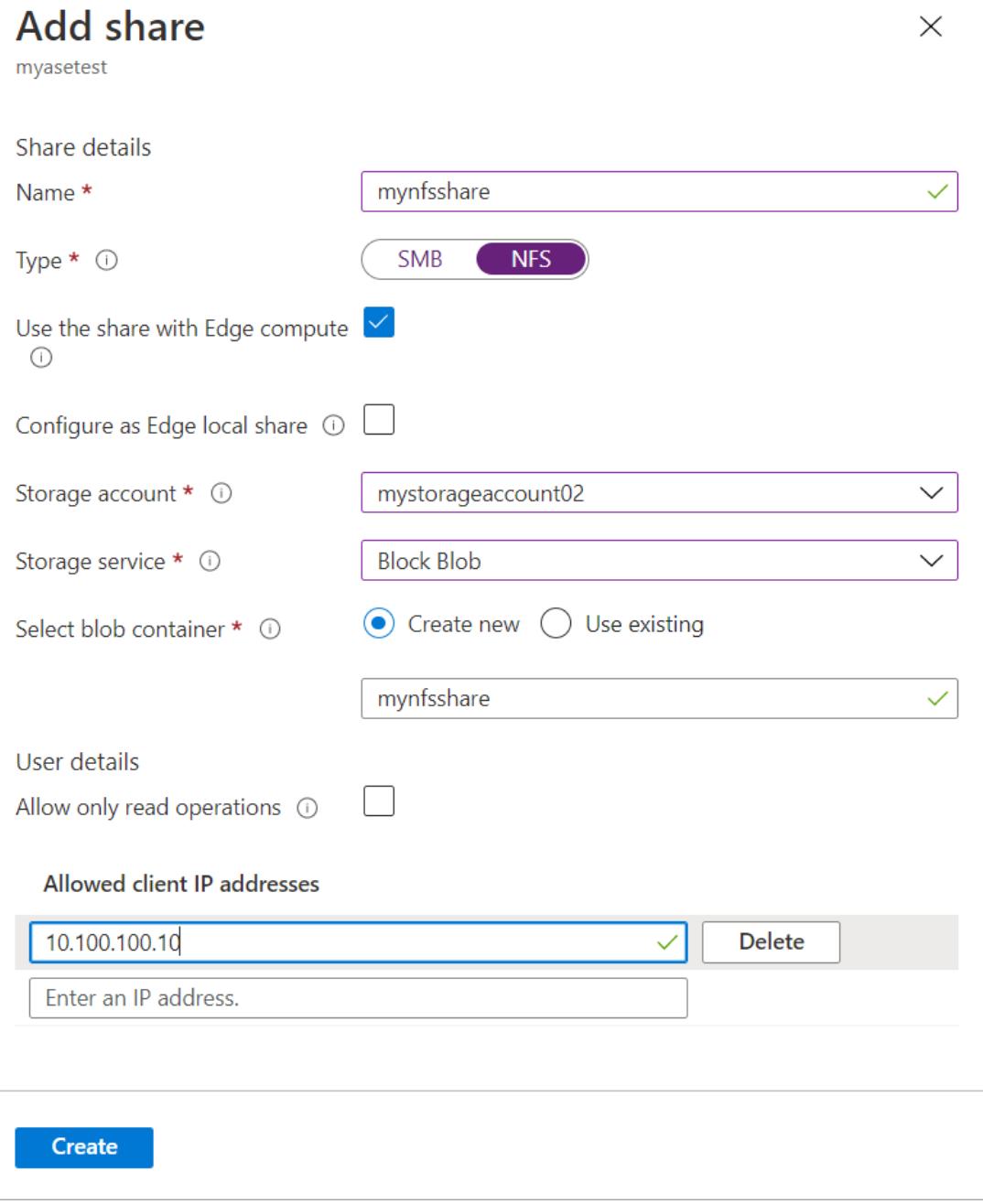
User details

Allow only read operations

Allowed client IP addresses

10.100.100.10

Enter an IP address.



4. Select **Create** to create the share.

You're notified that the share creation is in progress. After the share is created with the specified settings, the **Shares** tile updates to reflect the new share.

Connect to the share

You can now connect to one or more of the shares that you created in the last step. Depending upon whether you have an SMB or an NFS share, the steps can vary.

The first step is to ensure that the device name can be resolved when you are using SMB or NFS share.

Modify host file for name resolution

You will now add the IP of the device and the device friendly name that you defined on the local web UI of device to:

- The host file on the client, OR,
- The host file on the DNS server

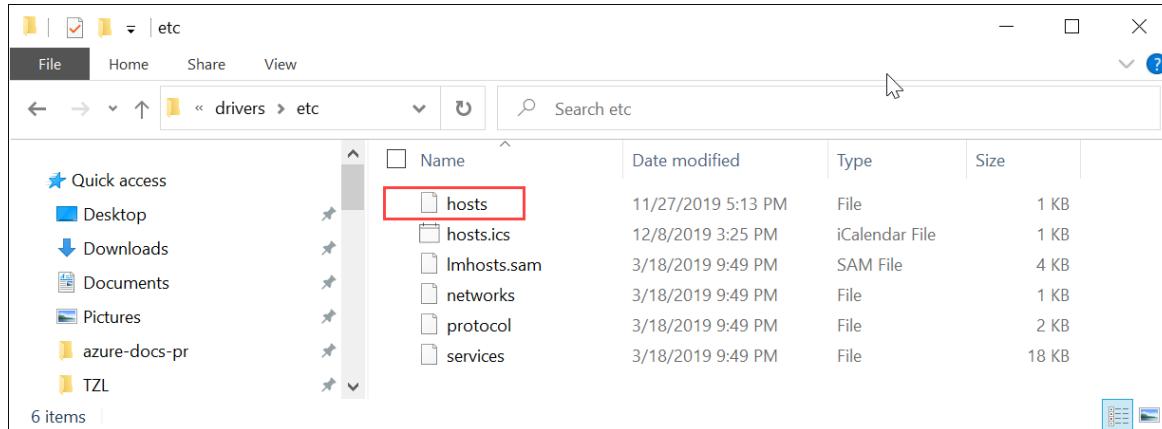
IMPORTANT

We recommend that you modify the host file on the DNS server for the device name resolution.

On your Windows client that you are using to connect to the device, take the following steps:

1. Start Notepad as an administrator, and then open the **hosts** file located at

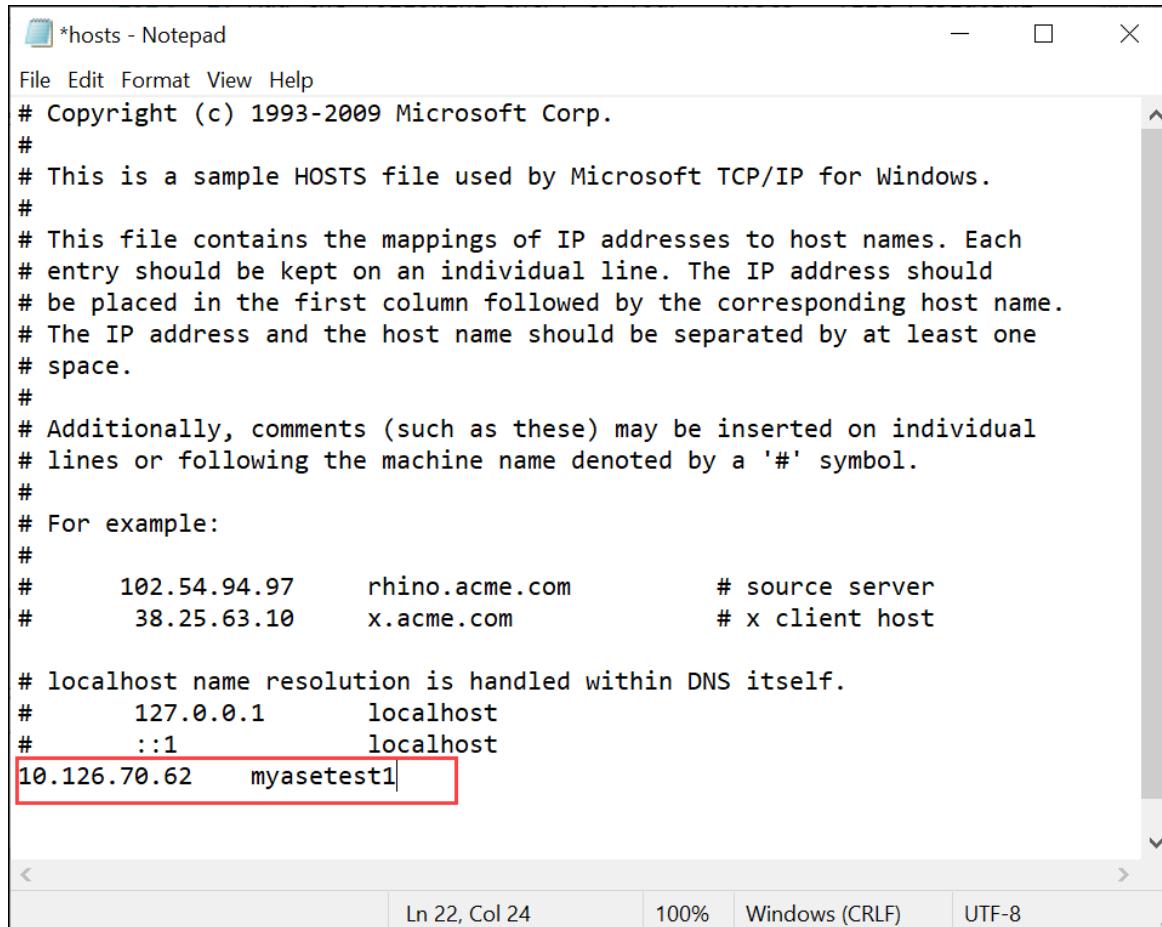
```
C:\Windows\System32\Drivers\etc\
```



2. Add the following entry to your **hosts** file replacing with appropriate values for your device:

```
<Device IP> <device friendly name>
```

You can get the device IP from the **Network** and the device friendly name from the **Device** page in the local web UI. The following screenshot of the hosts file shows the entry:



Connect to an SMB share

On your Windows Server client connected to your Azure Stack Edge Pro device, connect to an SMB share by entering the commands:

1. In a command window, type:

```
net use \\<Device name>\<share name> /u:<user name for the share>
```

NOTE

You can connect to an SMB share only with the device name and not via the device IP address.

2. When you're prompted to do so, enter the password for the share.

The sample output of this command is presented here.

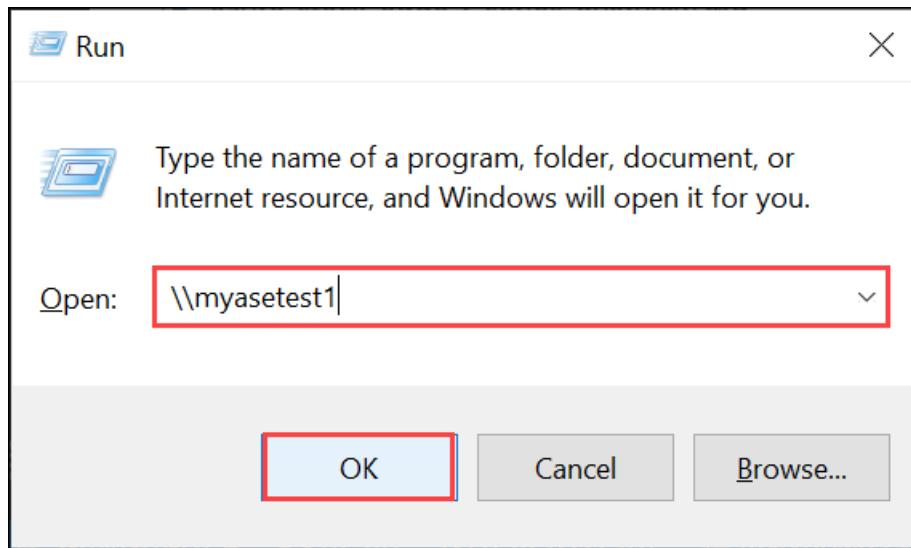
```
Microsoft Windows [Version 10.0.18363.476)
(c) 2017 Microsoft Corporation. All rights reserved.

C: \Users\AzureStackEdgeUser>net use \\myasetest1\myasesmbshare1 /u:aseuser
Enter the password for 'aseuser' to connect to 'myasetest1':
The command completed successfully.

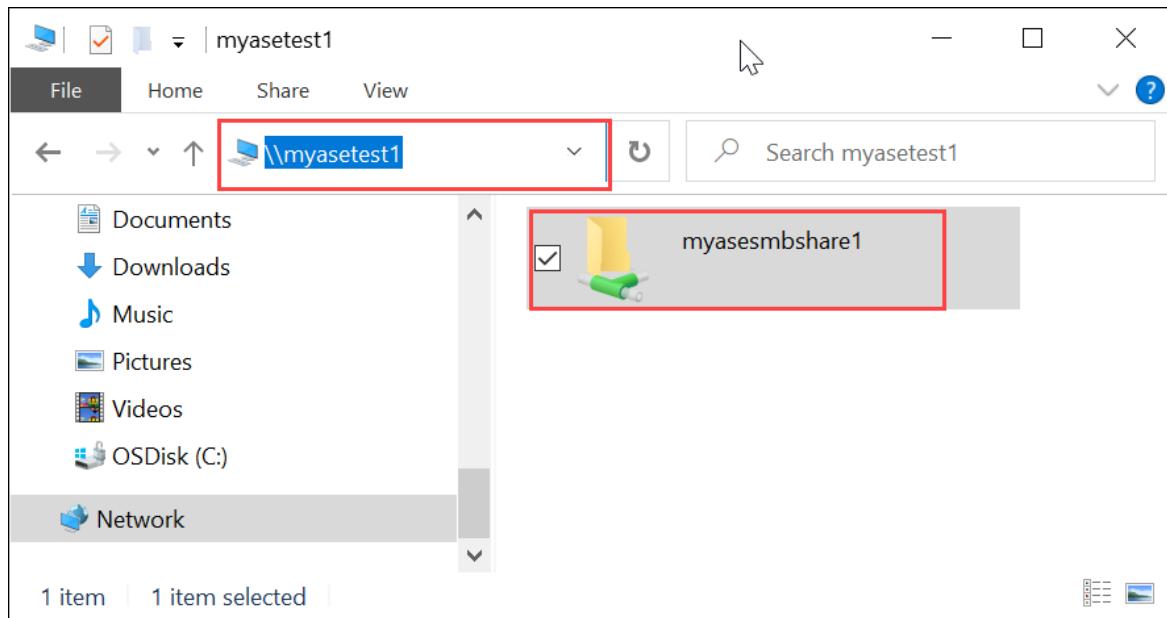
C: \Users\AzureStackEdgeUser>
```

3. On your keyboard, select Windows + R.

4. In the Run window, specify the `\\"<device name>`, and then select OK.



File Explorer opens. You should now be able to view the shares that you created as folders. In File Explorer, double-click a share (folder) to view the content.



The data is written to these shares as it is generated and the device pushes the data to cloud.

Connect to an NFS share

On your Linux client connected to your Azure Stack Edge Pro device, do the following procedure:

1. Make sure that the client has NFSv4 client installed. To install NFS client, use the following command:

```
sudo apt-get install nfs-common
```

For more information, go to [Install NFSv4 client](#).

2. After the NFS client is installed, mount the NFS share that you created on your Azure Stack Edge Pro device by using the following command:

```
sudo mount -t nfs -o sec=sys,resvport <device IP>/<NFS share on device> /home/username/<Folder on local Linux computer>
```

You can get the device IP from the **Network** page of your local web UI.

IMPORTANT

Use of `sync` option when mounting shares improves the transfer rates of large files. Before you mount the share, make sure that the directories that will act as mountpoints on your local computer are already created. These directories should not contain any files or subfolders.

The following example shows how to connect via NFS to a share on your Azure Stack Edge Pro device. The device IP is `10.10.10.60`. The share `mylinuxshare2` is mounted on the `ubuntuVM`. The share mount point is `/home/azurestakedgeubuntuhost/edge`.

```
sudo mount -t nfs -o sec=sys,resvport 10.10.10.60:/mylinuxshare2 /home/azurestakedgeubuntuhost/Edge
```

NOTE

The following caveats are applicable to this release:

- After a file is created in the share, renaming of the file isn't supported.
- Deleting a file from a share does not delete the entry in the Azure Storage account.
- When using `rsync` to copy over NFS, use the `--inplace` flag.

Next steps

In this tutorial, you learned about the following Azure Stack Edge Pro topics:

- Add a share
- Connect to share

To learn how to transform your data by using Azure Stack Edge Pro, advance to the next tutorial:

[Transform data with Azure Stack Edge Pro](#)

Tutorial: Transfer data via storage accounts with Azure Stack Edge Pro GPU

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This tutorial describes how to add and connect to storage accounts on your Azure Stack Edge Pro device. After you've added the storage accounts, Azure Stack Edge Pro can transfer data to Azure.

This procedure can take around 30 minutes to complete.

In this tutorial, you learn how to:

- Add a storage account
- Connect to the storage account

Prerequisites

Before you add storage accounts to Azure Stack Edge Pro, make sure that:

- You've installed your physical device as described in [Install Azure Stack Edge Pro](#).
- You've activated the physical device as described in [Activate your Azure Stack Edge Pro](#).

Add an Edge storage account

To create an Edge storage account, do the following procedure:

1. In the [Azure portal](#), select your Azure Stack Edge resource and then go to the **Overview**. Your device should be online. Go to **Cloud storage gateway > Storage accounts**.
2. Select **+ Add storage account** on the device command bar.

The screenshot shows the Azure Stack Edge Pro Cloud storage gateway Overview page. The left sidebar has tabs for Home, myasetest, Overview (which is selected), Shares, Storage accounts, Users, and Bandwidth. The main content area has a header 'Cloud storage gateway | Overview'. Below it, there's a search bar, a 'Add share' button, and a 'Add storage account' button (which is highlighted with a red box). A note says 'Use Edge shares or Edge storage accounts to transfer data from your device to Azure.' Below this is a section titled 'Edge shares' with a 'Total' count of '3 No'. It lists two shares: 'mysharelocal1' and 'mysmb-cloudshare', both marked as 'OK'. At the bottom is a 'View all' link.

3. In the **Add Edge storage account** pane, specify the following settings:

- a. Provide a unique name for the Edge storage account on your device. Storage account names can only contain lowercase numbers and letters. Special characters are not allowed. Storage account name has to be unique within the device (not across the devices).
 - b. Provide an optional description for the information on the data the storage account is holding.
 - c. By default, the Edge storage account is mapped to an Azure Storage account in the cloud, and the data from the storage account is automatically pushed to the cloud. Specify the Azure storage account that your Edge storage account is mapped to.
 - d. Create a new container, or select from an existing container in the Azure storage account. Any data from the device that is written to the Edge storage account is automatically uploaded to the selected storage container in the mapped Azure Storage account.
 - e. After all the storage account options are specified, select **Add** to create the Edge storage account. You are notified when the Edge storage account is successfully created. The new Edge storage account is then displayed in the list of storage accounts in the Azure portal.
4. If you select this new storage account and go to **Access keys**, you can find the blob service endpoint and the corresponding storage account name. Copy this information as these values together with the access keys will help you connect to the Edge storage account.

The screenshot shows the Azure portal interface for managing storage accounts. The URL in the address bar is 'Home > MyASEDevice - Storage accounts > myasetiered1 - Access keys'. On the left, there's a sidebar with 'Overview', 'Settings', and 'Access keys' (which is selected and highlighted with a red border). The main content area has a heading 'Use the blob service endpoint, storage account, storage account access keys to connect to your device. To retrieve your storage account access keys from your device, use the Azure Storage API or Azure CLI.' Below this, there are two input fields: 'Blob service endpoint' containing 'https://myasetiered1.blob.dbe-1dcnhq2.wdshcsso.com' and 'Edge storage account name' containing 'myasetiered1'. Both of these fields are also highlighted with a red border.

You get the access keys by [Connecting to the device local APIs using Azure Resource Manager](#).

Connect to the Edge storage account

You can now connect to Edge storage REST APIs over *http* or *https*.

- *Https* is the secure and recommended way.
- *Http* is used when connecting over trusted networks.

Connect via http

Connection to Edge storage REST APIs over http requires the following steps:

- Add the Azure consistent service VIP and blob service endpoint to the remote host
- Verify the connection

Each of these steps is described in the following sections.

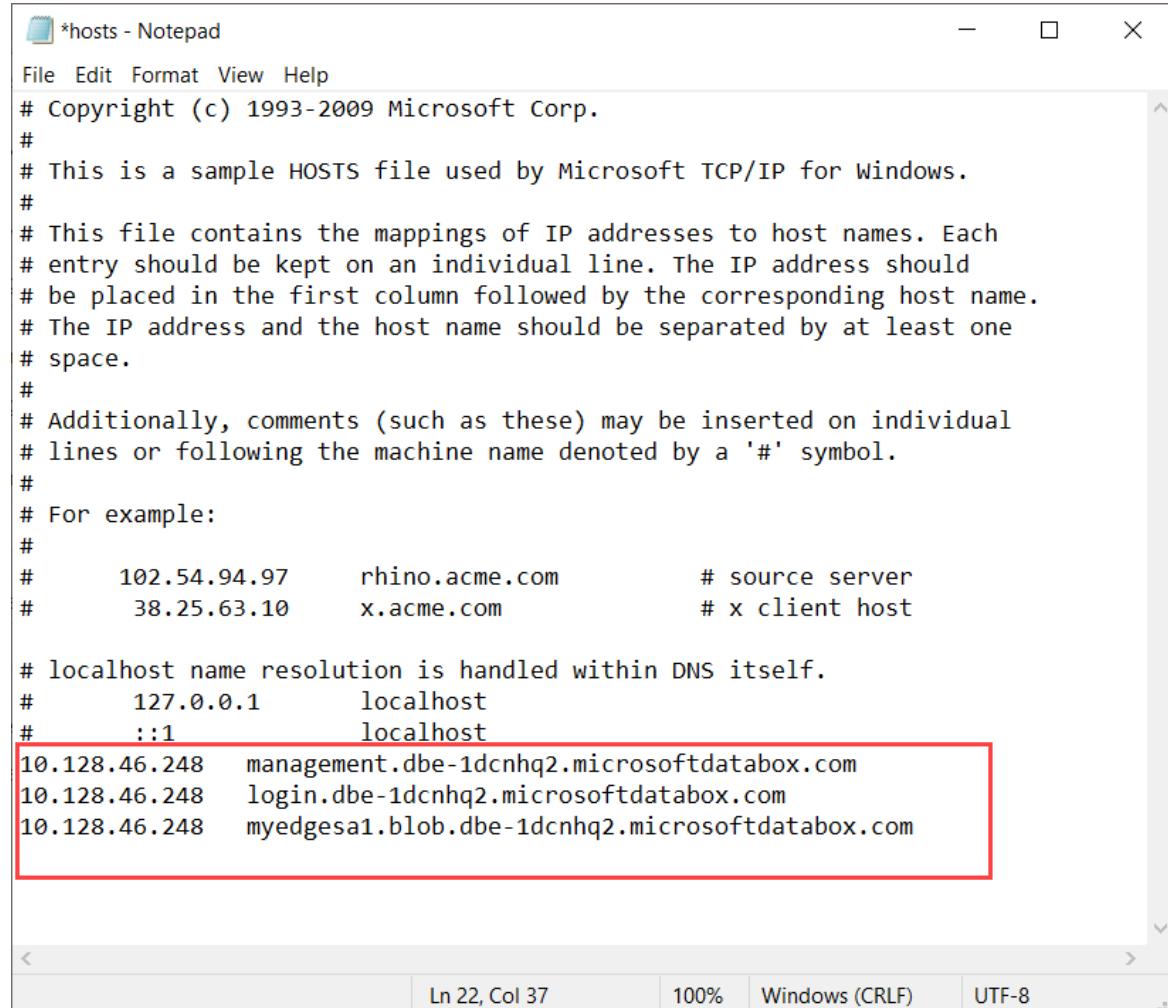
Add device IP address and blob service endpoint to the remote client

1. Go to the local web UI of your device and sign into your device. Ensure that the device is unlocked.
2. Go to the **Network settings** page. Make a note of the device IP address for the network interface used to connect to the client.
3. If working with a remote Windows client, start **Notepad** as an administrator, and then open the hosts file located at `C:\Windows\System32\Drivers\etc`.

4. Add the following entry to your hosts file: <Device IP address> <Blob service endpoint>

You got the blob service endpoint from the Edge storage account created in the Azure portal. You will use the suffix of the blob service endpoint only.

For reference, use the following image. Save the `hosts` file.



```
*hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97    rhino.acme.com          # source server
#      38.25.63.10      x.acme.com            # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost
10.128.46.248    management.dbe-1dcnhq2.microsoftdatabox.com
10.128.46.248    login.dbe-1dcnhq2.microsoftdatabox.com
10.128.46.248    myedgesa1.blob.dbe-1dcnhq2.microsoftdatabox.com
```

Verify connection

To verify the connection, you would typically need the following information (may vary) you gathered in the previous step:

- Storage account name.
- Storage account access key.
- Blob service endpoint.

You already have the storage account name and the blob service endpoint. You can get the storage account access key by connecting to the device via the Azure Resource Manager using an Azure PowerShell client.

Follow the steps in [Connect to the device via Azure Resource Manager](#). Once you have signed into the local device APIs via the Azure Resource Manager, get the list of storage accounts on the device. Run the following cmdlet:

```
Get-AzureRMStorageAccount
```

From the list of the storage accounts on the device, identify the storage account for which you need the access key. Note the storage account name and resource group.

A sample output is shown below:

```
PS C:\windows\system32> Get-AzureRmStorageAccount

StorageAccountName ResourceGroupName Location SkuName      Kind     AccessTier CreationTime
ProvisioningState EnableHttpsTrafficOnly
-----
-----
myasetiered1      myasetiered1      DBELocal StandardLRS Storage          11/27/2019 7:10:12 PM Succeeded
False
```

To get the access key, run the following cmdlet:

```
Get-AzureRmStorageAccountKey
```

A sample output is shown below:

```
PS C:\windows\system32> Get-AzureRmStorageAccountKey

cmdlet Get-AzureRmStorageAccountKey at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ResourceGroupName: myasetiered1
Name: myasetiered1

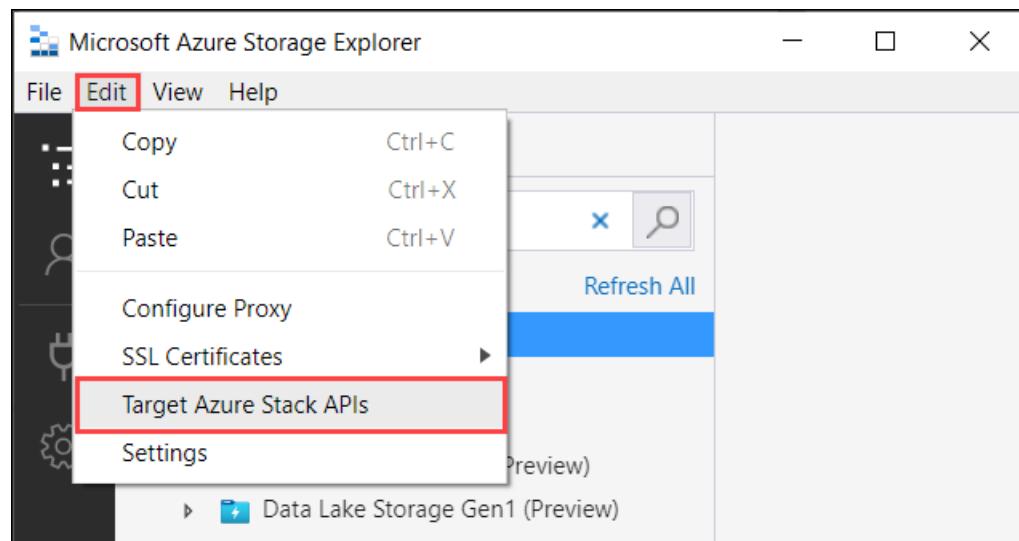
KeyName Value    Permissions
----- -----
key1   Jb2brRNjRNmArFcDWvL4ufspJJlo+Nieuh8Mp4YUOVQNbirA1uxEdHeV8Z0dXbsG7emejFWI9hxyR1T93ZncA==      Full
key2   6VANuHzHcJV04EFeyPiWRsFWhHPkgmX1+a3bt5q0Q2qIzohyskIF/2gfNMqp9rlNC/w+mBqQ2mI42QgoJSmavg==      Full
```

Copy and save this key. You will use this key to verify the connection using Azure Storage Explorer.

To verify that the connection is successfully established, use Storage Explorer to attach to an external storage account. If you do not have Storage Explorer, [download Storage Explorer](#).

If this is the first time you are using Storage Explorer, you need to perform the following steps.

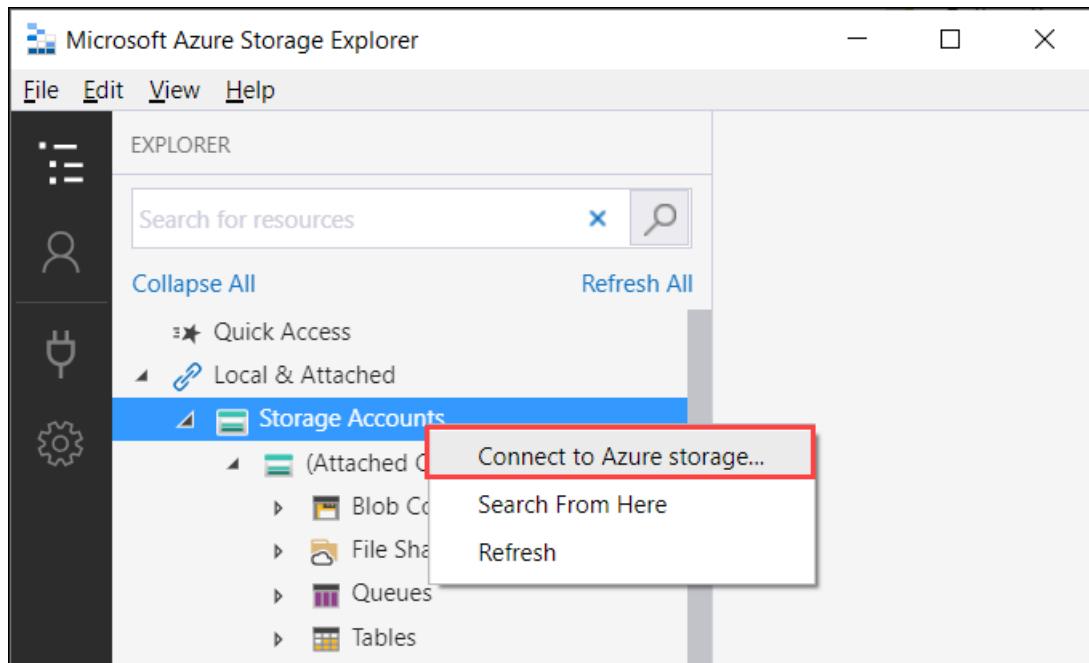
1. From the top command bar, go to Edit > Target Azure Stack APIs.



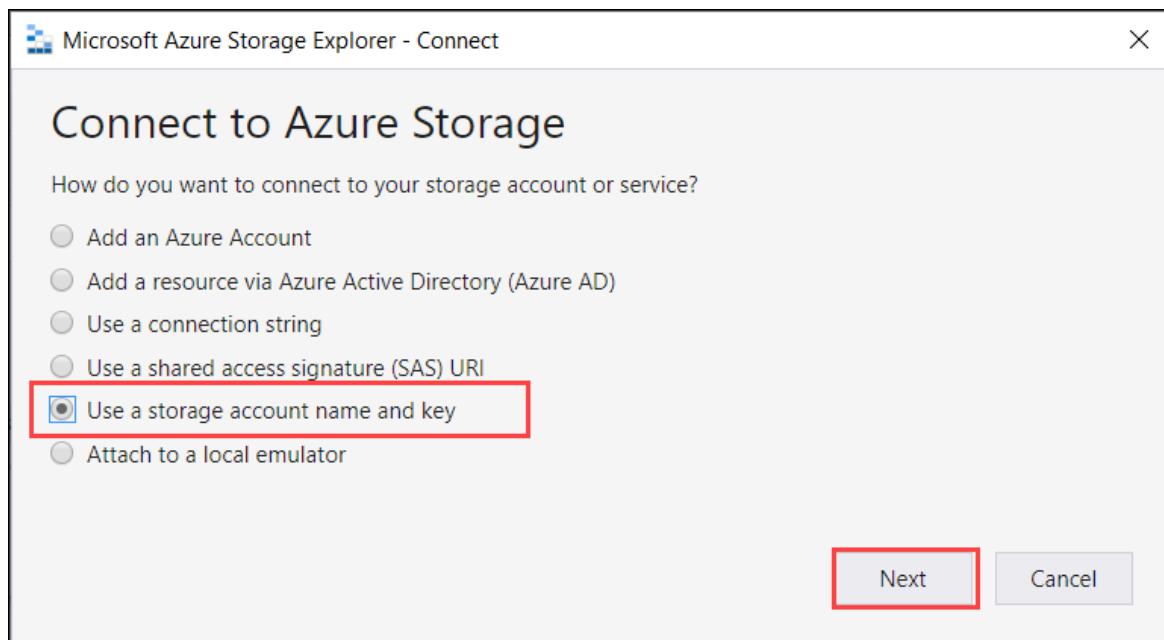
2. Restart the Storage Explorer for the changes to take effect.

Follow these steps to connect to the storage account and verify the connection.

1. In Storage Explorer, select storage accounts. Right-click and select the Connect to Azure Storage option.

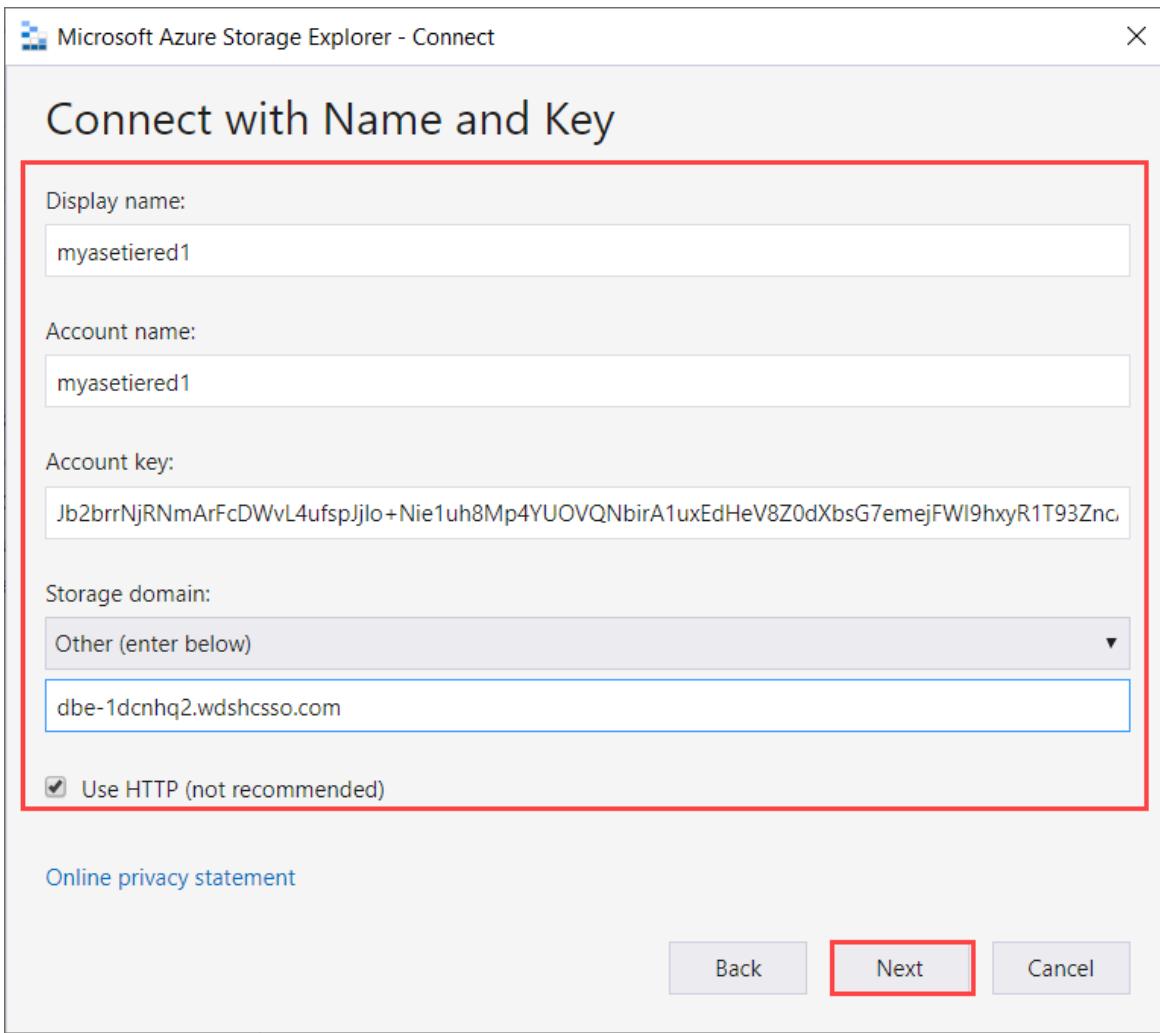


2. In the Connect to Azure Storage dialog, select **Use a storage account name and key**.

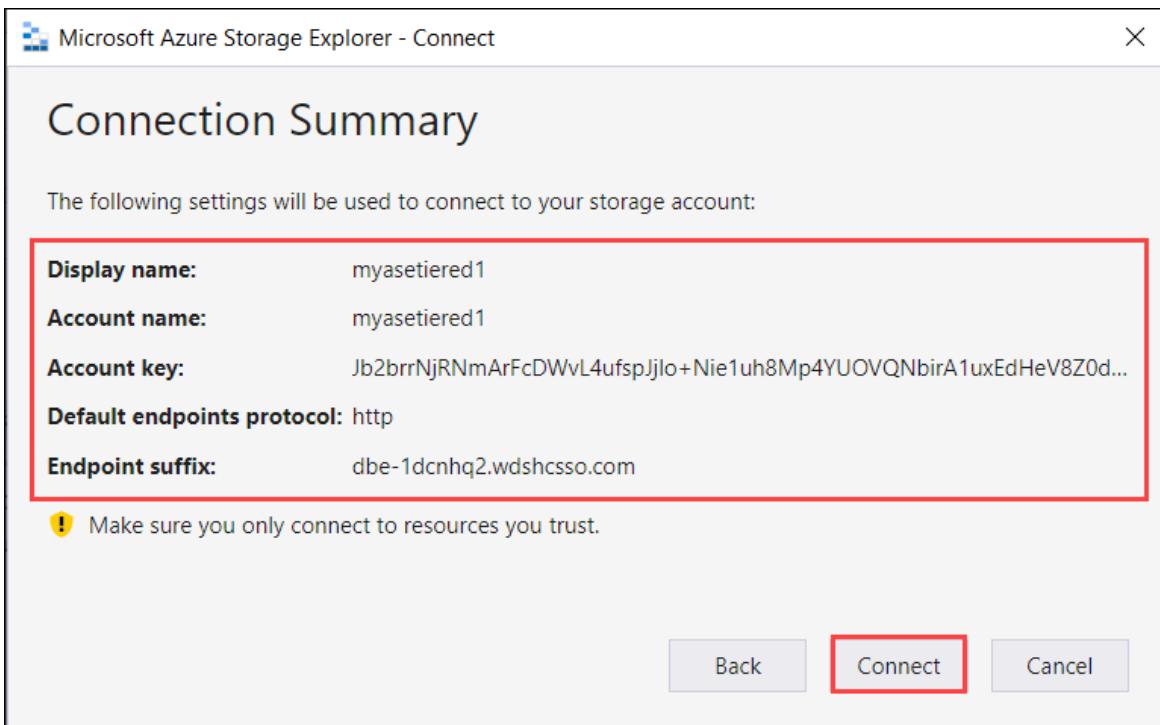


3. In the **Connect with Name and Key** dialog, take the following steps:

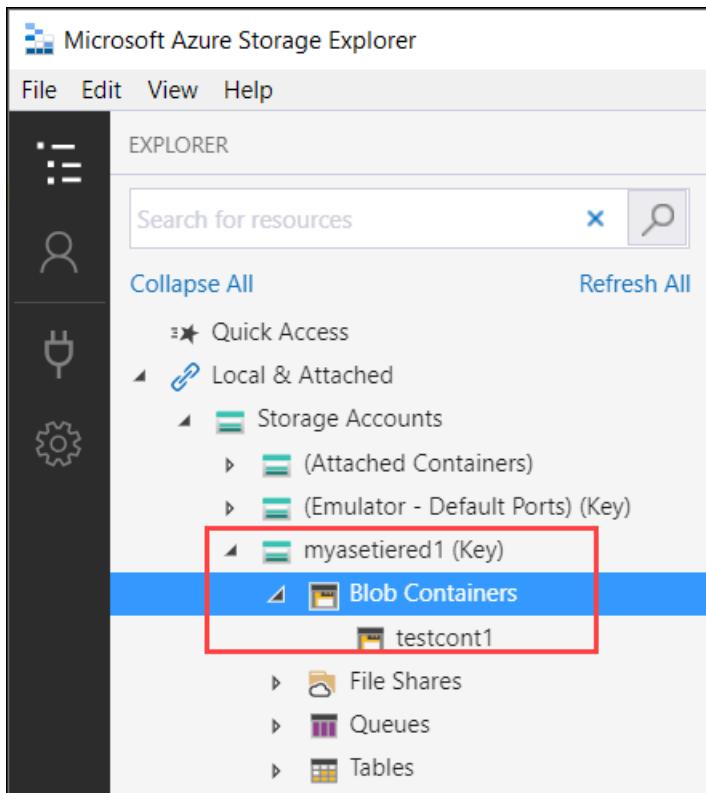
- Enter a display name for your Edge storage account.
- Provide the Edge storage account name.
- Paste the access key that you got from the device local APIs via Azure Resource Manager.
- Select Storage domain as **Other (enter below)** and then provide the suffix of blob service endpoint in the format: `<appliance name>.<DNSdomain>`.
- Check **Use HTTP** option as transfer is over *http*.
- Select **Next**.



4. In the **Connection Summary** dialog, review the provided information. Select **Connect**.



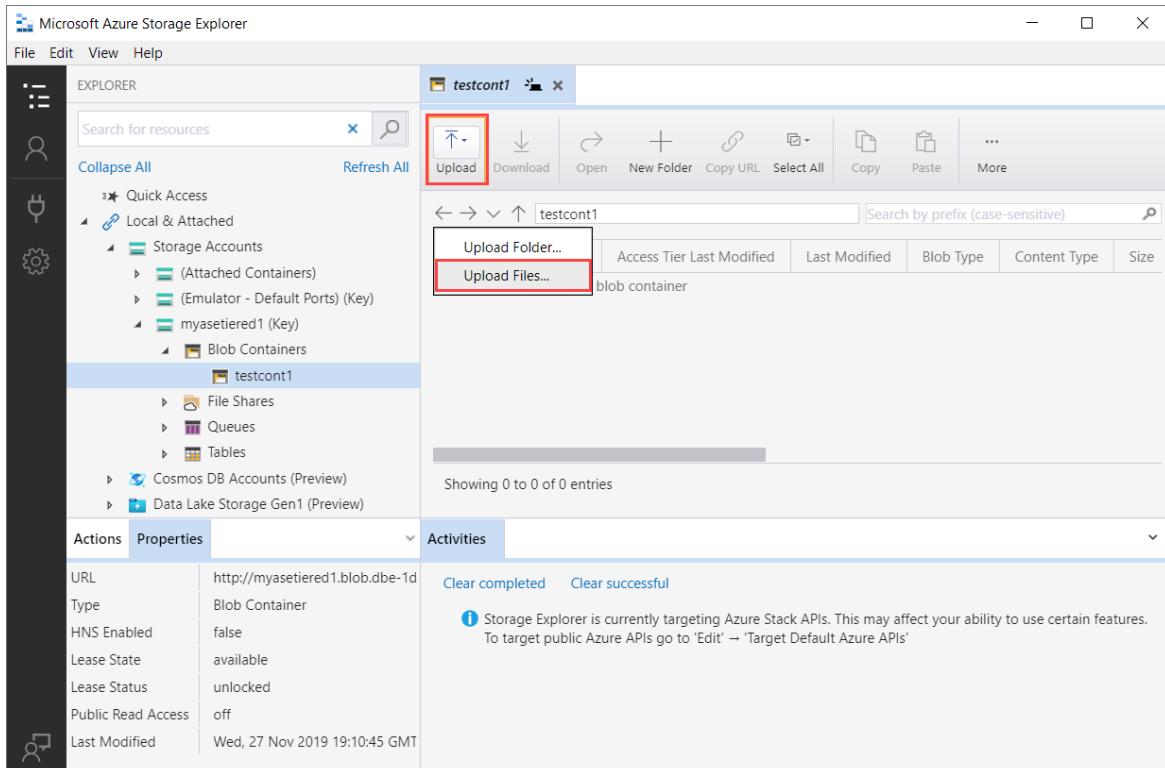
5. The account that you successfully added is displayed in the left pane of Storage Explorer with (External, Other) appended to its name. Select **Blob Containers** to view the container.



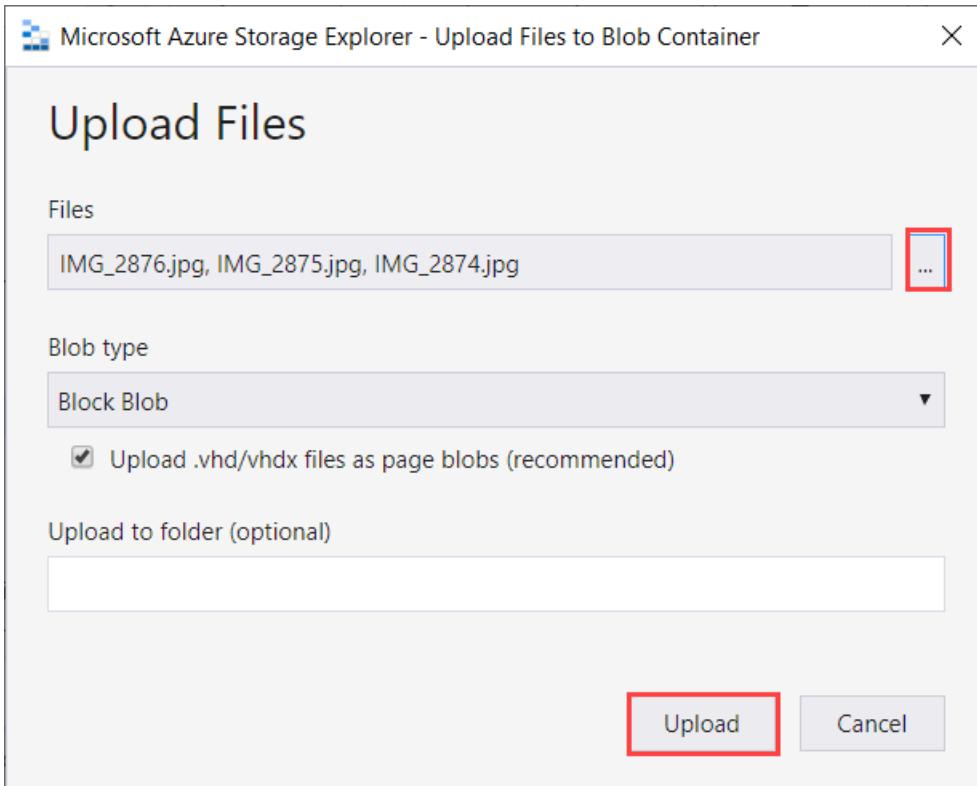
The next step to verify is that the data transfer is actually working correctly over this connection.

Take the following steps to load data into your Edge storage account on the device and it should automatically get tiered to the mapped Azure Storage account.

1. Select the container to which you want to load the data in your Edge storage account. Select **Upload** and then select **Upload files**.



2. In the **Upload files** dialog, navigate to and select the files that you want to upload. Select **Next**.



3. Verify that the files have uploaded. The uploaded files show up in the container.

Name	Access Tier	Last Modified	Blob Type	Con
IMG_2874.jpg		11/27/2019, 6:07:25 PM	Block Blob	imag
IMG_2875.jpg		11/27/2019, 6:07:25 PM	Block Blob	imag
IMG_2876.jpg		11/27/2019, 6:07:25 PM	Block Blob	imag

Showing 1 to 3 of 3 cached items

Activities

Clear completed Clear successful

Group upload complete: Uploaded: 3

Storage Explorer is currently targeting Azure Stack APIs. This may affect your ability to use certain features.
To target public Azure APIs go to 'Edit' → 'Target Default Azure APIs'

4. Next, you will connect to the Azure Storage account that was mapped to this Edge storage account. Any data that is uploaded to the Edge storage account should automatically tier to the Azure Storage account.

To get the connection string for the Azure Storage account, go to the **Azure Storage account > Access keys** and copy the connection string.

Home > mytests1 - Access keys

mytests1 - Access keys

Storage account

Search (Ctrl+)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Data transfer

Storage Explorer (preview)

Settings

Access keys

Geo-replication

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Storage account name: mytests1

key1

Key: VQdDqreatl60vNErQ/zLn4ajr8TcaCvoGmoQ5QNpWNGd7c9fueNNp8+Pf+eYURCKEINIJDZITBE0Y02PMpiBeQ==

Connection string: DefaultEndpointsProtocol=https;AccountName=mytests1;AccountKey=VQdDqreatl60vNErQ/zLn4ajr8TcaCvoGmoQ5QNpWNGd7c9fueNNp8+Pf+eYURCKEINIJDZITBE0Y02PMpiBeQ==

key2

Key: EYgYmYr8GgyHd1ZbT/MvSUR50ZTy4tBiZhQS6S3HJLHElmBV81L0WL4GUyUrbNxuUbz0G4GINbvSF85Tg8hIQ==

Connection string: DefaultEndpointsProtocol=https;AccountName=mytests1;AccountKey=EYgYmYr8GgyHd1ZbT/MvSUR50ZTy4tBiZhQS6S3HJLHElmBV81L0WL4GUyUrbNxuUbz0G4GINbvSF85Tg8hIQ==

Use the connection string to attach to the Azure Storage account.

Microsoft Azure Storage Explorer - Connect

Attach with Connection String

Display name: mytests1

Connection string: noQ5QNpWNGd7c9fueNNp8+Pf+eYURCKEINIJDZITBE0Y02PMpiBeQ==;EndpointSuffix=core.windows.net

Back Next Cancel

5. In the **Connection Summary** dialog, review the provided information. Select **Connect**.

Microsoft Azure Storage Explorer - Connect

Connection Summary

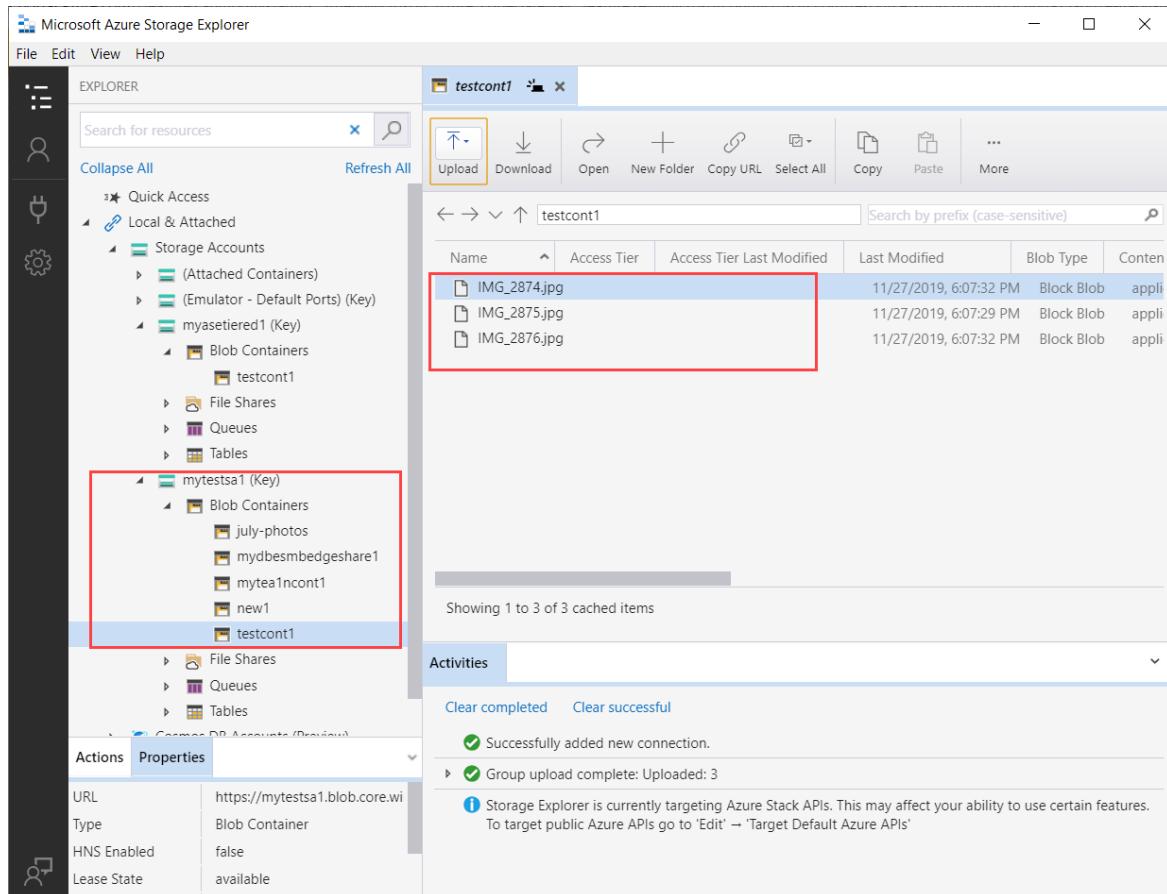
The following settings will be used to connect to your storage account:

Display name:	mytests1
Account name:	mytests1
Account key:	VQdDqreatl60vNErQ/zLn4ajr8TcaCvoGmoQ5QNpWNGd7c9fueNNp8+Pf+e...
Default endpoints protocol:	https
Endpoint suffix:	core.windows.net

! Make sure you only connect to resources you trust.

Back Connect Cancel

6. You will see that the files you uploaded in the Edge storage account were transferred to the Azure Storage account.



Connect via https

Connection to Azure Blob storage REST APIs over https requires the following steps:

- Get your blob endpoint certificate
- Import the certificate on the client or remote host
- Add the device IP and blob service endpoint to the client or remote host
- Configure and verify the connection

Each of these steps is described in the following sections.

Get certificate

Accessing Blob storage over HTTPS requires an SSL certificate for the device. You will also upload this certificate to your Azure Stack Edge Pro device as .pfx file with a private key attached to it. For more information on how to create (for test and dev purposes only) and upload these certificates to your Azure Stack Edge Pro device, go to:

- [Create the blob endpoint certificate.](#)
- [Upload the blob endpoint certificate.](#)
- [Import certificates on the client accessing the device.](#)

Import certificate

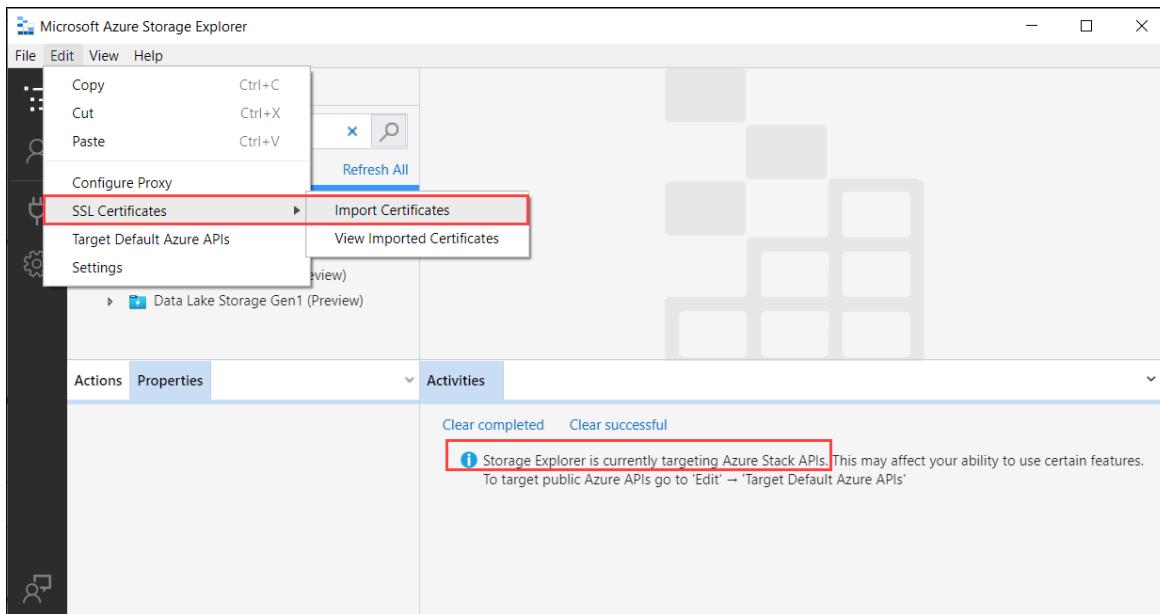
If using Azure Storage Explorer to connect to the storage accounts on the device, you also need to import certificate into Storage Explorer in PEM format. In Windows environment, Base-64 encoded .cer is the same as the PEM format.

Take the following steps to import the certificates on Azure Storage Explorer:

1. Make sure that Azure Storage Explorer is targeting the Azure Stack APIs. Go to **Edit > Target Azure**

Stack APIs. When prompted, restart Storage Explorer for the change to take effect.

2. To import SSL certificates, go to **Edit > SSL certificates > Import certificates**.



3. Navigate and provide the signing chain and blob certificates. Both the signing chain and the blob certificate should be in PEM format which is the same as Base64-encoded format on Windows system. You will be notified that the certificates were successfully imported.

Add device IP address and blob service endpoint

Follow the same steps to [add device IP address and blob service endpoint when connecting over http](#).

Configure and verify connection

Follow the steps to [Configure and verify connection that you used while connecting over http](#). The only difference is that you should leave the *Use http option* unchecked.

Next steps

In this tutorial, you learned about the following Azure Stack Edge Pro topics:

- Add a storage account
- Connect to a storage account

To learn how to transform your data by using Azure Stack Edge Pro, advance to the next tutorial:

[Transform data with Azure Stack Edge Pro](#)

Use Azure portal to manage shares on your Azure Stack Edge Pro

9/21/2022 • 9 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to manage shares on your Azure Stack Edge Pro. You can manage the Azure Stack Edge Pro via the Azure portal or via the local web UI. Use the Azure portal to add, delete, refresh shares, or sync storage key for storage account associated with the shares.

About shares

To transfer data to Azure, you need to create shares on your Azure Stack Edge Pro. The shares that you add on the Azure Stack Edge Pro device can be local shares or shares that push data to cloud.

- **Local shares:** Use these shares when you want the data to be processed locally on the device.
- **Shares:** Use these shares when you want the device data to be automatically pushed to your storage account in the cloud. All the cloud functions such as **Refresh** and **Sync storage keys** apply to the shares.

Add a share

Do the following steps in the Azure portal to create a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. Select **+ Add share** on the command bar.

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysmb-cloudshare	✓ OK	SMB	Disabled	mynewsa1	Block Blob	...
mysmb-localshare	✓ OK	SMB	Disabled	-	-	...

2. In **Add Share**, specify the share settings. Provide a unique name for your share.

Share names can only contain numbers, lowercase letters, and hyphens. The share name must be between 3 and 63 characters long and begin with a letter or a number. Each hyphen must be preceded and followed by a non-hyphen character.

3. Select a **Type** for the share. The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients. Depending upon whether you choose SMB or NFS shares, options presented are slightly different.
4. Provide a **Storage account** where the share lives. A container is created in the storage account with the share name if the container already doesn't exist. If the container already exists, then the existing container is used.

5. From the dropdown list, choose the **Storage service** from block blob, page blob, or files. The type of the service chosen depends on which format you want the data to reside in Azure. For example, in this instance, we want the data to reside as block blobs in Azure, hence we select **Block Blob**. If choosing **Page Blob**, you must ensure that your data is 512 bytes aligned. Use **Page blob** for VHDs or VHDX that are always 512 bytes aligned.

6. This step depends on whether you're creating an SMB or an NFS share.

- **If creating an SMB share** - In the **All privilege local user** field, choose from **Create new** or **Use existing**. If creating a new local user, provide the **username**, **password**, and then confirm password. This assigns the permissions to the local user. After you have assigned the permissions here, you can then use File Explorer to modify these permissions.

Add share

EdgeResource01

Share details

Name * mysharesmb1 ✓

Type * SMB NFS

Use the share with Edge compute

Configure as Edge local share

Storage account * teststorageaccountarja ✓

Storage service * Block Blob ✓

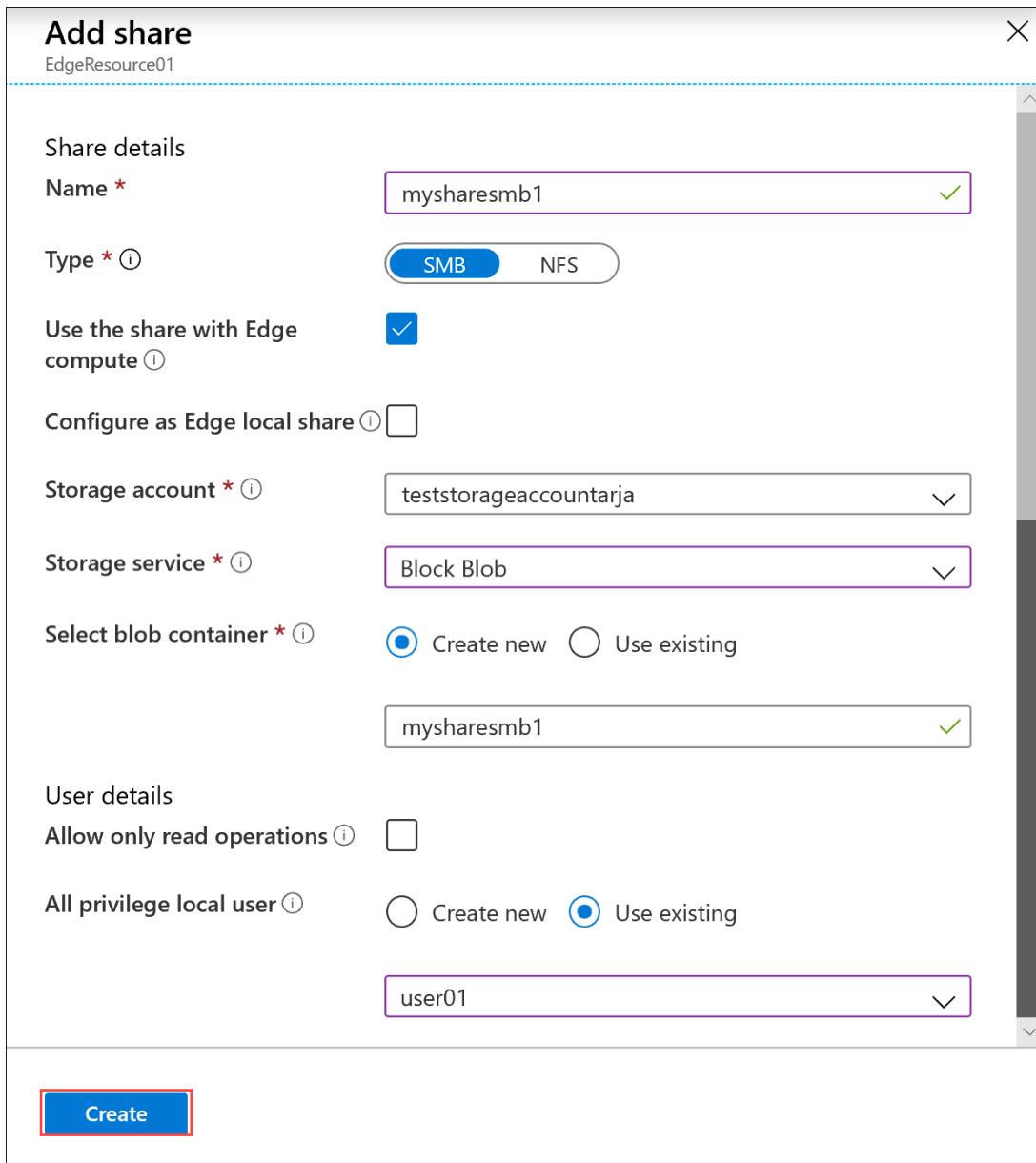
Select blob container * Create new Use existing
mysharesmb1 ✓

User details

Allow only read operations

All privilege local user Create new Use existing
user01 ✓

Create



If you check allow only read operations for this share data, you can specify read-only users.

- **If creating an NFS share** - You need to supply the **IP addresses of the allowed clients** that can access the share.

Add share

EdgeResource01

Share details

Name * mysharenf1

Type * ⓘ SMB NFS

Use the share with Edge compute ⓘ

Configure as Edge local share ⓘ

Storage account * ⓘ teststorageaccounttarja

Storage service * ⓘ Block Blob

Select blob container * ⓘ Create new Use existing
mysharenf1

User details

Allow only read operations ⓘ

Allowed client IP addresses

10.10.10.1

Enter an IP address.

- To easily access the shares from Edge compute modules, use the local mount point. Select **Use the share with Edge compute** so that the share is automatically mounted after it's created. When this option is selected, the Edge module can also use the compute with the local mount point.
- Select **Create** to create the share. You're notified that the share creation is in progress. After the share is created with the specified settings, the **Shares** blade updates to reflect the new share.

Add a local share

- In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. Select **+ Add share** on the command bar.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares myasetest

Search (Ctrl+/
+) Add share

Overview

Name	Status	Type	Used for compute	Storage account	Storage service
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

Shares

Storage accounts

Users

Bandwidth

2. In **Add Share**, specify the share settings. Provide a unique name for your share.

Share names can only contain numbers, lowercase and uppercase letters, and hyphens. The share name must be between 3 and 63 characters long and begin with a letter or a number. Each hyphen must be preceded and followed by a non-hyphen character.

3. Select a **Type** for the share. The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients. Depending upon whether you choose SMB or NFS shares, options presented are slightly different.

IMPORTANT

Make sure that the Azure Storage account that you use doesn't have immutability policies set on it if you're using it with a Azure Stack Edge Pro or Data Box Gateway device. For more information, see [Set and manage immutability policies for blob storage](#).

4. To easily access the shares from Edge compute modules, use the local mount point. Select **Use the share with Edge compute** so that the Edge module can use the compute with the local mount point.
5. Select **Configure as Edge local shares**. The data in local shares will stay locally on the device. You can process this data locally.
6. In the **All privilege local user** field, choose from **Create new** or **Use existing**.
7. Select **Create**.

Add share

X

myasetest

Share details

Name *

mysharelocal1



Type * ⓘ

SMB

NFS

Use the share with Edge compute



Configure as Edge local share ⓘ



Use an Edge local share to process data prior to upload to the cloud. Data in local shares stays on the device.

User details

All privilege local user ⓘ

Create new

Use existing

Admin



Create

You see a notification that the share creation is in progress. After the share is created with the specified settings, the **Shares** blade updates to reflect the new share.

Cloud storage gateway Shares						
Overview		Name	Status	Type	Used for compute	Storage account
<input checked="" type="checkbox"/>	Shares	mysharelocal1	OK	SMB	Enabled	-
<input type="checkbox"/>	Storage accounts	mysmb-cloudshare	OK	SMB	Disabled	mynewsa1 Block Blob
<input type="checkbox"/>	Users	mysmb-localshare	OK	SMB	Disabled	-

Select the share to view the local mountpoint for the Edge compute modules for this share.

mysharelocal1

EdgeResource01

Save Discard Refresh data Sync storage keys Mount Unmount Delete

This share stores data locally and won't be pushing data to cloud. Some cloud functionalities are disabled. Ensure you delete the data post processing to avoid running out of capacity.

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Local mount point for Edge compute modules	/mysharelocal1
Select users	user01

Mount a share

If you created a share before you configured compute on your Azure Stack Edge Pro device, you'll need to mount the share. Take the following steps to mount a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. From the list of the shares, select the share you want to mount. The **Used for compute** column will show the status as **Disabled** for the selected share.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares

myasetest

Search (Ctrl+ /) Add share Refresh

Overview Shares Storage accounts Users Bandwidth

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

2. Select **Mount**.

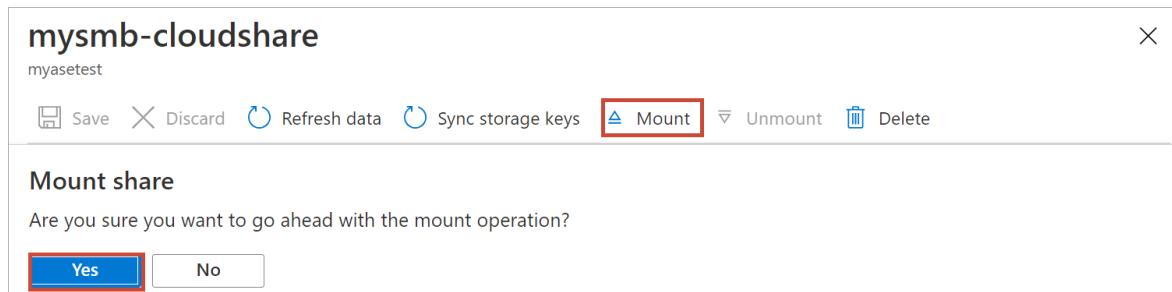
mysmb-cloudshare

myasetest

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Status	OK
Type	SMB
Mounted (Used for compute)	Disabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Select users	Admin

3. When prompted for confirmation, select **Yes**. This will mount the share.



4. After the share is mounted, go to the list of shares. You'll see that the **Used for compute** column shows the share status as **Enabled**.

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

5. Select the share again to view the local mountpoint for the share. Edge compute module uses this local mountpoint for the share.

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Local mount point for Edge compute modules	/home/databox-edge/hostgatewayshares/mysmb-cloudshare
Select users	Admin

Unmount a share

Do the following steps in the Azure portal to unmount a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. From the list of the shares, select the share that you want to unmount. You want to make sure that the share you unmount isn't used by any modules. If the share is used by a module, then you'll see issues with the corresponding module.

Cloud storage gateway | Shares

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

2. Select **Unmount**.

mysmb-cloudshare

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Local mount point for Edge compute modules	/home/databox-edge/hostgatewayshares/mysmb-cloudshare
Select users	Admin

3. When prompted for confirmation, select **Yes**. This will unmount the share.

mysmb-cloudshare

Unmount share

Ensure that the share isn't used by a module. If the share is in use, you will see issues with the module. Are you sure you want to unmount the share?

4. After the share is unmounted, go to the list of shares. You'll see that **Used for compute** column shows the share status as **Disabled**.

The screenshot shows the 'Shares' section of the Cloud storage gateway. The left sidebar has 'Shares' selected. The main table lists three shares:

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

Delete a share

Use the following steps in the Azure portal to delete a share.

- From the list of shares, select and click the share that you want to delete.

The screenshot shows the 'Shares' section of the Cloud storage gateway. The left sidebar has 'Shares' selected. The main table lists three shares:

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

- Select **Delete**.

The screenshot shows the details for the 'mysharelocal1' share. The top bar includes 'Save', 'Discard', 'Refresh data', 'Sync storage keys', 'Mount', 'Unmount', and a red-highlighted 'Delete' button.

Delete share
Ensure that the share isn't being used by any modules. If the share is in-use, you will see issues with the module. This does not remove the data residing in your storage account. Delete this data from your storage account to avoid charges. Are you sure you want to delete the share?

Yes **No**

- When prompted for confirmation, select **Yes**.

The screenshot shows the details for the 'mydbesmblocal2' share. The top bar includes 'Save', 'Discard', 'Refresh data', 'Sync storage keys', 'Mount', 'Unmount', and a red-highlighted 'Delete' button.

Delete share
Ensure that the share isn't being used by any modules. If the share is in-use, you will see issues with the module. This does not remove the data residing in your storage account. Delete this data from your storage account to avoid charges. Are you sure you want to delete the share?

Yes **No**

The list of shares updates to reflect the deletion.

Refresh shares

The refresh feature allows you to refresh the contents of a share. When you refresh a share, a search is initiated to find all the Azure objects including blobs and files that were added to the cloud since the last refresh. These

additional files are then downloaded to refresh the contents of the share on the device.

IMPORTANT

- You can't refresh local shares.
- Permissions and access control lists (ACLs) aren't preserved across a refresh operation.

Do the following steps in the Azure portal to refresh a share.

1. In the Azure portal, go to **Shares**. Select and click the share that you want to refresh.

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

2. Select Refresh.

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	teststorageaccounttarja
Storage account container	mysharesmb1
Last updated time	12/12/2019, 11:31:50
Last update error logs	teststorageaccounttarja\mysharesmb1__Microsoft Data Box Edge_\Refresh\Errors.xml
Local mount point for Edge compute modules	/home/hcsshares/mysharesmb1
Select users	user01

3. When prompted for confirmation, select **Yes**. A job starts to refresh the contents of the on-premises share.

Refresh Edge share

This action finds objects in Azure storage that were last added, modified, and removed from the on-premises share. The metadata for these objects is refreshed. Are you sure you want to refresh the share metadata?

Yes No

4. While the refresh is in progress, the refresh option is grayed out in the context menu. Select the job

notification to view the refresh job status.

5. The time to refresh depends on the number of files in the Azure container and the files on the device.

Once the refresh has successfully completed, the share timestamp is updated. Even if the refresh has partial failures, the operation is considered successful and the timestamp is updated. The refresh error logs are also updated.

The screenshot shows the Azure portal interface for a storage account named 'mydbesmb1'. At the top, there are several action buttons: Save, Discard, Refresh data, Sync storage keys, Mount, Unmount, and Delete. Below these, a table provides details about the storage account:

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mytests1
Storage account container name	mydbesmb1
Last refresh time	3/12/2019, 09:01:06
Last refresh error logs	mytests1\mydbesmb1__Microsoft Data Box Edge_\Refresh\Errors.xml
Local mount point for Edge compute modules	/home/hcsshares/mydbesmb1
Select users	Admin1

If there's a failure, an alert is raised. The alert details the cause and the recommendation to fix the issue. The alert also links to a file that has the complete summary of the failures including the files that failed to update or delete.

Sync pinned files

To automatically sync up pinned files, do the following steps in the Azure portal:

1. Select an existing Azure storage account.
2. Go to **Containers** and select **+ Container** to create a container. Name this container as *newcontainer*. Set the **Public access level** to Container.

The screenshot shows the Azure portal interface for a container named 'newcontainer'. The left sidebar lists various settings: Overview, Access Control (IAM), Settings, Access policy, Properties, **Metadata** (which is highlighted with a red box), and Editor (preview).

3. Select the container name and set the following metadata:

- Name = "Pinned"
- Value = "True"

The screenshot shows the 'Metadata' tab for a container named 'newcontainer'. The table contains one row with the key 'Pinned' and value 'True'. The entire row is highlighted with a red border.

key	value
Pinned	True

4. Create a new share on your device. Map it to the pinned container by choosing the existing container option. Mark the share as read only. Create a new user and specify the user name and a corresponding password for this share.

Add share

X

myasetest

Share details

Name * ✓

Type * ⓘ SMB NFS

Use the share with Edge compute ⓘ

Configure as Edge local share ⓘ

Storage account * ⓘ ▼

Storage service * ⓘ ▼

Select blob container * ⓘ Create new Use existing

▼

User details

Allow only read operations ⓘ

All privilege local user ⓘ Create new Use existing

User name *

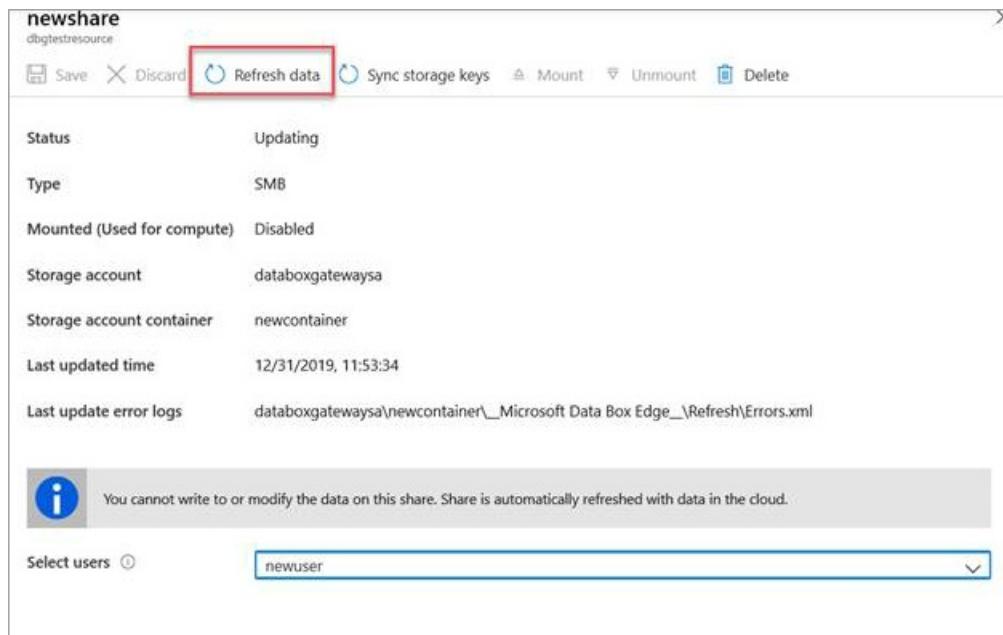
Password *

Confirm password *

Create

5. From the Azure portal, browse to the container that you created. Upload the file that you want to be pinned into the new container, that has the metadata set to pinned.

6. Select **Refresh data** in Azure portal for the device to download the pinning policy for that particular Azure Storage container.



- Access the new share that was created on the device. The file that was uploaded to the storage account is now downloaded to the local share.

Anytime the device is disconnected or reconnected, it triggers refresh. Refresh will bring down only those files that have changed.

Sync storage keys

If your storage account keys have been rotated, then you need to sync the storage access keys. The sync helps the device get the latest keys for your storage account.

Do the following steps in the Azure portal to sync your storage access key.

- Go to **Overview** in your resource. From the list of shares, select a share associated with the storage account that you need to sync.

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

- Select **Sync storage key**. Select **Yes** when prompted for confirmation.

- Exit out of the dialog once the sync is complete.

NOTE

You only have to do this once for a given storage account. You don't need to repeat this action for all the shares associated with the same storage account.

Next steps

- Learn how to [Manage users via Azure portal](#).

Use the Azure portal to manage users on your Azure Stack Edge Pro

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to manage users on your Azure Stack Edge Pro. You can manage the Azure Stack Edge Pro via the Azure portal or via the local web UI. Use the Azure portal to add, modify, or delete users.

In this article, you learn how to:

- Add a user
- Modify user
- Delete a user

About users

Users can be read-only or full privilege. Read-only users can only view the share data. Full privilege users can read share data, write to these shares, and modify or delete the share data.

- **Full privilege user** - A local user with full access.
- **Read-only user** - A local user with read-only access. These users are associated with shares that allow read-only operations.

The user permissions are first defined when the user is created during share creation. They can be modified by using File Explorer.

Add a user

Do the following steps in the Azure portal to add a user.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Users**. Select **+ Add user** on the command bar.

User name	Associated shares	⋮
Admin	mysharelocal1, mysmb-cloudshare, mysmb-localshare	⋮

2. Specify the username and password for the user you want to add. Confirm the password and select **Add**.

Add user

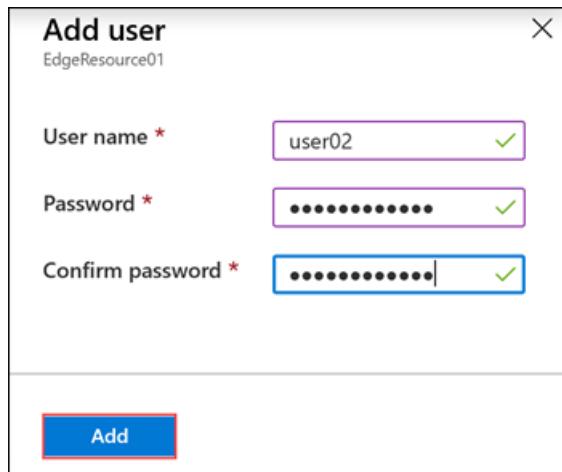
EdgeResource01

User name * ✓

Password * ✓

Confirm password * ✓

Add



IMPORTANT

These users are reserved by the system and should not be used: Administrator, EdgeUser, EdgeSupport, HcsSetupUser, WDAGUtilityAccount, CLIUSR, DefaultAccount, Guest.

3. A notification is shown when the user creation starts and is completed. After the user is created, from the command bar, select **Refresh** to view the updated list of users.

Modify user

You can change the password associated with a user once the user is created. Select from the list of users. Enter and confirm the new password. Save the changes.

Modify user

EdgeResource01

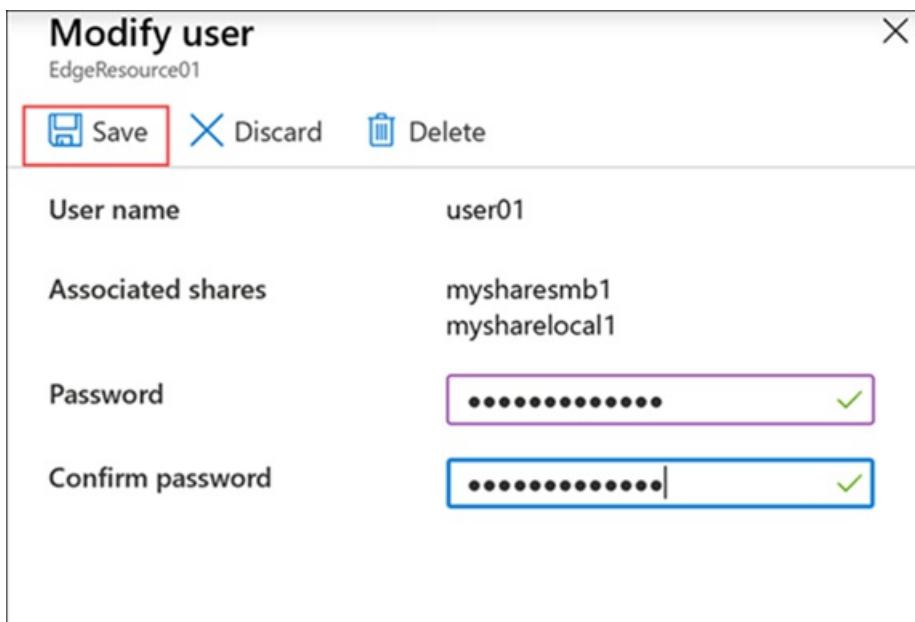
Save **Discard** **Delete**

User name user01

Associated shares mysharesmb1
mysharelocal1

Password ✓

Confirm password ✓



Delete a user

Do the following steps in the Azure portal to delete a user.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Users**.

The screenshot shows the 'Cloud storage gateway | Users' page. On the left, there's a sidebar with links: Overview, Shares, Storage accounts, and Users (which is selected and highlighted with a red box). The main area has a search bar, an 'Add user' button, and a 'Refresh' button. A filter bar allows you to search by 'User name'. Below is a table with columns 'User name' and 'Associated shares'. It shows two entries: 'Admin' associated with 'mysharelocal1, mysmb-cloudshare, mysmb-localshare' and 'user01' associated with '-'. There are three-dot menus next to each entry.

2. Select a user from the list of users and then select **Delete**. When prompted, confirm the deletion.

The screenshot shows the 'Modify user' dialog for 'user01'. At the top, there are 'Save' and 'Discard' buttons, and a 'Delete' button which is highlighted with a red box. The main part of the dialog shows the user's details: 'User name' is 'user01', and 'Associated shares' are 'mysharesmb1' and 'mysharelocal1'. Below these, there are fields for 'Password' and 'Confirm password', both of which are masked with dots. A large red box surrounds the entire content area of the dialog.

The list of users is updated to reflect the deleted user.

The screenshot shows the 'Cloud storage gateway | Users' page again. The sidebar and search/filter options are identical to the first screenshot. The main table now only shows one entry: 'Admin' associated with 'mysharelocal1, mysmb-cloudshare, mysmb-localshare'. This entry is highlighted with a red box.

Next steps

- Learn how to [Manage bandwidth](#).

Use the Azure portal to manage Edge storage accounts on your Azure Stack Edge Pro GPU

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

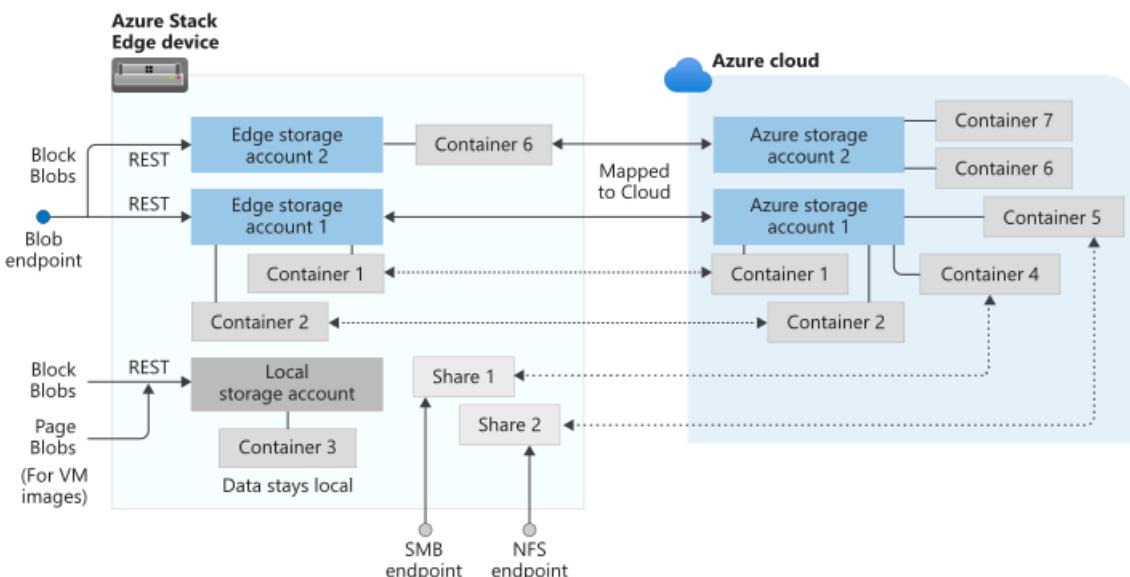
This article describes how to manage Edge storage accounts and local storage accounts on your Azure Stack Edge. You can manage the Azure Stack Edge Pro device via the Azure portal or via the local web UI. Use the Azure portal to add or delete Edge storage accounts on your device. Use Azure PowerShell to add local storage accounts on your device.

About Edge storage accounts

You can transfer data from your Azure Stack Edge Pro GPU device via the SMB, NFS, or REST protocols. To transfer data to Blob storage using the REST APIs, you need to create Edge storage accounts on your device.

The Edge storage accounts that you add on the Azure Stack Edge Pro GPU device are mapped to Azure Storage accounts. Any data written to the Edge storage accounts is automatically pushed to the cloud.

A diagram detailing the two types of accounts and how the data flows from each of these accounts to Azure is shown below:



In this article, you learn how to:

- Add an Edge storage account
- Delete an Edge storage account

Add an Edge storage account

To create an Edge storage account, do the following procedure:

1. In the [Azure portal](#), select your Azure Stack Edge resource and then go to the **Overview**. Your device should be online. Go to **Cloud storage gateway > Storage accounts**.
2. Select **+ Add storage account** on the device command bar.

The screenshot shows the 'Cloud storage gateway | Overview' page for a device named 'myasetest'. The left sidebar has links for Overview, Shares, Storage accounts, Users, and Bandwidth. The main area displays 'Edge shares' with a total of 3, showing two entries: 'mysharelocal1' and 'mysmb-cloudshare', both marked as 'OK'. A red box highlights the 'Add storage account' button in the top navigation bar.

3. In the **Add Edge storage account** pane, specify the following settings:
 - a. Provide a unique name for the Edge storage account on your device. Storage account names can only contain lowercase numbers and letters. Special characters are not allowed. Storage account name has to be unique within the device (not across the devices).
 - b. Provide an optional description for the information on the data the storage account is holding.
 - c. By default, the Edge storage account is mapped to an Azure Storage account in the cloud, and the data from the storage account is automatically pushed to the cloud. Specify the Azure storage account that your Edge storage account is mapped to.
 - d. Create a new container, or select from an existing container in the Azure storage account. Any data from the device that is written to the Edge storage account is automatically uploaded to the selected storage container in the mapped Azure Storage account.
 - e. After all the storage account options are specified, select **Add** to create the Edge storage account. You are notified when the Edge storage account is successfully created. The new Edge storage account is then displayed in the list of storage accounts in the Azure portal.
4. If you select this new storage account and go to **Access keys**, you can find the blob service endpoint and the corresponding storage account name. Copy this information as these values together with the access keys will help you connect to the Edge storage account.

The screenshot shows the 'Access keys' page for the storage account 'myasetiered1'. The left sidebar has links for Overview, Settings, and Access keys. The main area displays the 'Blob service endpoint' as 'https://myasetiered1.blob.dbe-1dcnq2.wdshcsso.com' and the 'Edge storage account name' as 'myasetiered1'. A red box highlights the 'Access keys' link in the sidebar and the 'Blob service endpoint' and 'Edge storage account name' fields.

You get the access keys by [Connecting to the device local APIs using Azure Resource Manager](#).

Create a local storage account

Create a new local storage account by using an existing resource group. Use this local storage account to upload the virtual disk image when creating a VM.

Before you create a local storage account, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

- [Az](#)
- [AzureRM](#)

1. Set some parameters.

```
$StorageAccountName = "<Storage account name>"
```

2. Create a new local storage account on your device.

```
New-AzStorageAccount -Name $StorageAccountName -ResourceGroupName $ResourceGroupName -Location  
DBELocal -SkuName Standard_LRS
```

NOTE

By using Azure Resource Manager, you can create only local storage accounts, such as locally redundant storage (standard or premium). To create tiered storage accounts, see [Tutorial: Transfer data via storage accounts with Azure Stack Edge Pro with GPU](#).

Here's an example output:

```
PS C:\WINDOWS\system32> New-AzStorageAccount -Name myaseazsa -ResourceGroupName myaseazrg -Location  
DBELocal -SkuName Standard_LRS

StorageAccountName ResourceGroupName PrimaryLocation SkuName      Kind      AccessTier CreationTime  
----- ----- ----- -----  
myaseazsa        myaseazrg       DBELocal     Standard_LRS Storage      6/10/2021  
11:45...

PS C:\WINDOWS\system32>
```

Get access keys for a local storage account

Before you get the access keys, you must configure your client to connect to the device via Azure Resource Manager over Azure PowerShell. For detailed instructions, see [Connect to Azure Resource Manager on your Azure Stack Edge device](#).

To get the access keys for an existing local storage account that you have created, provide the associated resource group name and the local storage account name.

- [Az](#)
- [AzureRM](#)

```
Get-AzStorageAccountKey
```

Here's an example output:

```
PS C:\WINDOWS\system32> Get-AzStorageAccountKey
```

```
cmdlet Get-AzStorageAccountKey at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ResourceGroupName: myaseazrg
Name: myaseazsa
```

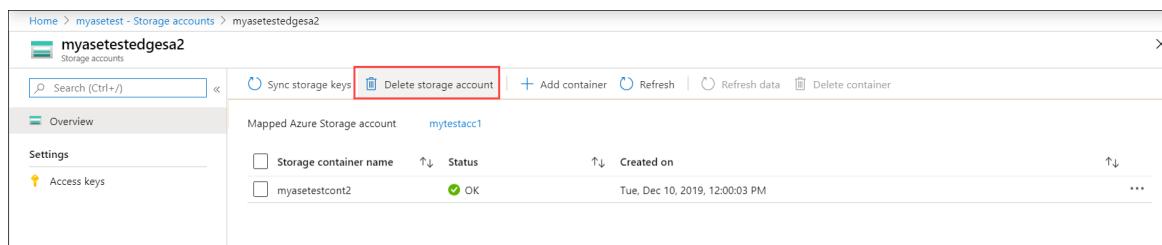
KeyName	Value	Permissions
key1	gv30F57tuPDyzBNc1M7fhil2UAiiwnhTT6zgiwE3T1F/CD217Cvw2YCPcrKF47joNKRvzp44leUe5HtVkJx8RQ==	Full
key2	kmEynIs3xnpmsXwbu41h5a7DZD7v4gGV3yXa2NbPbmhrPt10+QmE5PkOxxypeSqbqzd9si+ArNvbsqIRuLH2Lw==	Full

```
PS C:\WINDOWS\system32>
```

Delete an Edge storage account

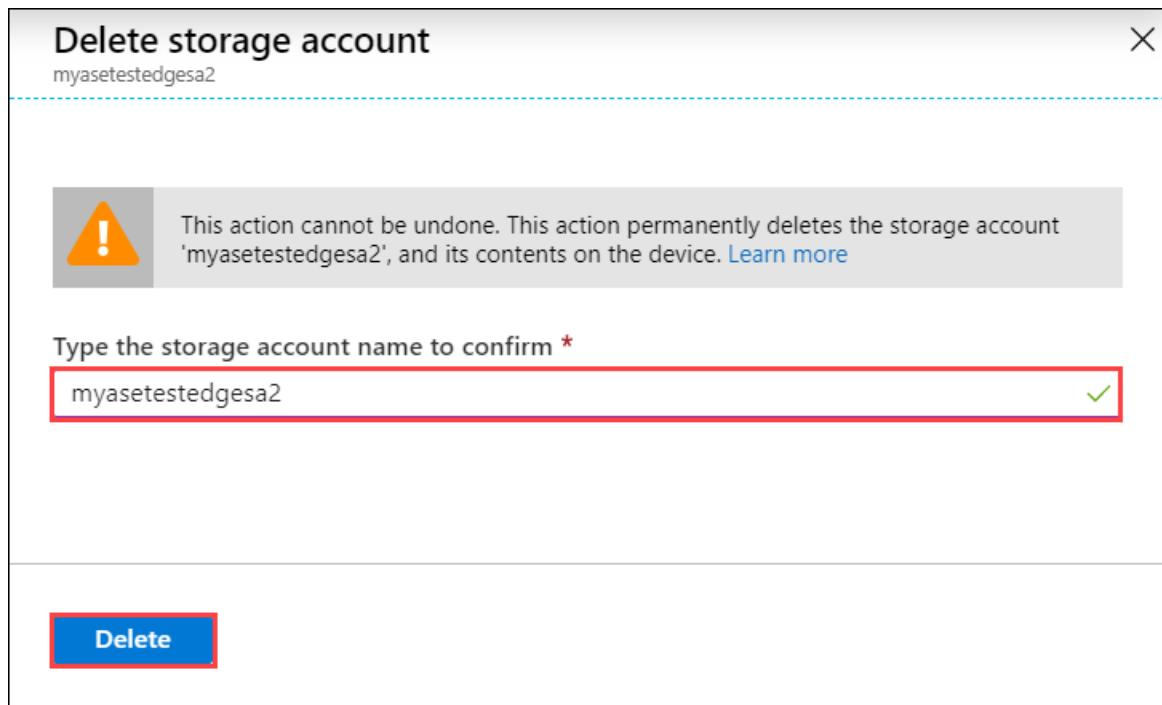
Take the following steps to delete an Edge storage account.

1. Go to **Configuration > Storage accounts** in your resource. From the list of storage accounts, select the storage account you want to delete. From the top command bar, select **Delete storage account**.



The screenshot shows the Azure portal interface for managing storage accounts. The left sidebar shows 'myasetestedgesa2' under 'Storage accounts'. The main area displays a table of storage accounts. One row is selected, showing 'mytestacc1' as the mapped Azure Storage account. A red box highlights the 'Delete storage account' button in the top right of the table header. Other buttons visible include 'Sync storage keys', 'Add container', 'Refresh', 'Refresh data', and 'Delete container'.

2. In the **Delete storage account** blade, confirm the storage account to delete and select **Delete**.



The screenshot shows the 'Delete storage account' confirmation dialog. At the top, it says 'Delete storage account' and 'myasetestedgesa2'. Below that is a warning message: 'This action cannot be undone. This action permanently deletes the storage account 'myasetestedgesa2', and its contents on the device.' A 'Learn more' link is provided. A red box highlights the input field where 'myasetestedgesa2' is typed to confirm the deletion. A green checkmark icon is to the right of the input field. At the bottom is a large blue 'Delete' button with a red border.

The list of storage accounts is updated to reflect the deletion.

Add, delete a container

You can also add or delete the containers for these storage accounts.

To add a container, take the following steps:

1. Select the storage account that you want to manage. From the top command bar, select **+ Add container**.

The screenshot shows the Azure Storage Accounts Overview page for the storage account 'myasetestedgesa2'. The top navigation bar includes 'Home > All resources > myasetest - Storage accounts > myasetestedgesa2'. Below the navigation is a search bar and a toolbar with 'Sync storage keys', 'Delete storage account', '+ Add container' (which is highlighted with a red box), 'Refresh', 'Refresh data', and 'Delete container'. The left sidebar has 'Overview' selected (highlighted with a red box) and 'Settings' with 'Access keys'. The main area shows a table for 'Mapped Azure Storage account testedgesa' with columns 'Storage container name', 'Status', and 'Created on'. Two containers are listed: 'myasetestcont2' (status OK, created on Tue, Dec 10, 2019, 4:34:18 PM) and 'myasetestcont3' (status OK, created on Tue, Dec 10, 2019, 4:38:23 PM). A 'More' button is at the bottom right of the table.

2. Provide a name for your container. This container is created in your Edge storage account as well as the Azure storage account mapped to this account.

The screenshot shows the 'Add Edge storage container' dialog box. At the top, it says 'Add Edge storage container' and 'myasetestedgesa2'. Below that is a note: 'Create or select an existing container in the Azure Storage account that is mapped to your storage account on this device. [Learn more](#)'. There are two radio buttons: 'Azure storage container' (with a help icon) and 'Create new' (which is selected and highlighted with a red box). Below that is a 'Container name *' field containing 'myasetestcont3' (which is also highlighted with a red box). At the bottom is a large blue 'Add' button (highlighted with a red box).

The list of containers is updated to reflect the newly added container.

The screenshot shows the Azure Storage Accounts Overview page for the storage account 'myasetestedgesa2'. The top navigation bar and sidebar are identical to the previous screenshot. The main area shows the updated table for 'Mapped Azure Storage account testedgesa'. Now, there are three rows: 'myasetestcont2' (status OK, created on Tue, Dec 10, 2019, 4:34:18 PM) and 'myasetestcont3' (status OK, created on Tue, Dec 10, 2019, 4:38:23 PM), both of which are highlighted with red boxes.

You can now select a container from this list and select **+ Delete container** from the top command bar.

Storage container name Status Created on

myasetestcont2	OK	Tue, Dec 10, 2019, 4:34:18 PM
myasetestcont3	OK	Tue, Dec 10, 2019, 4:38:23 PM

Sync storage keys

Each Azure Storage account has two 512-bit storage access keys that are used for authentication when the storage account is accessed. One of these two keys must be supplied when your Azure Stack Edge device accesses your cloud storage service provider (in this case, Azure).

An Azure administrator can regenerate or change the access key by directly accessing the storage account (via the Azure Storage service). The Azure Stack Edge service and the device do not see this change automatically.

To inform Azure Stack Edge of the change, you will need to access the Azure Stack Edge service, access the storage account, and then synchronize the access key. The service then gets the latest key, encrypts the keys, and sends the encrypted key to the device. When the device gets the new key, it can continue to transfer data to the Azure Storage account.

To provide the new keys to the device, access the Azure portal and synchronize storage access keys. Take the following steps:

1. In your resource, select the storage account that you want to manage. From the top command bar, select **Sync storage key**.

Sync storage keys

2. When prompted for confirmation, select **Yes**.

Synchronize storage account keys
This action updates the access keys for the storage account attached to your device. Are you sure you want to synchronize the keys?

Yes No

Next steps

- Learn how to [Manage users via Azure portal](#).

Use the Azure portal to manage bandwidth schedules on your Azure Stack Edge Pro GPU

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to manage bandwidth schedules on your Azure Stack Edge Pro. Bandwidth schedules allow you to configure network bandwidth usage across multiple time-of-day schedules. These schedules can be applied to the upload and download operations from your device to the cloud.

You can add, modify, or delete the bandwidth schedules for your Azure Stack Edge Pro via the Azure portal.

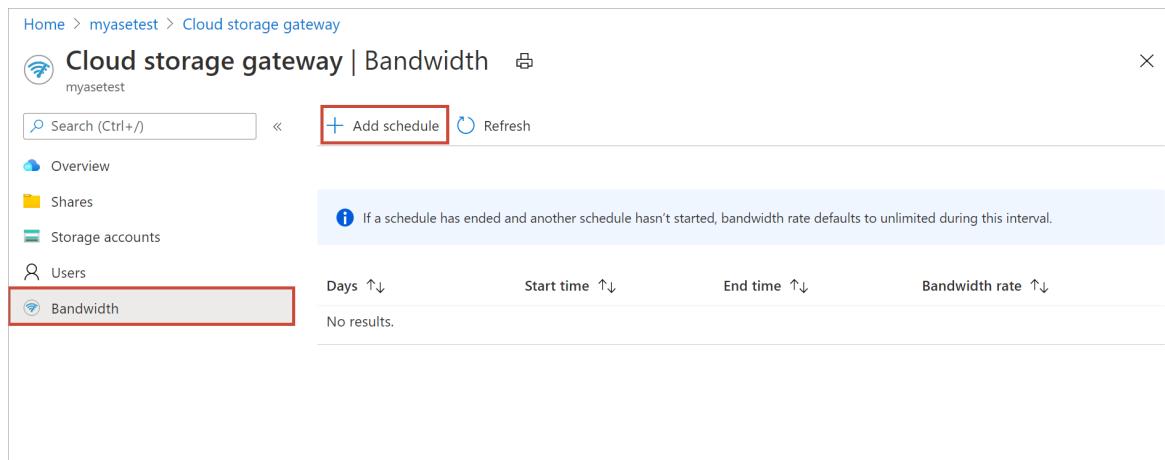
In this article, you learn how to:

- Add a schedule
- Modify schedule
- Delete a schedule

Add a schedule

Do the following steps in the Azure portal to add a schedule.

1. In the Azure portal for your Azure Stack Edge resource, go to **Bandwidth**.
2. In the right-pane, select **+ Add schedule**.



3. In the **Add schedule**:
 - a. Provide the **Start day**, **End day**, **Start time**, and **End time** of the schedule.
 - b. Check the **All day** option if this schedule should run all day.
 - c. **Bandwidth rate** is the bandwidth in Megabits per second (Mbps) used by your device in operations involving the cloud (both uploads and downloads). Supply a number between 64 and 2,147,483,647 for this field.
 - d. Select **Unlimited bandwidth** if you do not want to throttle the date upload and download.
 - e. Select **Add**.

Add schedule

myasetest

Start day *	Monday
End day *	Friday
Daily recurrence pattern	
All day	<input type="checkbox"/>
Start time *	8:00 AM
End time *	6:00 PM
Bandwidth configuration	
Unlimited bandwidth ⓘ	<input type="checkbox"/>
Bandwidth rate (Mbps) ⓘ	64 ✓
Add	

4. A schedule is created with the specified parameters. This schedule is then displayed in the list of bandwidth schedules in the portal.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Bandwidth

If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Days ↑↓	Start time ↑↓	End time ↑↓	Bandwidth rate ↑↓
Monday, Tuesday, Wednesday...	08:00:00	18:00:00	64 (Mbps)

Edit schedule

Do the following steps to edit a bandwidth schedule.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Bandwidth**.
2. From the list of bandwidth schedules, select a schedule that you want to modify.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Bandwidth

myasetest

Search (Ctrl+ /) <> + Add schedule Refresh

Overview Shares Storage accounts Users Bandwidth

If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Days	Start time	End time	Bandwidth rate
Monday, Tuesday, Wednesday...	08:00:00	18:00:00	64 (Mbps)

3. Make the desired changes and save the changes.

Edit schedule

myasetest

Save Discard Delete

Start day * Monday

End day * Friday

Daily recurrence pattern

All day

Start time * 8:00 AM

End time * 5:00 PM

Bandwidth configuration

Unlimited bandwidth

Bandwidth rate (Mbps) 64

4. After the schedule is modified, the list of schedules is updated to reflect the modified schedule.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Bandwidth

myasetest

Search (Ctrl+ /) <> + Add schedule Refresh

Overview Shares Storage accounts Users Bandwidth

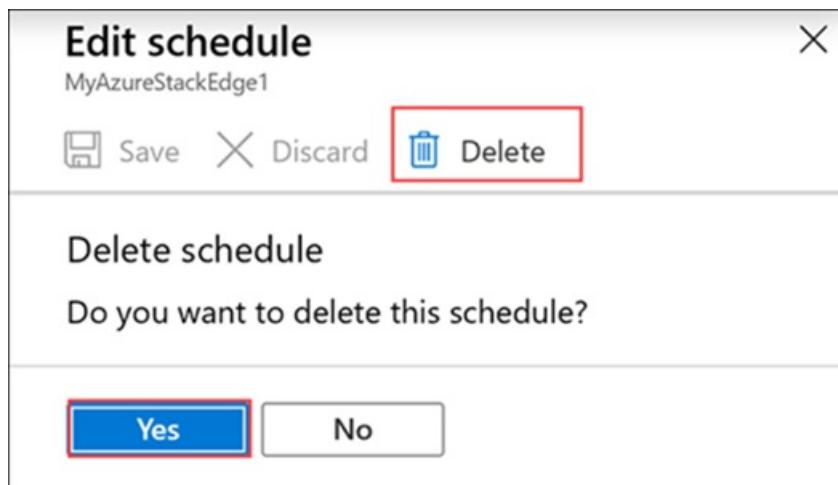
If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Days	Start time	End time	Bandwidth rate
Monday, Tuesday, Wednesday...	08:00:00	17:00:00	64 (Mbps)

Delete a schedule

Do the following steps to delete a bandwidth schedule associated with your Azure Stack Edge Pro device.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Bandwidth**.
2. From the list of bandwidth schedules, select a schedule that you want to delete. In the **Edit schedule**, select **Delete**. When prompted for confirmation, select **Yes**.



3. After the schedule is deleted, the list of schedules is updated.

Next steps

- Learn how to [Manage shares](#).

Troubleshoot Blob storage issues for an Azure Stack Edge device

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to troubleshoot issues with Blob storage for your Azure Stack Edge device.

Errors for Blob storage on device

Here are the errors related to Blob storage for an Azure Stack Edge device.

ISSUE / ERRORS	RESOLUTION
Unable to retrieve child resources. The value for one of the HTTP headers is not in the correct format. <pre>getaddrinfo ENOTFOUND <accountname>.blob.<serialnumber>.microsoftdatabox.com</pre>	From the Edit menu, select Target Azure Stack APIs . Then, restart Azure Storage Explorer.
Unable to retrieve child resources. Details: self-signed certificate <pre>Failed to enumerate directory https://... The remote name could not be resolved <accountname>.blob.<serialnumber>.microsoftdatabox.com</pre>	Check that the endpoint name <code><accountname>.blob.<serialnumber>.microsoftdatabox.com</code> is added to the hosts file at this path, <code>C:\Windows\System32\drivers\etc\hosts</code> , on Windows, or at <code>/etc/hosts</code> on Linux.
AzCopy command appears to stop responding for a minute before displaying this error: <pre>Error parsing source location. The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel</pre>	Import the SSL certificate for your device into Azure Storage Explorer: <ol style="list-style-type: none">Generate and download the certificate.From the Edit menu, select SSL Certificates and then select Import Certificates.
AzCopy command appears to stop responding for a minute before displaying this error: <pre>azcopy: error: unrecognized argument: https://<accountname>.blob.<serialnumber>.microsoftdatabox.com</pre>	Check that the endpoint name <code><accountname>.blob.<serialnumber>.microsoftdatabox.com</code> is added to the hosts file at: <code>C:\Windows\System32\drivers\etc\hosts</code> .
AzCopy command appears to stop responding for 20 minutes before displaying this error: <pre>Error parsing source location https://<accountname>.blob.<serialnumber>.microsoftdatabox.com/<cntnr>. No such device or address</pre>	Import the SSL certificate for your device into Azure Storage Explorer: <ol style="list-style-type: none">Generate and download the certificate.From the Edit menu, select SSL Certificates and then select Import Certificates.
AzCopy command appears to stop responding for 20 minutes before displaying this error: <pre>Error parsing source location https://<accountname>.blob.<serialnumber>.microsoftdatabox.com/<cntnr>. No such device or address</pre>	Check that the endpoint name <code><accountname>.blob.<serialnumber>.microsoftdatabox.com</code> is added to the hosts file at: <code>/etc/hosts</code> .

ISSUE / ERRORS	RESOLUTION
<p>AzCopy command appears to stop responding for 20 minutes before displaying this error:</p> <pre data-bbox="176 233 742 287">Error parsing source location... The SSL connection could not be established</pre>	<p>Import the SSL certificate for your device into Azure Storage Explorer:</p> <ol style="list-style-type: none"> 1. Generate and download the certificate. 2. From the Edit menu, select SSL Certificates and then select Import Certificates.
<p>AzCopy command appears to stop responding for 20 minutes before displaying this error:</p> <pre data-bbox="176 473 720 579">Error parsing source location https://<accountname>.blob.<serialnumber>.microsoftdatabox.com/<cntnr>. No such device or address</pre>	<p>Check that the endpoint name <code><accountname>.blob.<serialnumber>.microsoftdatabox.com</code> is added to the hosts file at: <code>/etc/hosts</code>.</p>
<p>AzCopy command appears to stop responding for 20 minutes before displaying this error:</p> <pre data-bbox="176 705 742 759">Error parsing source location... The SSL connection could not be established</pre>	<p>Import the SSL certificate for your device into the system's certificate store. For more information, see Download the certificate.</p>
<p>The value for one of the HTTP headers is not in the correct format.</p>	<p>The installed version of the Microsoft Azure Storage Library for Python is not supported by Azure Stack Edge. For supported library versions, see Supported Azure client libraries.</p>
<p>... [SSL: CERTIFICATE_VERIFY_FAILED] ...</p>	<p>Before running Python, set the <code>REQUESTS_CA_BUNDLE</code> environment variable to the path of the Base64-encoded SSL certificate file (see how to Download the certificate). For example, run:</p> <pre data-bbox="814 1136 1288 1208">export REQUESTS_CA_BUNDLE=/tmp/mycert.cer python</pre> <p>Alternately, add the certificate to the system's certificate store, and then set this environment variable to the path of that store. For example, on Ubuntu, run:</p> <pre data-bbox="814 1304 1320 1399">export REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca-certificates.crt python</pre>
<p>The connection times out.</p>	<p>Sign in on your device, and then check whether it's unlocked. Anytime the device restarts, it stays locked until someone signs in.</p>
<p>Could not create or update storageaccount. Ensure that the access key for your storage account is valid. If needed, update the key on the device.</p>	<p>Sync the storage account keys. Follow the steps outlined here.</p>

Next steps

- [Troubleshoot device upload and refresh errors.](#)

Choosing a region for Azure Stack Edge

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R Azure Stack Edge Mini R Azure Stack Edge Pro - FPGA

This article describes region availability for the Azure Stack Edge service, data storage, and device shipments for an Azure Stack Edge device, and explains how your choice of regions affects service, performance, and billings.

Overview

The Azure datacenters operate in multiple geographic regions around the world to meet customers' demands of performance, requirements, and preferences for data location. An Azure geography is a defined area of the world that contains at least one Azure region. An Azure region is an area within a geography, containing one or more datacenters.

Choosing an Azure region is very important, and the choice of region is influenced by factors such as data residency and sovereignty, service availability, performance, cost, and redundancy. For more information on how to choose a region, go to [Which Azure region is right for me?](#).

For an Azure Stack Edge Pro GPU device, the choice of region is determined by the following factors:

- Regions where the Azure Stack Edge service is available.
- Regions where the storage accounts that store Azure Stack Edge data should be located for the best performance.
- Countries/regions that the Azure Stack Edge device can be shipped to.

Region availability for the service

The Azure Stack Edge service is currently supported in the US East, West Europe, and SE Asia public regions. **These three regions support geographic locations worldwide.**

The region of the service is the country or region assigned to the Azure Stack Edge management resource. The management resource uses the Azure Stack Edge service to activate, deploy, and return an Azure Stack Edge device.

The Azure Stack Edge service also monitors the health of the device - issues, errors, alerts, and whether the device is "alive". And the service monitors usage and consumption meters for billing - the control plane information on the device. The region assigned to the management resource is the region where billings occur.

The device must connect to the Azure Stack Edge service to activate. If you don't want any further interaction with the service, you can switch the device to disconnected mode.

Data doesn't flow through the Azure Stack Edge service. Data flows between the device and the storage account that is deployed in the customer's region of data origin.

In general, a location closest to the geographical region where the device is deployed is chosen. But the device and the service can also be deployed in different locations.

Region availability for data storage

Azure Stack Edge data is stored in Azure storage accounts, and these accounts are available in all the Azure regions. When you create an Azure storage account, you choose the primary location of the storage account.

That choice determines the region where the data resides.

You choose a storage account when you [create a share on your device](#). Your Azure Stack Edge service and Azure storage can be in two separate locations.

In general, choose the nearest region to your service for your storage account. However, the nearest Microsoft Azure region might not actually be the region with the lowest latency. The latency dictates network service performance and hence the performance of the device. So if you're choosing a storage account in a different region, it's important to know what the latencies are between your service and the region associated with your storage account.

Region of device

To find out the countries and geographic regions where Azure Stack Edge models are available, see the product overview:

- [Region availability for Azure Stack Edge Pro with GPU](#)
- [Region availability for Azure Stack Edge Pro R](#)
- [Region availability for Azure Stack Edge Mini R](#)

Microsoft can ship physical hardware and provide hardware spare parts replacement for Azure Stack Edge to those geographic regions.

IMPORTANT

Do not place an Azure Stack Edge physical device in a region where Azure Stack Edge is not supported. Microsoft will not be able to ship any replacement parts to countries/regions where Azure Stack Edge is not supported.

Next steps

- Learn more about the [pricing for various Azure Stack Edge models](#).
- [Prepare to deploy your Azure Stack Edge Pro device](#).

GPU sharing on your Azure Stack Edge Pro GPU device

9/21/2022 • 3 minutes to read • [Edit Online](#)

Graphics processing unit (GPU) is a specialized processor designed to accelerate graphics rendering. GPUs can process many pieces of data simultaneously, making them useful for machine learning, video editing, and gaming applications. In addition to CPU for general purpose compute, your Azure Stack Edge Pro GPU devices can contain one or two Nvidia Tesla T4 GPUs for compute-intensive workloads such as hardware accelerated inferencing. For more information, see [Nvidia's Tesla T4 GPU](#).

About GPU sharing

Many machine learning or other compute workloads may not need a dedicated GPU. GPUs can be shared and sharing GPUs among containerized or VM workloads helps increase the GPU utilization without significantly affecting the performance benefits of GPU.

Using GPU with VMs

On your Azure Stack Edge Pro device, a GPU can't be shared when deploying VM workloads. A GPU can only be mapped to one VM. This implies that you can only have one GPU VM on a device with one GPU and two VMs on a device that is equipped with two GPUs. There are other factors that must also be considered when using GPU VMs on a device that has Kubernetes configured for containerized workloads. For more information, see [GPU VMs and Kubernetes](#).

Using GPU with containers

If you are deploying containerized workloads, a GPU can be shared in more than one ways at the hardware and software layer. With the Tesla T4 GPU on your Azure Stack Edge Pro device, we are limited to software sharing. On your device, the following two approaches for software sharing of GPU are used:

- The first approach involves using environment variables to specify the number of GPUs that can be time shared. Consider the following caveats when using this approach:
 - You can specify one or both or no GPUs with this method. It is not possible to specify fractional usage.
 - Multiple modules can map to one GPU but the same module cannot be mapped to more than one GPU.
 - With the Nvidia SMI output, you can see the overall GPU utilization including the memory utilization.For more information, see how to [Deploy an IoT Edge module that uses GPU](#) on your device.
- The second approach requires you to enable the Multi-Process Service on your Nvidia GPUs. MPS is a runtime service that lets multiple processes using CUDA to run concurrently on a single shared GPU. MPS allows overlapping of kernel and memcpy operations from different processes on the GPU to achieve maximum utilization. For more information, see [Multi-Process Service](#).

Consider the following caveats when using this approach:

- MPS allows you to specify more flags in GPU deployment.
- You can specify fractional usage via MPS thereby limiting the usage of each application deployed on the device. You can specify the GPU percentage to use for each app under the `env` section of the `deployment.yaml` by adding the following parameter:

```
// Example: application wants to limit gpu percentage to 20%  
  
env:  
  - name: CUDA_MPS_ACTIVE_THREAD_PERCENTAGE  
    value: "20"
```

GPU utilization

When you share GPU on containerized workloads deployed on your device, you can use the Nvidia System Management Interface (nvidia-smi). Nvidia-smi is a command-line utility that helps you manage and monitor Nvidia GPU devices. For more information, see [Nvidia System Management Interface](#).

To view GPU usage, first connect to the PowerShell interface of the device. Run the `Get-HcsNvidiaSmi` command and view the Nvidia SMI output. You can also view how the GPU utilization changes by enabling MPS and then deploying multiple workloads on the device. For more information, see [Enable Multi-Process Service](#).

Next steps

- [GPU sharing for Kubernetes deployments on your Azure Stack Edge Pro](#).
- [GPU sharing for IoT deployments on your Azure Stack Edge Pro](#).

Data residency and resiliency for Azure Stack Edge

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the information that you need to help understand the data residency and resiliency behavior for Azure Stack Edge and how to enable data residency in the service.

About data residency for Azure Stack Edge

Azure Stack Edge services uses [Azure Regional Pairs](#) when storing and processing customer data in all the geos where the service is available. For the Southeast Asia (Singapore) region, the service is currently paired with Hong Kong. The Azure region pairing implies that any data stored in Singapore is replicated in Hong Kong. Singapore has laws in place that require that the customer data not leave the country boundaries.

To ensure that the customer data resides in a single region only, a new option is enabled in the Azure Stack Edge service. This option when selected, lets the service store and process the customer data only in Singapore region. The customer data is not replicated to Hong Kong. There is service-specific metadata (which is not sensitive data) that is still replicated to the paired region.

With this option enabled, the service is resilient to zone-wide outages, but not to region-wide outages. If region-wide outages are important for you, then you should select the regional pair based replication.

The single region data residency option is available only for Southeast Asia (Singapore). For all other regions, Azure Stack Edge stores and processes customer data in the customer-specified geo.

The data residency posture of the Azure Stack Edge services can be summarized for the following aspects of the service:

- Existing Azure Stack Edge ordering and management service.
- New Azure Edge Hardware Center that will be used for new orders going forward.

Azure Stack Edge service also integrates with the following dependent services and their behavior is also summarized:

- Azure Arc-enabled Kubernetes
- Azure IoT Hub and Azure IoT Edge

NOTE

- If you provide a support package with a crash dump for the Azure Stack Edge device, it can contain End User Identifiable Information (EUII) or End User Pseudonymous Information (EUPI) which will be processed and stored outside South East Asia.

Azure Stack Edge classic ordering and management resource

If you are using the classic experience to place an order for Azure Stack Edge, the service currently uses Azure Regional Pair to implement data resiliency against region-wide outages. For existing Azure Stack Edge resources in Singapore, the data is replicated to Hong Kong.

If you are creating a new Azure Stack Edge resource, you have the option to enable data residency only in

Singapore. When this option is selected, data is not replicated to Hong Kong. If there is a region-wide service outage, you have two options:

- Wait for the Singapore region to be restored.
- Create a resource in another region, reset the device, and manage your device via the new resource. For detailed instructions, see [Reset and reactivate your Azure Stack Edge device](#).

Azure Edge Hardware Center ordering and management resource

The new Azure Edge Hardware Center service is now available and allows you to create and manage Azure Stack Edge resources. When placing an order in Southeast Asia region, you can select the option to have your data resides only within Singapore and not be replicated.

In the event of region-wide outages, you won't be able to access the order resources. You will not be able to return, cancel, or delete the resources. If you request for updates on your order status or need to initiate a device return urgently during the service outage, Microsoft Support will handle those requests.

For detailed instructions, see [Create an order via the Azure Edge Hardware Center](#).

Azure Stack Edge dependent services

Azure Arc-enabled Kubernetes, Azure IoT Hub and Azure IoT Edge, and Azure Key Vault are services that integrate with Azure Stack Edge.

Azure Arc-enabled Kubernetes

Azure Arc-enabled Kubernetes is available as an add-on for Azure Stack Edge. For Singapore (Southeast Asia), Azure Arc data resides only within Singapore and is not replicated in Hong Kong.

Azure IoT

Azure IoT is available as an add-on for Azure Stack Edge. For Singapore (Southeast Asia), Azure IoT uses paired region and replicates data to Hong Kong. This means that Azure IoT is resilient to region-wide outages.

Next steps

- Learn more about [Azure data residency requirements](#).

Data resiliency for Azure Stack Edge

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article explains the data resiliency behavior for Azure Stack Edge service that runs in Azure and manages Azure Stack Edge devices.

About Azure Stack Edge

Azure Stack Edge service is used to deploy compute workloads on purpose-built hardware devices, right at the edge where the data is created. The purpose-built Azure Stack Edge devices are available in various form factors and can be ordered, configured, and monitored via the Azure portal. Azure Stack Edge solution can also be deployed in Azure public and Azure Government cloud environments.

Regions for Azure Stack Edge

Region information is used for Azure Stack Edge service in the following ways:

- You specify an Azure region when creating an Azure Stack Edge Hardware Center order for the Azure Stack Edge device. Data residency norms apply to Edge Hardware Center orders. For more information, see [Data residency for Edge Hardware Center](#).
- You specify an Azure region when creating a management resource for the Azure Stack Edge device. This region is used to store the metadata associated with the resource. The metadata can be stored in a location different than the physical device.
- Finally, there's a region associated with the storage accounts where the customer data is stored by the Azure Stack Edge service. You can configure SMB or NFS shares on the service to store customer data and then associate an Azure Storage account with each configured share.

Depending on the Azure Storage account configured for the share, your data is automatically and transparently replicated. For example, Azure Geo-Redundant Storage account (GRS) is configured by default when an Azure Storage account is created. With GRS, your data is automatically replicated three times within the primary region, and three times in the paired region. For more information, see [Azure Storage redundancy options](#).

Non-paired region vs. regional pairs

Azure Stack Edge service is a non-regional, always-available service and has no dependency on a specific Azure region. Azure Stack Edge service is also resilient to zone-wide outages and region-wide outages.

- **Regional pairs** - In general, Azure Stack Edge service uses Azure Regional Pairs when storing and processing customer data in all the geographies except Singapore. If there's a regional failure, the instance of the service in the Azure paired region continues to service customers. This ensures that the service is fully resilient to all the zone-wide and region-wide outages.

For all the Azure Regional Pairs, by default, Microsoft is responsible for the disaster recovery (DR) setup, execution, and testing. In the event of region outage, when the service instance fails over to from the primary region to the secondary region, the Azure Stack Edge service may be inaccessible for a short duration.

- **Non-paired region** - In Singapore, customer can choose that the customer data for Azure Stack Edge reside only in Singapore and not get replicated to the paired region, Hong Kong. With this option

enabled, the service is resilient to zone-wide outages, but not to region-wide outages. Once the data residency is set to non-paired region, it persists during the lifetime of the resource and can't be changed.

In Singapore (South East Asia) region, if the customer has chosen single data residency option that won't allow replication in the paired region, the customer will be responsible for the DR setup, execution, and testing.

Cross-region disaster recovery

Cross region disaster recovery for all regions for multiple region geographies is done via using the Azure regional pairs. A regional pair consists of two regions, primary and secondary, within the same geography. Azure serializes platform updates (planned maintenance) across regional pairs, ensuring that only one region in each pair updates at a time. If an outage affects multiple regions, at least one region in each pair is prioritized for recovery. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority. For more information, see [Cross-region replication in Azure](#).

In the event of region outage, when the service instance fails over to from the primary region to the secondary region, the Azure Stack Edge service may be inaccessible for a short duration.

For cross-region DR, Microsoft is responsible. The Recovery Time Objective (RTO) for DR is 8 hours, and Recovery Point Objective (RPO) is 15 minutes. For more information, see [Resiliency and continuity overview](#).

Cross region disaster recovery for non-paired region geography only pertains to Singapore. If there's a region-wide service outage in Singapore and you have chosen to keep your data only within Singapore and not replicated to regional pair Hong Kong, you have two options:

- Wait for the Singapore region to be restored.
- Create a resource in another region, reset the device, and manage your device via the new resource. For detailed instructions, see [Reset and reactivate your Azure Stack Edge device](#).

In this case, the customer is responsible for DR and must set up a new device and then deploy all the workloads.

Non-paired region disaster recovery

The disaster recovery isn't identical for non-paired region and multi-region geographies for this service.

For Azure Stack Edge service, all regions use regional pairs except for Singapore where you can configure the service for non-paired region data residency.

- In Singapore, you can configure the service for non-paired region data residency. The single-region geography disaster recovery support applies only to Singapore when the customer has chosen to not enable the regional pair Hong Kong. The customer is responsible for the Singapore customer enabled disaster recovery (CEDR).
- Except for Singapore, all other regions use regional pairs and Microsoft owns the regional pair disaster recovery.

For the single-region disaster recovery for which the customer is responsible:

- Both the control plane (service side) and the data plane (device data) need to be configured by the customer.
- There's a potential for data loss if the disaster recovery isn't appropriately configured by the customer. Features and functions remain intact as a new resource is created and the device is reactivated against this resource.

Here are the high-level steps to set up disaster recovery using Azure portal for Azure Stack Edge:

- Create a resource in another region. For more information, see how to [Create a management resource for Azure Stack Edge device](#).

- [Reset the device](#). When the device is reset, the local data on the device is lost. It's necessary that you back up the device prior to the reset. Use a third-party backup solution provider to back up the local data on your device. For more information, see how to [Protect data in Edge cloud shares, Edge local shares, VMs and folders for disaster recovery](#).
- [Reactivate device against a new resource](#). When you move to the new resource, you'll also need to restore data on the new resource. For more information, see how to [Restore Edge cloud shares](#), [Restore Edge local shares](#) and [Restore VM files and folders](#).

For detailed instructions, see [Reset and reactivate your Azure Stack Edge device](#).

Planning disaster recovery

Microsoft and its customers operate under the [Shared responsibility model](#). This means that for customer-enabled (responsible services DR), the customer must address disaster recovery for any service they deploy and control. To ensure that recovery is proactive, customers should always pre-deploy secondaries because there's no guarantee of capacity at time of impact for those who haven't pre-allocated.

When using Azure Stack Edge service, the customer can create a resource proactively, ahead of time, in another supported region. In the event of a disaster, this resource can then be deployed.

Testing disaster recovery

Azure Stack Edge doesn't have DR available as a feature. This implies that the interested customers should perform their own DF failover testing for this service. If a customer is trying to restore a workload or configuration in a new device, they are responsible for the end-to-end configuration.

Next steps

- Learn more about [Azure data residency requirements](#).

Manage Azure Stack Edge secrets using Azure Key Vault

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Azure Key Vault is integrated with Azure Stack Edge resource for secret management. This article provides details on how an Azure Key Vault is created for Azure Stack Edge resource during device activation and is then used for secret management.

About key vault and Azure Stack Edge

Azure Key Vault cloud service is used to securely store and control access to tokens, passwords, certificates, API keys, and other secrets. Key Vault also makes it easy to create and control the encryption keys used to encrypt your data.

For Azure Stack Edge service, the integration with key vault provides the following benefits:

- Stores customer secrets. One of the secrets used for the Azure Stack Edge service is Channel Integrity Key (CIK). This key allows you to encrypt your secrets and is securely stored in the key vault. Device secrets such as BitLocker recovery key and Baseboard Management Controller (BMC) user password are also stored in the key vault.

For more information, see [Securely store secrets and keys](#).

- Passes encrypted customer secrets to the device.
- Displays device secrets for easy access if the device is down.

Generate activation key and create key vault

A key vault is created for Azure Stack Edge resource during the process of activation key generation. The key vault is created in the same resource group where the Azure Stack Edge resource is present. Contributor permission is required on the key vault.

Prerequisites for key vault

Prior to the key vault creation during activation, the following prerequisites must be satisfied:

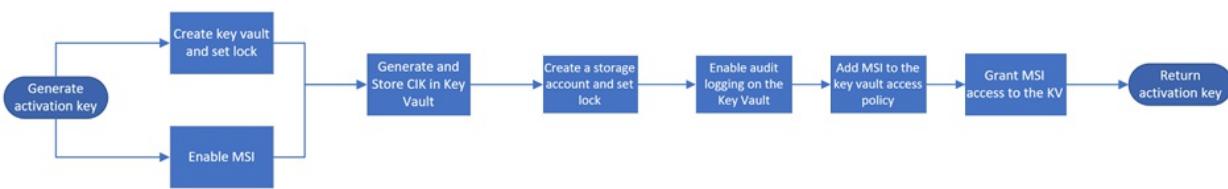
- Register the *Microsoft.KeyVault* resource provider before you create the Azure Stack Edge resource. The resource provider is automatically registered if you have owner or contributor access to the subscription. The key vault is created in the same subscription and the resource group as the Azure Stack Edge resource.
- When you create an Azure Stack Edge resource, a system-assigned managed identity is also created that persists for the lifetime of the resource and communicates with the resource provider on the cloud.

When the managed identity is enabled, Azure creates a trusted identity for the Azure Stack Edge resource.

Key vault creation

After you have created the resource, you need to activate the resource with the device. To do so, you'll generate an activation key from the Azure portal.

When you generate an activation key, the following events occur:



- You request an activation key in the Azure portal. The request is then sent to key vault resource provider.
- A standard tier key vault with access policy is created and is locked by default.
 - This key vault uses the default name or a 3 to 24 character long custom name that you specified. You cannot use a key vault that is already in use.
 - The key vault details are stored in the service. This key vault is used for secret management and persists for as long as the Azure Stack Edge resource exists.

The screenshot shows the Azure Stack Edge portal interface. The left sidebar includes sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring (Device events, Alerts, Metrics). The main content area displays a message: "Device is not activated. Review the steps to configure and activate your device." Below this, under "Activate device once it arrives", there is a form with "Azure key vault name" set to "ase-myasetest-ed30d9ee38" and a "Generate activation key" button highlighted with a red box. A note below says "Ensure that your infrastructure is configured. Refer [steps to configure](#)". The "Edge services" section shows cards for Virtual machines, IoT Edge, and Cloud storage gateway.

- A resource lock is enabled on the key vault to prevent accidental deletion. A soft-delete is also enabled on the key vault that allows the key vault to be restored within 90 days if there is an accidental deletion. For more information, see [Azure Key Vault soft-delete overview](#).
- A system-assigned managed identity that was created when you created the Azure Stack Edge resource, is now enabled.
- A channel integrity key (CIK) is generated and placed in the key vault. The CIK details are displayed in the service.
- A Zone redundant storage account (ZRS) is also created in the same scope as the Azure Stack Edge resource and a lock is placed on the account.
 - This account is used to store the audit logs.
 - The storage account creation is a long running process and takes a few minutes.
 - The storage account is tagged with the key vault name.
- A diagnostics setting is added to the key vault and the logging is enabled.
- The managed identity is added to the key vault access policy to allow access to the key vault as the device uses the key vault to store and retrieve secrets.
- The key vault authenticates the request with managed identity to generate activation key. The activation key is returned to the Azure portal. You can then copy this key and use it in the local UI to activate your device.

NOTE

- If you had an existing Azure Stack Edge resource before the Azure Key Vault was integrated with Azure Stack Edge resource, you are not affected. You can continue to use your existing Azure Stack Edge resource.
- The creation of key vault and storage account adds to the overall resource cost. For more information about allowed transactions and corresponding charges, see [Pricing for Azure Key Vault](#) and [Pricing for Storage account](#).

If you run into any issues related to key vault and device activation, see [Troubleshoot device activation issues](#).

View key vault properties

After the activation key is generated and key vault is created, you may want to access the key vault to view the secrets, access policies, diagnostics, and insights. The following procedure describes each of these operations.

View secrets

After the activation key is generated and key vault is created, you may want to access the key vault.

To access the key vault and view the secrets, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. In the right-pane, under **Security**, you can view the **Secrets**.
3. You can also navigate to the key vault associated with your Azure Stack Edge resource. Select **Key vault name**.

The screenshot shows the Azure portal interface for an Azure Stack Edge resource named "myasegpudevice". On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Locks and Properties), Security (which is selected and highlighted with a red box), Order details, Edge services, and Virtual machines. The main content area is titled "myasegpudevice | Security". It displays the "Key Vault name" as "ase-myasegpude-1e7b5e1e9" and "Key Vault monitoring" as "ase-myasegpude-1e7b5e1e9". Under the "Secrets" section, it says "To view all the secrets, access your key vault." and lists "Channel integrity key (CIK)" and "BitLocker recovery key", each with a "Show secret" button. A "Sync device secrets" button and a "Refresh" button are also present.

4. To view the secrets stored in your key vault, go to **Secrets**. Channel integrity key, BitLocker recovery key and Baseboard management controller (BMC) user passwords are stored in the key vault. If the device goes down, the portal provides easy access to BitLocker recovery key and BMC user password.

The screenshot shows the Azure portal interface for a key vault named "ase-myasegpude-1e7b5e1e9". On the left, there's a navigation menu with options like Diagnose and solve problems, Events, Settings (with Keys selected and highlighted with a red box), Certificates, Access policies, and Networking. The main content area is titled "ase-myasegpude-1e7b5e1e9 | Secrets". It has buttons for Generate/Import, Refresh, Restore Backup, and Manage deleted secrets. A table lists the secrets:

Name	Type	Status	Expiration date
ase-cik-8023e34e-ea57...		✓ Enabled	
ase-seke7af458edb098...		✓ Enabled	
HcsDataBitLockerExtKe...		✓ Enabled	
HcsIntBitLockerExtKey...		✓ Enabled	
SystemVolBitLockerKey...		✓ Enabled	

View managed identity access policies

To access the access policies for your key vault and managed identity, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. Select the link corresponding to **Key vault name** to navigate to the key vault associated with your Azure Stack Edge resource.

The screenshot shows the 'myasegpudevice | Security' blade in the Azure Stack Edge portal. The left sidebar has a red box around the 'Security' item. The main area shows the 'Key Vault name' as 'ase-myasegpude-1e7b5e1e9'. Below it, 'Key Vault monitoring' is set to 'ase-myasegpude-1e7b5e1e9' and 'System assigned managed identity' is 'Enabled'. Under the 'Secrets' section, there are two entries: 'Channel integrity key (CIK)' and 'BitLocker recovery key', each with a 'Show secret' button. A red box highlights the 'Show secret' button for the BitLocker recovery key.

3. To view the access policies associated with your key vault, go to **Access policies**. You can see that the managed identity has been given access. Select **Secret permissions**. You can see that the managed identity access is restricted only to the **Get** and **Set** of the secret.

The screenshot shows the 'ase-myasegpude-1e7b5e1e9 | Access policies' blade. The left sidebar has a red box around the 'Access policies' item. The main area shows 'Enable Access to:' with three checked options: 'Azure Virtual Machines for deployment', 'Azure Resource Manager for template deployment', and 'Azure Disk Encryption for volume encryption'. The 'Permission model' is set to 'Vault access policy'. On the right, a 'Secret Management ...' dropdown is open, showing 'Get' and 'Set' checkboxes, both of which are checked. A red box highlights the 'Get' and 'Set' checkboxes. Below this, the 'Current Access Policies' table lists one entry: 'myasegpudevice' under the 'APPLICATION' column, with 'Key Permissions' set to '0 selected'. A red box highlights the '0 selected' dropdown. The table also includes columns for 'Privileged Secret Ope...', 'Certificate Permissions', and 'Action'.

View audit logs

To access the key vault and view the diagnostics settings and the audit logs, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. Select the link corresponding to **Key vault name** to navigate to the key vault associated with your Azure Stack Edge resource.

The screenshot shows the Azure Stack Edge portal interface. On the left, there's a navigation bar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Properties, Security (which is highlighted with a red box), Order details, Edge services, and Virtual machines. The main content area is titled 'myasegpudevice | Security'. It shows a 'Key Vault name' field with the value 'ase-myasegpude-1e7b5e1e9' and a 'Key Vault monitoring' status of 'ase-myasegpude-1e7b5e1e9'. Under the 'Secrets' section, it lists 'Channel integrity key (CIK)' and 'BitLocker recovery key', each with a 'Show secret' button.

3. To view the diagnostics settings associated with your key vault, go to **Diagnostics settings**. This setting lets you monitor how and when your key vaults are accessed, and by whom. You can see that a diagnostics setting has been created. Logs are flowing into the storage account that was also created. Audit events are also created in the key vault.

The screenshot shows the Azure portal interface. On the left, there's a navigation bar with links like Networking, Security, Properties, Locks, Monitoring, Alerts, Metrics, and Diagnostic settings (which is highlighted with a red box). The main content area is titled 'ase-myasegpude-1e7b5e1e9 | Diagnostic settings'. It shows a table of diagnostic settings with one entry: 'ase-audit-ase-m-de740fa...' (Storage account: asekvlogbase33ebabd000...). There's a 'Edit setting' button next to the entry, which is highlighted with a red box. Below the table, there's a note: 'Click 'Add Diagnostic setting' above to configure the collection of the following data:' followed by 'AuditEvent' and 'AllMetrics'.

If you have configured a different storage target for logs on the key vault, then you can view the logs directly in that storage account.

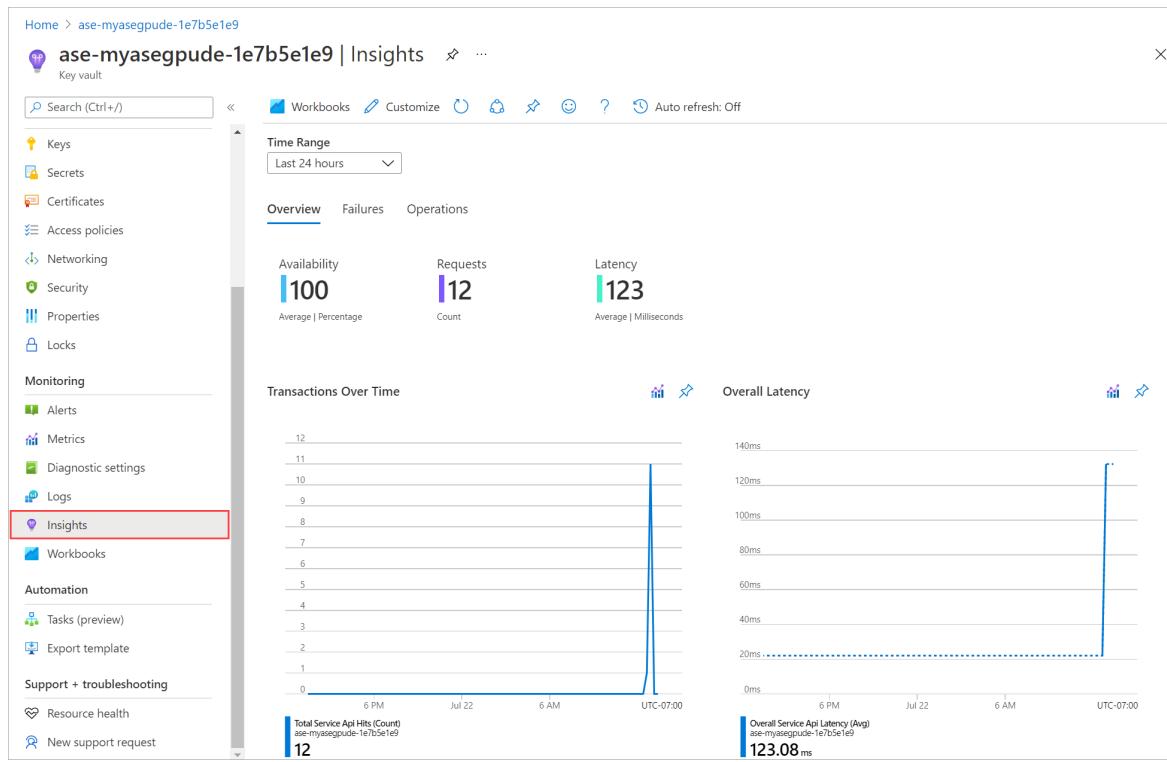
View insights

To access the key vault insights including the operations performed on the key vault, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. Select the link corresponding to **Key vault diagnostics**.

This screenshot is identical to the one at the top of the page, showing the 'myasegpudevice | Security' blade in the Azure Stack Edge portal. The 'Security' link in the left navigation bar is highlighted with a red box. The 'Key Vault name' field shows 'ase-myasegpude-1e7b5e1e9'.

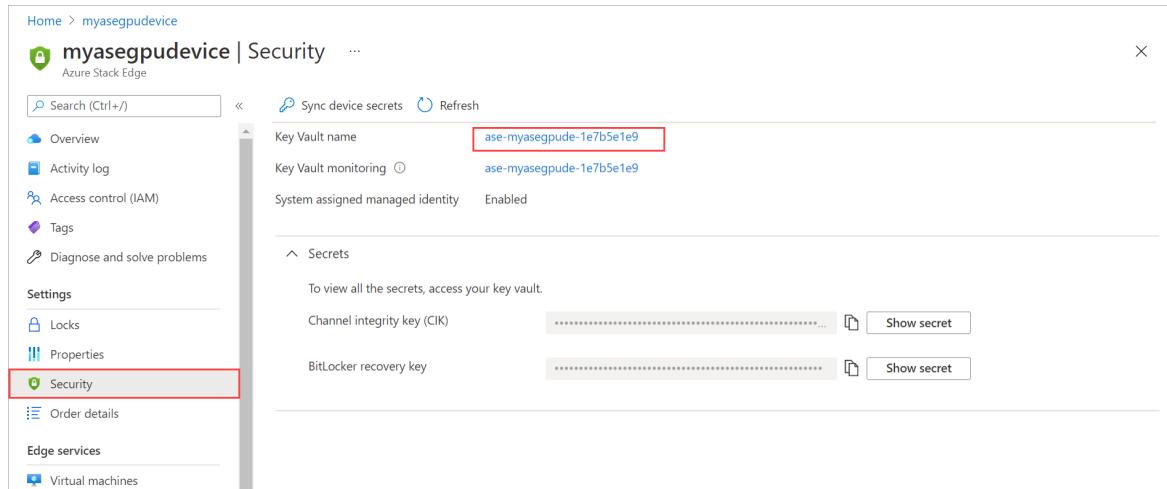
3. The **Insights** blade gives an overview of the operations performed on the key vault.



View managed identity status

To view the status of the system-assigned managed identity associated with your Azure Stack Edge resource, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. In the right-pane, go to **system-assigned managed identity** to view if the system-assigned managed identity is enabled or disabled.



View key vault locks

To access the key vault and view the locks, follow these steps:

1. In the Azure portal for your Azure Stack Edge resource, go to **Security**.
2. Select the link corresponding to **Key vault name** to navigate to the key vault associated with your Azure Stack Edge resource.

The screenshot shows the Azure Stack Edge portal interface. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Properties, Security (which is highlighted with a red box), Order details, Edge services, and Virtual machines. The main content area is titled "myasegpudevice | Security". It shows a "Key Vault name" field with "ase-myasegpude-1e7b5e1e9" and a "Sync device secrets" button. Below that, "Key Vault monitoring" is set to "ase-myasegpude-1e7b5e1e9" and "System assigned managed identity" is "Enabled". A section titled "Secrets" is expanded, showing "Channel integrity key (CIK)" and "BitLocker recovery key", each with a "Show secret" button. At the bottom of the main content area, there's a "Secrets" link.

3. To view the locks on your key vault, go to **Locks**. To prevent accidental deletion, a resource lock is enabled on the key vault.

The screenshot shows the Azure portal interface for a key vault named "ase-myasegpude-1e7b5e1e9". The left sidebar has options for Networking, Security, Properties, Locks (which is highlighted with a red box), and Monitoring. The main content area is titled "ase-myasegpude-1e7b5e1e9 | Locks". It shows a table with columns: Lock name, Lock type, Scope, and Notes. There is one row visible: "DoNotDelete" with "Delete" as the lock type, and the scope is "ase-myasegpude-1e7...". There are "Edit" and "Delete" buttons at the end of the row. The "Scope" column contains a small icon of a globe.

Regenerate activation key

In certain instances, you may need to regenerate activation key. When you regenerate an activation key, the following events occur:

1. You request to regenerate an activation key in the Azure portal.
2. The activation key is returned to the Azure portal. You can then copy this key and use it.

The key vault is not accessed when you regenerate the activation key.

Recover device secrets

If the CIK is accidentally deleted or secrets (for example, BMC user password) have become stale in the key vault, then you would need to push secrets from the device to update the key vault secrets.

Follow these steps to sync device secrets:

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Security**.
2. In the right-pane, from the top command bar, select **Sync device secrets**.
3. The device secrets are pushed to the key vault to restore or update the secrets in the key vault. You'll see a notification when the sync is completed.

The screenshot shows the Azure Stack Edge device settings page for 'myasegpudevice'. The left sidebar has a 'Security' section highlighted with a red box. The main pane shows 'Sync device secrets' status as 'Successfully completed the operation.' Below it, 'Key Vault name' is set to 'ase-myasegpude-1e7b5e1e9'. Under 'Secrets', there are two entries: 'Channel integrity key (CIK)' and 'BitLocker recovery key', each with a 'Show secret' button.

Delete key vault

There are two ways to delete the key vault associated with the Azure Stack Edge resource:

- Delete the Azure Stack Edge resource and choose to delete the associated key vault at the same time.
- Accidentally deleted the key vault directly.

When your Azure Stack Edge resource is deleted, the key vault is also deleted with the resource. You are prompted for confirmation. If you are storing other keys in this key vault and do not intend to delete this key vault, you can choose to not provide consent. Only the Azure Stack Edge resource is deleted leaving the key vault intact.

Follow these steps to delete the Azure Stack Edge resource and the associated key vault:

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Overview**.
2. In the right pane, select **Delete**. This action will delete the Azure Stack Edge resource.

The screenshot shows the Azure Key Vault overview page for 'ase-myasegpude-1e7b5e1e9'. The left sidebar has an 'Overview' section highlighted with a red box. The main pane shows the 'Delete' button highlighted with a red box. The right pane displays vault details: Resource group: myasegpure, Location: East US, Subscription: Edge Gateway Test, Subscription ID: <Subscription ID>, Vault URI: https://ase-myasegpude-1e7b5e1e9.vault.azure.net/, Sku (Pricing tier): Standard, Directory ID: 72f988bf-86f1-41af-91ab-2d7cd011db47, Directory Name: Microsoft, Soft-delete: Enabled, Purge protection: Disabled.

3. You'll see a confirmation blade. Type your Azure Stack Edge resource name. To confirm the deletion of the associated key vault, type **Yes**.

Delete key vault

X

ase-myasegpude-1e7b5e1e9

! The soft delete feature has been enabled on this key vault. After you soft delete this key vault, it will remain in your subscription as a hidden vault. It will get purged after the retention period you specified. You may purge it sooner, or restore the vault, using Azure Portal, Azure PowerShell, or Azure CLI. See this page for reference: <https://docs.microsoft.com/azure/key-vault/key-vault-ovw-soft-delete>

Key vault name

ase-myasegpude-1e7b5e1e9

Delete

Cancel

4. Select **Delete**.

The Azure Stack Edge resource and the key vault are deleted.

The key vault may be deleted accidentally when the Azure Stack Edge resource is in use. If this happens, a critical alert is raised in the **Security** page for your Azure Stack Edge resource. You can navigate to this page to recover your key vault.

Recover key vault

You can recover the key vault associated with your Azure Stack Edge resource if it is deleted accidentally or purged. If this key vault was used to store other keys, then you will need to recover those keys by restoring the key vault.

- Within 90 days of deletion, you can restore the key vault that was deleted.
- If the purge-protection period of 90 days has already elapsed, you can't restore the key vault. Instead you'll need to create a new key vault.

Within 90 days of deletion, follow these steps to recover your key vault:

- In the Azure portal, go to the **Security** page of your Azure Stack Edge resource. You'll see a notification to the effect that the key vault associated with your resource was deleted. You can select the notification or select **Reconfigure** against the key vault name under **Security preferences** to recover your key vault.

- In the Recover key vault blade, select **Configure**. The following operations are performed as a part of the recovery:



- A key vault is recovered with the same name and a lock is placed on the key vault resource.

NOTE

If your key vault is deleted, and the purge-protection period of 90 days hasn't elapsed, then in that time period, the key vault name can't be used to create a new key vault.

- A storage account is created to store the audit logs.
- The system-assigned managed identity is granted access to the key vault.
- Device secrets are pushed to the key vault.

Select **Configure**.

Recover key vault

X

myasegpudevice

Recover your key vault if it is deleted or purged.

i The Key Vault has been deleted within the past 90 days, it will be restored. [Learn more.](#)

Key Vault name i

ase-myasegpude-1e7b5e1e9

The following operations are performed as a part of the recovery:

- Key vault is recovered.
- Storage account is created to store audit logs.
- System-assigned managed identity is granted access to the key vault.
- Device secrets are pushed to the key vault.

[Learn more](#) about the procedure.

Click **Configure** to complete the recovery.

Configure

Close

The key vault is recovered and when the recovery is complete, a notification is shown to that effect.

If the key vault is deleted and the purge-protection period of 90 days has elapsed, then you'll have the option of creating a new key vault through the [Recover key procedure](#) described above. In this case, you'll provide a new name for your key vault. A new storage account is created, managed identity is granted access to this key vault, and device secrets are pushed to this key vault.

Recover managed identity access

If the system-assigned managed identity access policy is deleted, an alert is raised when the device is unable to resync the key vault secrets. If the managed identity doesn't have access to the key vault, again a device alert is raised. Select the alert in each case to open the **Recover key vault blade** and reconfigure. This process should restore the managed identity access.



Next steps

- Learn more about how to [Generate activation key](#).
- [Troubleshoot key vault errors](#) on your Azure Stack Edge device.

Disconnected scenario for Azure Stack Edge

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article helps you identify things to consider when you need to use Azure Stack Edge disconnected from the internet.

Typically, Azure Stack Edge is deployed in a connected scenario with access to the Azure portal, services, and resources in the cloud. However, security or other restrictions sometime require that you deploy your Azure Stack Edge device in an environment with no internet connection. As a result, Azure Stack Edge becomes a standalone deployment that is disconnected from and doesn't communicate with Azure and other Azure services.

Assumptions

Before you disconnect your Azure Stack Edge device from the network that allows internet access, you'll make these preparations:

- To ensure most of the Azure Stack Edge features function in this disconnected mode, you'll activate your device via the Azure portal and deploy containerized and non-containerized workloads such as Kerberos, virtual machines (VMs), and IoT Edge use cases while you have an internet connection.

During offline use, you won't have access to the Azure portal to manage workloads; all management will be performed via operations local control plane operations. For a list of Azure endpoints that can't be reached during offline use, see [URL patterns for firewall rules](#).

- For an IoT Edge and Kubernetes deployment, you'll complete these tasks before you disconnect:

1. Enable and configure IoT Edge and/or Kubernetes components.
2. Deploy compute modules and containers on the device.
3. Make sure the modules and components are running.

For Kubernetes deployment guidance, see [Choose the deployment type](#). For IoT Edge deployment guidance, see [Run a compute workload with IoT Edge module on Azure Stack Edge](#).

NOTE

Some workloads running in VMs, Kerberos, and IoT Edge may require connectivity to Azure. For example, some cognitive services require connectivity for billing.

Key differences for disconnected use

When an Azure Stack Edge deployment is disconnected, it can't reach Azure endpoints. This lack of access affects the features that are available.

The following table describes the behavior of features and components when the device is disconnected.

AZURE STACK EDGE FEATURE/COMPONENT	IMPACT/BEHAVIOR WHEN DISCONNECTED
------------------------------------	-----------------------------------

AZURE STACK EDGE FEATURE/COMPONENT	IMPACT/BEHAVIOR WHEN DISCONNECTED
Local UI and Windows PowerShell interface	Local access via the local web UI or the Windows PowerShell interface is available by connecting a client computer directly to the device.
Kubernetes	<p>Kubernetes deployments on a disconnected device have these differences:</p> <ul style="list-style-type: none"> After you create your Kubernetes cluster, you can connect to and manage the cluster locally from your device using a native tool such as <code>kubectl</code>. With <code>kubectl</code>, a <code>kubeconfig</code> file allows the Kubernetes client to talk directly to the Kubernetes cluster without connecting to PowerShell interface of your device. Once you have the config file, you can direct the cluster using <code>kubectl</code> commands, without physical access to the cluster. For more information, see Create and Manage a Kubernetes cluster on an Azure Stack Edge Pro GPU device. Azure Stack Edge has a local container registry - the Edge container registry - to host container images. While your device is disconnected, you'll manage the deployment of these images, pushing them to and deleting them from the Edge container registry over your local network. You won't have direct access to the Azure Container Registry in the cloud. For more information, see Enable an Edge container registry on an Azure Stack Edge Pro GPU device. You can't monitor the Kubernetes cluster using Azure Monitor. Instead, use the local Kubernetes dashboard, available on the compute network. For more information, see Monitor your Azure Stack Edge Pro device via the Kubernetes dashboard. <p>For more information, see Kubernetes on your Azure Stack Edge Pro GPU device.</p>
Azure Arc on Kubernetes	An Azure Arc-enabled Kubernetes deployment can't be used in a disconnected deployment.
Azure Arc-enabled data services	After the container images are deployed on the device, Azure Arc-enabled data services continue to run in a disconnected deployment. You'll deploy and manage those images over your local network. You'll push images to and delete them from the Edge container registry. For more information, see Manage container registry images .
IoT Edge	IoT Edge modules need to be deployed and updated while connected to Azure. If disconnected from Azure, they continue to run.
Azure Storage access tiers	<p>During disconnected use:</p> <ul style="list-style-type: none"> Data in your Azure Storage account won't be uploaded to and from access tiers in the Azure cloud. Ghosted data can't be accessed directly through the device. Any access attempt fails with an error. The Refresh option can't be used to sync data in your Azure Storage account with shares in the Azure cloud. Data syncs resume when connectivity is established.

AZURE STACK EDGE FEATURE/COMPONENT	IMPACT/BEHAVIOR WHEN DISCONNECTED
VM management	During disconnected use, virtual machines can be created, modified, stopped, started, and deleted using the local Azure Resource Manager (ARM) . However, VM images can't be downloaded to the device from the cloud. For more information, see Deploy VMs on your Azure Stack Edge device via Azure PowerShell .
Local ARM	Local Azure Resource Manager (ARM) can function without connectivity to Azure. However, connectivity is required during registration and configuration of Local ARM - for example, to set the ARM Edge user password and ARM subscription ID.
VPN	A configured virtual private network (VPN) remains intact when there's no connection to Azure. When connectivity to Azure is established, data-in-motion transfers over the VPN.
Updates	Automatic updates from Windows Server Update Services (WSUS) aren't available during disconnected use. To apply updates, download update packages manually and then apply them via the device's local web UI.
Supportability / Support log collection / Remote supportability	<p>Microsoft Support is available, with these differences:</p> <ul style="list-style-type: none"> You can't automatically generate a support request and send logs to Microsoft Support via the Azure portal. Instead, collect a support package via the device's local web UI. Microsoft Support will send you a shared access signature (SAS) URI to upload the support packages to. Microsoft can't perform remote diagnostics and repairs while the device is disconnected. Running the commands on the device requires direct communication with Azure.
Billing	Billing for your order resource or management resource continues whether or not your Azure Stack Edge device is connected to the internet.

Next steps

- Review use cases for [Azure Stack Edge Pro with GPU](#), [Azure Stack Edge Pro R](#), and [Azure Stack Edge Mini R](#).
- [Get pricing](#).

Security and data protection for Azure Stack Edge Pro 2, Azure Stack Edge Pro R, and Azure Stack Edge Mini R

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Security is a major concern when you're adopting a new technology, especially if the technology is used with confidential or proprietary data. Azure Stack Edge Pro R and Azure Stack Edge Mini R help you ensure that only authorized entities can view, modify, or delete your data.

This article describes the Azure Stack Edge Pro R and Azure Stack Edge Mini R security features that help protect each of the solution components and the data stored in them.

The solution consists of four main components that interact with each other:

- **Azure Stack Edge service, hosted in Azure public or Azure Government cloud.** The management resource that you use to create the device order, configure the device, and then track the order to completion.
- **Azure Stack Edge rugged device.** The rugged, physical device that's shipped to you so you can import your on-premises data into Azure public or Azure Government cloud. The device could be Azure Stack Edge Pro R or Azure Stack Edge Mini R.
- **Clients/hosts connected to the device.** The clients in your infrastructure that connect to the device and contain data that needs to be protected.
- **Cloud storage.** The location in the Azure cloud platform where data is stored. This location is typically the storage account linked to the Azure Stack Edge resource that you create.

Service protection

The Azure Stack Edge service is a management service that's hosted in Azure. The service is used to configure and manage the device.

- To access the Data Box Edge service, your organization needs to have an Enterprise Agreement (EA) or Cloud Solution Provider (CSP) subscription. For more information, see [Sign up for an Azure subscription](#).
- Because this management service is hosted in Azure, it's protected by the Azure security features. For more information about the security features provided by Azure, go to the [Microsoft Azure Trust Center](#).
- For SDK management operations, you can get the encryption key for your resource in **Device properties**. You can view the encryption key only if you have permissions for the Resource Graph API.

Device protection

The rugged device is an on-premises device that helps transform your data by processing it locally and then sending it to Azure. Your device:

- Needs an activation key to access the Azure Stack Edge service.
- Is protected at all times by a device password.
- Is a locked-down device. The device baseboard management controller (BMC) and BIOS are password-protected. The BMC is protected by limited user-access.
- Has secure boot enabled that ensures the device boots up only using the trusted software provided by

Microsoft.

- Runs Windows Defender Application Control (WDAC). WDAC lets you run only trusted applications that you define in your code-integrity policies.
- Has a Trusted Platform Module (TPM) that performs hardware-based, security-related functions. Specifically, the TPM manages and protects secrets and data that needs to be persisted on the device.
- Only the required ports are opened on the device and all the other ports are blocked. For more information, see the list of [Port requirements for device](#).
- All the access to the device hardware as well as software is logged.
 - For the device software, default firewall logs are collected for inbound and outbound traffic from the device. These logs are bundled in the support package.
 - For the device hardware, all the device chassis events such as opening and closing of the device chassis, are logged in the device.

For more information on the specific logs that contain the hardware and software intrusion events and how to get the logs, go to [Gather advanced security logs](#).

Protect the device via activation key

Only an authorized Azure Stack Edge Pro R or Azure Stack Edge Mini R device is allowed to join the Azure Stack Edge service that you create in your Azure subscription. To authorize a device, you need to use an activation key to activate the device with the Azure Stack Edge service.

The activation key that you use:

- Is an Azure Active Directory (Azure AD) based authentication key.
- Expires after three days.
- Isn't used after device activation.

After you activate a device, it uses tokens to communicate with Azure.

For more information, see [Get an activation key](#).

Protect the device via password

Passwords ensure that only authorized users can access your data. Azure Stack Edge Pro R devices boot up in a locked state.

You can:

- Connect to the local web UI of the device via a browser and then provide a password to sign in to the device.
- Remotely connect to the device PowerShell interface over HTTP. Remote management is turned on by default. Remote management is also configured to use Just Enough Administration (JEA) to limit what the users can do. You can then provide the device password to sign in to the device. For more information, see [Connect remotely to your device](#).
- The local Edge user on the device has limited access to the device for initial configuration, and troubleshooting. The compute workloads running on the device, data transfer, and the storage can all be accessed from the Azure public or government portal for the resource in the cloud.

Keep these best practices in mind:

- We recommend that you store all passwords in a secure place so you don't have to reset a password if it's forgotten. The management service can't retrieve existing passwords. It can only reset them via the Azure portal. If you reset a password, be sure to notify all users before you reset it.
- You can access the Windows PowerShell interface of your device remotely over HTTP. As a security best practice, you should use HTTP only on trusted networks.

- Ensure that device passwords are strong and well protected. Follow the [password best practices](#).
- Use the local web UI to [Change the password](#). If you change the password, be sure to notify all remote access users so they don't have problems signing in.

Establish trust with the device via certificates

Azure Stack Edge rugged device lets you bring your own certificates and install those to be used for all public endpoints. For more information, go to [Upload your certificate](#). For a list of all the certificates that can be installed on your device, go to [Manage certificates on your device](#).

- When you configure compute on your device, an IoT device and an IoT Edge device are created. These devices are automatically assigned symmetric access keys. As a security best practice, these keys are rotated regularly via the IoT Hub service.

Protect your data

This section describes the security features that protect in-transit and stored data.

Protect data at rest

All the data at rest on the device is double-encrypted, the access to data is controlled and once the device is deactivated, the data is securely erased off the data disks.

Double-encryption of data

Data on your disks is protected by two layers of encryption:

- First layer of encryption is the BitLocker XTS-AES 256-bit encryption on the data volumes.
- Second layer is the hard disks that have a built-in encryption.
- The OS volume has BitLocker as the single layer of encryption.

NOTE

The OS disk has single layer BitLocker XTS-AES-256 software encryption.

Before you activate the device, you are required to configure encryption-at-rest on your device. This is a required setting and until this is successfully configured, you can't activate the device.

At the factory, once the devices are imaged, the volume level BitLocker encryption is enabled. After you receive the device, you need to configure the encryption-at-rest. The storage pool and volumes are recreated and you can provide BitLocker keys to enable encryption-at-rest and thus create another layer of encryption for your data-at-rest.

The encryption-at-rest key is a 32 character long Base-64 encoded key that you provide and this key is used to protect the actual encryption key. Microsoft does not have access to this encryption-at-rest key that protects your data. The key is saved in a key file on the [Cloud details](#) page after the device is activated.

When the device is activated, you are prompted to save the key file that contains recovery keys that help recover the data on the device if the device doesn't boot up. Certain recovery scenarios will prompt you for the key file that you have saved. The key file has the following recovery keys:

- A key that unlocks the first layer of encryption.
- A key that unlocks the hardware encryption in the data disks.
- A key that helps recover the device configuration on the OS volumes.
- A key that protects the data flowing through the Azure service.

IMPORTANT

Save the key file in a secure location outside the device itself. If the device doesn't boot up, and you don't have the key, it could potentially result in data loss.

Restricted access to data

Access to data stored in shares and storage accounts is restricted.

- SMB clients that access share data need user credentials associated with the share. These credentials are defined when the share is created.
- NFS clients that access a share need to have their IP address added explicitly when the share is created.
- The Edge storage accounts that are created on the device are local and are protected by the encryption on the data disks. The Azure storage accounts that these Edge storage accounts are mapped to are protected by subscription and two 512-bit storage access keys associated with the Edge storage account (these keys are different than those associated with your Azure Storage accounts). For more information, see [Protect data in storage accounts](#).
- BitLocker XTS-AES 256-bit encryption is used to protect local data.

Secure data erasure

When the device undergoes a hard reset, a secure wipe is performed on the device. The secure wipe performs data erasure on the disks using the NIST SP 800-88r1 purge.

Protect data in flight

For data in flight:

- Standard Transport Layer Security (TLS) 1.2 is used for data that travels between the device and Azure. There is no fallback to TLS 1.1 and earlier. Agent communication will be blocked if TLS 1.2 isn't supported. TLS 1.2 is also required for portal and SDK management.
- When clients access your device through the local web UI of a browser, standard TLS 1.2 is used as the default secure protocol.
 - The best practice is to configure your browser to use TLS 1.2.
 - Your device only supports TLS 1.2 and does not support older versions TLS 1.1 nor TLS 1.0.
- We recommend that you use SMB 3.0 with encryption to protect data when you copy it from your data servers.

Protect data in storage accounts

Your device is associated with a storage account that's used as a destination for your data in Azure. Access to the storage account is controlled by the subscription and two 512-bit storage access keys associated with that storage account.

One of the keys is used for authentication when the Azure Stack Edge device accesses the storage account. The other key is held in reserve, so you can rotate the keys periodically.

For security reasons, many datacenters require key rotation. We recommend that you follow these best practices for key rotation:

- Your storage account key is similar to the root password for your storage account. Carefully protect your account key. Don't distribute the password to other users, hard code it, or save it anywhere in plain text that's accessible to others.
- [Regenerate your account key](#) via the Azure portal if you think it could be compromised.
- Your Azure admin should periodically change or regenerate the primary or secondary key by using the Storage section of the Azure portal to access the storage account directly.
- You can also use your own encryption key to protect the data in your Azure storage account. When you

specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. For more information on how to secure your data, see [Enable customer-managed keys for your Azure Storage account](#).

- Rotate and then [sync your storage account keys](#) regularly to help protect your storage account from unauthorized users.

Manage personal information

The Azure Stack Edge service collects personal information in the following scenarios:

- **Order details.** When an order is created, the shipping address, email address, and contact information of the user is stored in the Azure portal. The information saved includes:

- Contact name
- Phone number
- Email address
- Street address
- City
- ZIP Code/postal code
- State
- Country/province/region
- Shipping tracking number

Order details are encrypted and stored in the service. The service retains the information until you explicitly delete the resource or order. The deletion of the resource and the corresponding order is blocked from the time the device is shipped until the device returns to Microsoft.

- **Shipping address.** After an order is placed, Data Box service provides the shipping address to third-party carriers like UPS.
- **Share users.** Users on your device can also access the data located on the shares. A list of users who can access the share data can be viewed. When the shares are deleted, this list is also deleted.

To view the list of users who can access or delete a share, follow the steps in [Manage shares on the Azure Stack Edge](#).

For more information, review the Microsoft privacy policy on the [Trust Center](#).

Next steps

[Deploy your Azure Stack Edge Pro R device](#)

Check network readiness for Azure Stack Edge devices

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to check to see how ready your network is for deployment of Azure Stack Edge devices.

You'll use the Azure Stack Network Readiness Checker, a PowerShell tool that runs a series of tests to check mandatory and optional settings on the network where you deploy your Azure Stack Edge devices. The tool returns Pass/Fail status for each test and saves a log file and report file with more detail.

You can run the tool from any computer on the network where you'll deploy the Azure Stack Edge devices. The tool works with PowerShell 5.1, which is built into Windows.

About the tool

The Azure Stack Network Readiness Checker can check whether a network meets the following prerequisites:

- The Domain Name System (DNS) server is available and functioning.
- The Network Time Protocol (NTP) server is available and functioning.
- Azure endpoints are available and respond on HTTPS, with or without a proxy server.
- The Windows Update server - either the customer-provided Windows Server Update services (WSUS) server or the public Windows Update server - is available and functioning.
- The network path has a Maximum Transmission Unit (MTU) of at least 1,500 bytes, as required by the Azure Stack Edge service.
- There are no overlapping IP addresses for Edge Compute.
- DNS resource records for Azure Stack Edge can be resolved.

Report file

The tool saves a report, `AzsReadinessCheckerReport.json`, with detailed diagnostics that are collected during each test. This information can be helpful if you need to [contact Microsoft Support](#).

For example, the report provides:

- A list of network adapters on the machine used to run the tests, with the driver version, MAC address, and connection state for each network adapter.
- IP configuration of the machine used to run the tests.
- Detailed DNS response properties that the DNS server returned for each test.
- Detailed HTTP response for each test of a URL.
- Network route trace for each test.

Prerequisites

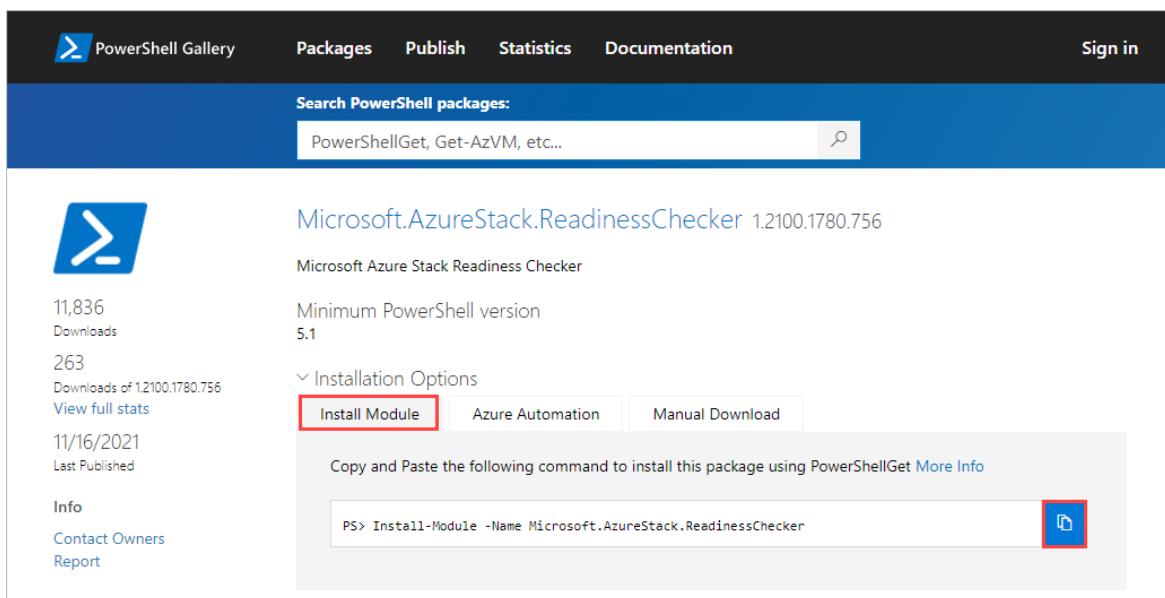
Before you begin, complete the following tasks:

- Review network requirements in the [Deployment checklist for your Azure Stack Edge Pro GPU device](#).
- Make sure you have access to a client computer that is running on the network where you'll deploy your Azure Stack Edge devices.
- Install the Azure Stack Network Readiness Checker tool in PowerShell by following the steps in [Install Network Readiness Checker](#), below.

Install Network Readiness Checker

To install the Azure Stack Network Readiness Checker on the client computer, do these steps:

1. Open PowerShell on the client computer. If you need to install PowerShell, see [Installing PowerShell on Windows](#).
2. In a browser, go to [Microsoft.AzureStack.ReadinessChecker](#) in the PowerShell Gallery. Version 1.2100.1780.756 of the Microsoft.AzureStack.ReadinessChecker module is displayed.
3. On the **Install Module** tab, select the Copy icon to copy the Install-Module command that installs version 1.2100.1396.426 of the Microsoft.AzureStack.ReadinessChecker.



The screenshot shows the PowerShell Gallery interface. At the top, there's a navigation bar with links for 'PowerShell Gallery', 'Packages', 'Publish', 'Statistics', 'Documentation', and 'Sign in'. Below the navigation bar is a search bar with the placeholder text 'Search PowerShell packages:' and a magnifying glass icon. The main content area displays the details for the 'Microsoft.AzureStack.ReadinessChecker' module. It includes the module name, version (1.2100.1780.756), a brief description ('Microsoft Azure Stack Readiness Checker'), download statistics (11,836 Downloads, 263 Downloads of 12100.1780.756), and a 'View full stats' link. It also shows the last published date (11/16/2021) and a 'Last Published' link. On the left, there are links for 'Info', 'Contact Owners', and 'Report'. The 'Installation Options' section contains three buttons: 'Install Module' (which is highlighted with a red box), 'Azure Automation', and 'Manual Download'. Below these buttons is a text box containing the PowerShell command 'PS> Install-Module -Name Microsoft.AzureStack.ReadinessChecker'. To the right of the command is a blue 'Copy' button, which is also highlighted with a red box.

4. Paste in the command at the PowerShell command prompt, and press **Enter**.

5. Press **Y** (Yes) or **A** (Yes to All) at the following prompt to install the module.

```
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the
modules from ' PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
```

Run a network readiness check

When you run the Azure Stack Network Readiness Checker tool, you'll need to provide network and device information from the [Deployment checklist for your Azure Stack Edge Pro GPU device](#).

To run a network readiness check, do these steps:

1. Open PowerShell on a client computer running on the network where you'll deploy the Azure Stack Edge

device.

- Run a network readiness check by entering the following command:

```
Invoke-AzsNetworkValidation -DnsServer <string[]> -DeviceFqdn <string> [-TimeServer <string[]>] `  
[-Proxy <uri>] [-ProxyCredential <pscredential>] [-WindowsUpdateServer <uri[]>] [-CustomUrl  
<url[]>] `  
[-AzureEnvironment {AzureCloud | AzureChinaCloud | AzureGermanCloud | AzureUSGovernment |  
CustomCloud}] `  
[-SkipTests {LinkLayer | Ipcfg | DnsServer | TimeServer | PathMtu | DuplicateIP | AzureEndpoint  
| WindowsUpdateServer | DnsRegistration}] `  
[-OutputPath <string>]
```

To get meaningful Network Readiness Checker results that find key issues in your network setup, you need to include all of the following parameters that apply to your environment.

PARAMETER	DESCRIPTION
<code>-DnsServer</code>	IP addresses of the DNS servers (for example, your primary and secondary DNS servers).
<code>-DeviceFqdn</code>	Fully qualified domain name (FQDN) that you plan to use for the Azure Stack Edge device.
<code>-TimeServer</code>	FQDN of one or more Network Time Protocol (NTP) servers. (Recommended)
<code>-Proxy</code>	URI for the proxy server, if you're using a proxy server. (Optional)
<code>-ProxyCredential</code>	PSCredential object containing the username and password used on the proxy server. (Required if proxy server requires user authentication)
<code>-WindowsUpdateServer</code>	URLs for one or more Windows Server Update Services (WSUS) servers. (Optional)
<code>-ComputeIPs</code>	The Compute IP range to be used by Kubernetes. Specify the Start IP and End IP separated by a hyphen.
<code>-CustomUrl</code>	Lists other URLs that you want to test HTTP access to. (Optional)
<code>-AzureEnvironment</code>	Indicates the Azure environment. Required if the device is deployed to an environment other than the Azure public cloud (Azure Cloud).
<code>-SkipTests</code>	Can be used to exclude tests. (Optional) Separate test names with a comma.
<code>-OutputPath</code>	Tells where to store the log file and report from the tests. (Optional) If you don't use this path, the files are stored in the following path: <code>C:\Users\<username>\AppData\Local\Temp\AzsReadinessChecker\</code> Each run of the Network Readiness Checker overwrites the existing report.

Sample output

The following samples are the output from successful and unsuccessful runs of the Azure Stack Network Readiness Checker tool.

Sample output: Successful test

The following sample is the output from a successful run of the Network Readiness Checker tool with these parameters:

```
Invoke-AzsNetworkValidation -DnsServer '10.50.10.50', '10.50.50.50' -DeviceFqdn 'aseclient.contoso.com' -TimeServer 'pool.ntp.org' -Proxy 'http://proxy.contoso.com:3128/' -SkipTests DuplicateIP -WindowsUpdateServer 'http://ase-prod.contoso.com' -OutputPath `C:\ase-network-tests`
```

The tool returned this output:

```
PS C:\Users\Administrator> Invoke-AzsNetworkValidation -DnsServer '10.50.10.50', '10.50.50.50' -DeviceFqdn 'aseclient.contoso.com' -TimeServer 'pool.ntp.org' -Proxy 'http://proxy.contoso.com:3128/' -SkipTests DuplicateIP -WindowsUpdateServer 'http://ase-prod.contoso.com' -OutputPath C:\ase-network-tests

Invoke-AzsNetworkValidation v1.2100.1396.426 started.
The following tests will be executed: LinkLayer, IPConfig, DnsServer, PathMtu, TimeServer, AzureEndpoint, WindowsUpdateServer, DnsRegistration, Proxy
Validating input parameters
Validating Azure Stack Edge Network Readiness
    Link Layer: OK
    IP Configuration: OK
Using network adapter name 'vEthernet (corp-1g-Static)', description 'Hyper-V Virtual Ethernet Adapter'
    DNS Server 10.50.10.50: OK
    DNS Server 10.50.50.50: OK
    Network Path MTU: OK
    Time Server pool.ntp.org: OK
    Proxy Server 10.57.48.80: OK
    Azure ARM Endpoint: OK
    Azure Graph Endpoint: OK
    Azure Login Endpoint: OK
    Azure ManagementService Endpoint: OK
    Azure AseService Endpoint: OK
    Azure AseServiceBus Endpoint: OK
    Azure AseStorageAccount Endpoint: OK
    Windows Update Server ase-prod.contoso.com port 80: OK
    DNS Registration for aseclient.contoso.com: OK
    DNS Registration for login.aseclient.contoso.com: OK
    DNS Registration for management.aseclient.contoso.com: OK
    DNS Registration for *.blob.aseclient.contoso.com: OK
    DNS Registration for compute.aseclient.contoso.com: OK

Log location (contains PII): C:\ase-network-tests\AzsReadinessChecker.log
Report location (contains PII): C:\ase-network-tests\AzsReadinessCheckerReport.json
Invoke-AzsNetworkValidation Completed
```

Sample output: Failed test

If a test fails, the Network Readiness Checker returns information to help you resolve the issue, as shown in the sample output below.

The following sample is the output from this command:

```
Invoke-AzsNetworkValidation -DnsServer '10.50.10.50' -TimeServer 'time.windows.com' -DeviceFqdn aseclient.contoso.com -ComputeIPs 10.10.52.1-10.10.52.20 -CustomUrl 'http://www.nytimes.com','http://fakename.fakeurl.com'
```

The tool returned this output:

```
PS C:\Users\Administrator> Invoke-AzsNetworkValidation -DnsServer '10.50.10.50' -TimeServer  
'time.windows.com' -DeviceFqdn aseclient.contoso.com -ComputeIPs 10.10.52.1-10.10.52.20 -CustomUrl  
'http://www.nytimes.com','http://fakename.fakeurl.com'

Invoke-AzsNetworkValidation v1.2100.1396.426 started.
Validating input parameters
The following tests will be executed: LinkLayer, IPConfig, DnsServer, PathMtu, TimeServer, AzureEndpoint,
WindowsUpdateServer, DuplicateIP, DnsRegistration, CustomUrl
Validating Azure Stack Edge Network Readiness
    Link Layer: OK
    IP Configuration: OK
    DNS Server 10.50.10.50: OK
    Network Path MTU: OK
    Time Server time.windows.com: OK
    Azure ARM Endpoint: OK
    Azure Graph Endpoint: OK
    Azure Login Endpoint: OK
    Azure ManagementService Endpoint: OK
    Azure AseService Endpoint: OK
    Azure AseServiceBus Endpoint: OK
    Azure AseStorageAccount Endpoint: OK
    URL http://www.nytimes.com/: OK
    URL http://fakename.fakeurl.com/: Fail
    Windows Update Server windowsupdate.microsoft.com port 80: OK
    Windows Update Server update.microsoft.com port 80: OK
    Windows Update Server update.microsoft.com port 443: OK
    Windows Update Server download.windowsupdate.com port 80: OK
    Windows Update Server download.microsoft.com port 443: OK
    Windows Update Server go.microsoft.com port 80: OK
    Duplicate IP: Warning
    DNS Registration for aseclient.contoso.com: OK
    DNS Registration for login.aseclient.contoso.com: Fail
    DNS Registration for management.aseclient.contoso.com: Fail
    DNS Registration for *.blob.aseclient.contoso.com: Fail
    DNS Registration for compute.aseclient.contoso.com: Fail
Details:
[-] URL http://fakename.fakeurl.com/: fakename.fakeurl.com : DNS name does not exist
[-] Duplicate IP: Some IP addresses allocated to Azure Stack may be active on the network. Check the output log for the detailed list.
[-] DNS Registration for login.aseclient.contoso.com: login.aseclient.contoso.com : DNS name does not exist
[-] DNS Registration for management.aseclient.contoso.com: management.aseclient.contoso.com : DNS name does not exist
[-] DNS Registration for *.blob.aseclient.contoso.com: testname.aseclient.contoso.com : DNS name does not exist
[-] DNS Registration for compute.aseclient.contoso.com: compute.aseclient.contoso.com : DNS name does not exist
Additional help URL http://aka.ms/azsnrc

Log location (contains PII): C:\Users\  
[*redacted*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessChecker.log
Report location (contains PII): C:\Users\  
[*redacted*]\AppData\Local\Temp\AzsReadinessChecker\AzsReadinessCheckerReport.json
Invoke-AzsNetworkValidation Completed
```

Review log and report

For more information, you can review the log and report. By default, both files are saved in the following location:

- Log: C:\Users\<username>\AppData\Local\Temp\AzsReadinessChecker\AzrReadinessChecker.log
- Report: C:\Users\<username>\AppData\Local\Temp\AzsReadinessChecker\AzrReadinessCheckerReport.json

Next steps

- Learn how to connect to your Azure Stack Edge device: [Pro GPU device](#), [Pro R device](#), [Mini R device](#).
- Review a deployment checklist for your device: [Pro GPU checklist](#), [Pro R checklist](#), [Mini R checklist](#).
- [Contact Microsoft Support](#).

Manage compute on your Azure Stack Edge Pro GPU

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to manage compute via IoT Edge service on your Azure Stack Edge Pro GPU device. You can manage the compute via the Azure portal or via the local web UI. Use the Azure portal to manage modules, triggers, and IoT Edge configuration, and the local web UI to manage compute network settings.

Manage triggers

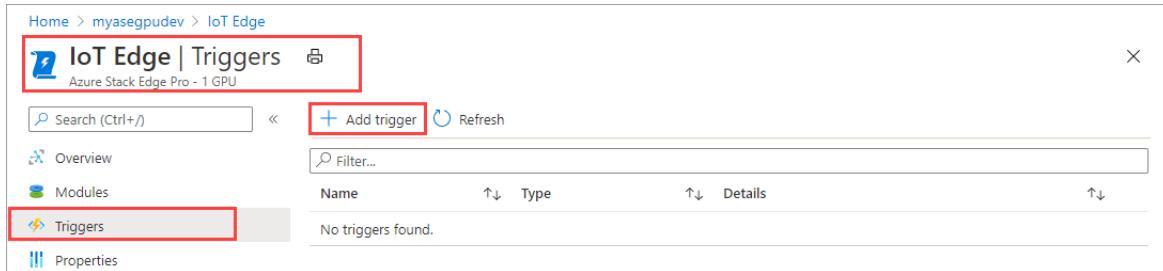
Events are things that happen within your cloud environment or on your device that you might want to take action on. For example, when a file is created in a share, it is an event. Triggers raise the events. For your Azure Stack Edge Pro, triggers can be in response to file events or a schedule.

- **File:** These triggers are in response to file events such as creation of a file, modification of a file.
- **Scheduled:** These triggers are in response to a schedule that you can define with a start date, start time, and the repeat interval.

Add a trigger

Take the following steps in the Azure portal to create a trigger.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge**. Go to **Triggers** and select **+ Add trigger** on the command bar.



2. In **Add trigger** blade, provide a unique name for your trigger.
3. Select a **Type** for the trigger. Choose **File** when the trigger is in response to a file event. Select **Scheduled** when you want the trigger to start at a defined time and run at a specified repeat interval. Depending on your selection, a different set of options is presented.
 - **File trigger** - Choose from the dropdown list a mounted share. When a file event is fired in this share, the trigger would invoke an Azure Function.

Add trigger

X

Triggers help invoke functions in a module. Triggers can be file event or scheduled. [Learn more](#)

Name *

myasettrigger1



Type * ⓘ

File (When file is written to input share)



Input Edge local share * ⓘ

myasesmblocalshare1



Add

- **Scheduled trigger** - Specify the start date/time, and the repeat interval in hours, minutes, or seconds. Also, enter the name for a topic. A topic will give you the flexibility to route the trigger to a module deployed on the device.

An example route string is:

```
"route3": "FROM /* WHERE topic = 'topicname' INTO  
BrokeredEndpoint(\"modules/modulename/inputs/input1\")"
```

Add trigger

X

Triggers help invoke functions in a module. Triggers can be file event or scheduled. [Learn more](#)

Name *

myasettrigger2



Type * ⓘ

Scheduled (Run at repeat interval)



Start date & time * ⓘ

01/27/2021



6:28:15 PM

Repeat interval * ⓘ

2



Minutes



Topic * ⓘ

mytopic1



Add

4. Select **Add** to create the trigger. A notification shows that the trigger creation is in progress. After the trigger is created, the blade updates to reflect the new trigger.

Home > myaseguudev > IoT Edge

IoT Edge | Triggers

Azure Stack Edge Pro - 1 GPU

Search (Ctrl+J)

+ Add trigger



Refresh

Overview

Modules

Triggers

Properties

Name	Type	Details	⋮
myasettrigger1	File	Associated share: myasesmblocalshare1	⋮
myasettrigger2	Scheduled	Scheduled start: 1/27/2021, 18:28:15, Repeat interval: Every 2 ...	⋮

Delete a trigger

Take the following steps in the Azure portal to delete a trigger.

- From the list of triggers, select the trigger that you want to delete.

Name	Type	Details
myasetrigger1	File	Associated share: myasesmblocalshare1
myasetrigger2	Scheduled	Scheduled start: 1/27/2021, 18:28:15, Repeat interval: Every 2 ...

- Right-click and then select **Delete**.

Name	Type	Details
myasetrigger1	File	Associated share: myasesmblocalshare1
myasetrigger2	Scheduled	Scheduled start: 1/27/2021, 18:28:15, Repeat interval: Every 2 ...

- When prompted for confirmation, click **Yes**.

Do you want to delete this trigger?

You are about to delete the trigger 'myasetrigger1'. Modules using this trigger will not be able to emit events. Are you sure you want to delete this trigger?

OK **Cancel**

The list of triggers updates to reflect the deletion.

Manage IoT Edge configuration

Use the Azure portal to view the compute configuration, remove an existing compute configuration, or to refresh the compute configuration to sync up access keys for the IoT device and IoT Edge device for your Azure Stack Edge Pro.

View IoT Edge configuration

Take the following steps in the Azure portal to view the IoT Edge configuration for your device.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge**. After IoT Edge service is enabled on your device, the Overview page indicates that the IoT Edge service is running fine.

The screenshot shows the IoT Edge Overview page. At the top, it says "IoT Edge | Overview" and "Azure Stack Edge Pro - 1 GPU". Below that is a search bar and a command bar with "Add module", "Add trigger", "Refresh configuration", "Remove", and "Refresh". On the left, there's a navigation menu with "Overview", "Modules", "Triggers", and "Properties". The main area has a message "IoT Edge service is running fine!" followed by "Start processing the data using IoT Edge modules. [Learn more](#)". Under "Modules", it says "IoT Edge modules are containers that run Azure services, third-party services, or your own code." and "To read data from Edge local shares for processing and uploading it to cloud, add a Module. If multiple containers are deployed, which are chained together for pipeline processing, go to [Azure IoT Hub](#)". There's a "Add module" button. To the right, under "Triggers", it shows "Total 2 No" with entries "myasetrigger1" and "myasetrigger2", and a link "View all triggers".

2. Go to **Properties** to view the IoT Edge configuration on your device. When you configured compute, you created an IoT Hub resource. Under that IoT Hub resource, an IoT device and an IoT Edge device are configured. Only the Linux modules are supported to run on the IoT Edge device.

The screenshot shows the IoT Edge Properties page. At the top, it says "Home > myasegpudev > IoT Edge" and "IoT Edge | Properties" with "Azure Stack Edge Pro - 1 GPU". Below that is a search bar and a command bar with "Refresh". On the left, there's a navigation menu with "Overview", "Modules", "Triggers", and "Properties" (which is highlighted with a red box). The main area shows configuration details in a table:

IoT Hub	ase-myasegpudev-64cba977d9dec37033a44ec0b783fada5d
IoT Edge device	myasegpudev-edge
IoT device for storage gateway	myasegpudev-storageegateway
Platform	Linux

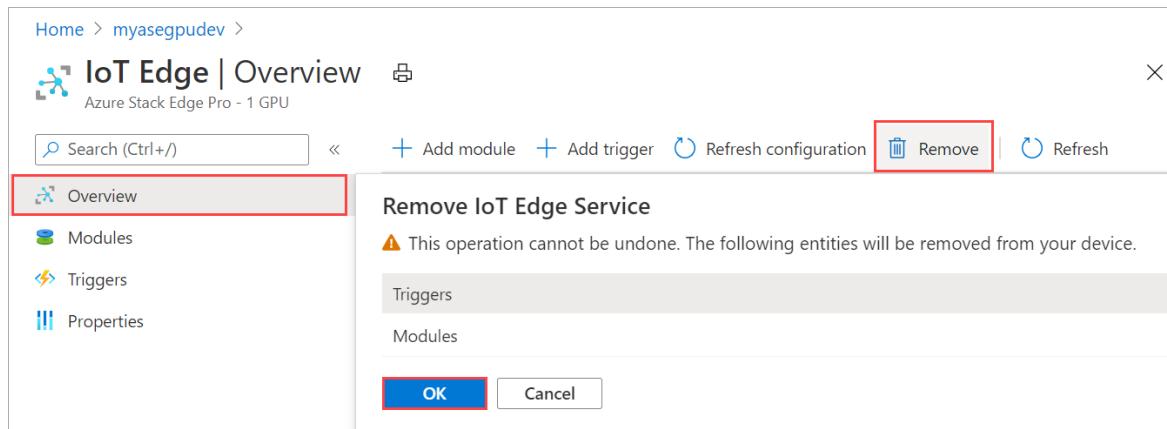
Remove IoT Edge service

Take the following steps in the Azure portal to remove the existing IoT Edge configuration for your device.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge**. Go to **Overview** and select **Remove** on the command bar.

The screenshot shows the IoT Edge Overview page. At the top, it says "Home > myasegpudev > IoT Edge | Overview" and "Azure Stack Edge Pro - 1 GPU". Below that is a search bar and a command bar with "Add module", "Add trigger", "Refresh configuration", "Remove" (which is highlighted with a red box), and "Refresh". On the left, there's a navigation menu with "Overview" (highlighted with a red box), "Modules", "Triggers", and "Properties". The main area has a message "IoT Edge service is running fine!" followed by "Start processing the data using IoT Edge modules. [Learn more](#)".

2. If you remove the IoT Edge service, the action is irreversible and can't be undone. The modules and triggers that you created will also be deleted. You will need to reconfigure your device in case you need to use IoT Edge again. When prompted for confirmation, select **OK**.



Sync up IoT device and IoT Edge device access keys

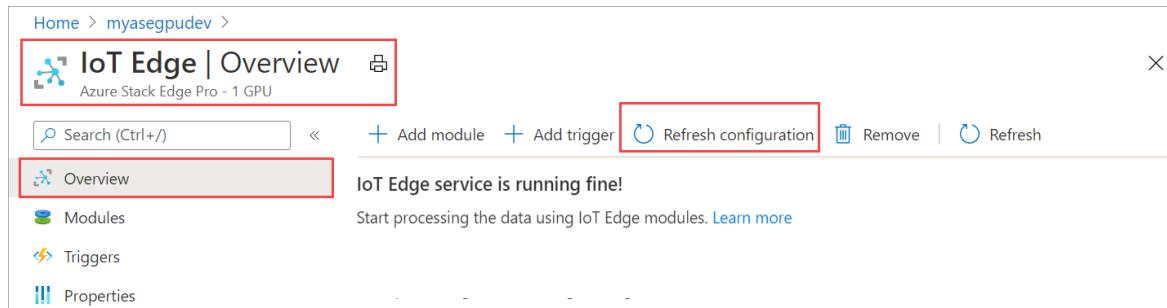
When you configure compute on your Azure Stack Edge Pro, an IoT device and an IoT Edge device are created. These devices are automatically assigned symmetric access keys. As a security best practice, these keys are rotated regularly via the IoT Hub service.

To rotate these keys, you can go to the IoT Hub service that you created and select the IoT device or the IoT Edge device. Each device has a primary access key and a secondary access keys. Assign the primary access key to the secondary access key and then regenerate the primary access key.

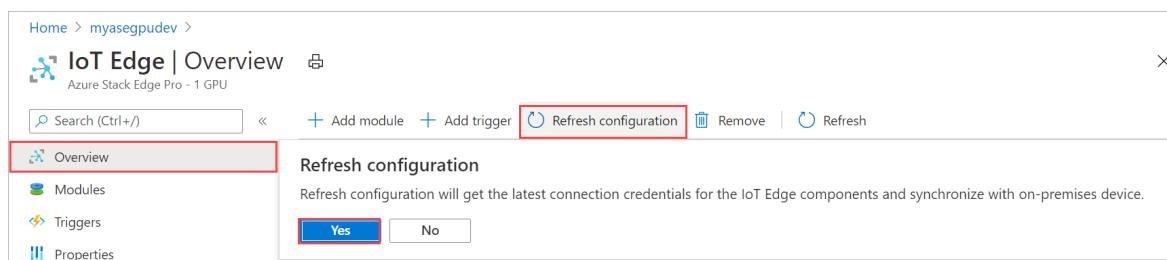
If your IoT device and IoT Edge device keys have been rotated, then you need to refresh the configuration on your Azure Stack Edge Pro to get the latest access keys. The sync helps the device get the latest keys for your IoT device and IoT Edge device. Azure Stack Edge Pro uses only the primary access keys.

Take the following steps in the Azure portal to sync the access keys for your device.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge compute**. Go to **Overview** and select **Refresh configuration** on the command bar.



2. Select **Yes** when prompted for confirmation.



3. Exit out of the dialog once the sync is complete.

Change external service IPs for containers

Kubernetes external service IPs are used to reach out to services that are exposed outside the Kubernetes cluster. After your device is activated, you can set or modify the external service IPs for containerized workloads for your device by accessing the local UI.

1. In the local UI of the device, go to **Compute**.
2. Select the port whose network is configured for compute. In the blade that opens up, specify (new) or modify (if existing) the Kubernetes external service IPs. These IPs are used for any services that need to be exposed outside of the Kubernetes cluster.
 - You need a minimum of 1 service IP for the `edgehub` service that runs on your device and is used by IoT Edge modules.
 - You will need an IP for each additional IoT Edge module or container that you intend to deploy.
 - These are static, contiguous IPs.

The screenshot shows the Azure Stack Edge Pro (1 GPU) local UI. On the left, the navigation menu includes Overview, Configuration (Get started, Network, Compute, Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change, Device reset), and Troubleshooting. The Compute option is selected and highlighted with a red box. On the right, the 'Compute' blade is open, showing 'Network settings (Port2)'.

Name	Network	Enabled
Port 1	192.168.100.0	No
Port 2	10.57.48.0	Yes
Port 3	192.168.0.0	No
Port 4	192.168.0.0	No
Port 5	192.168.0.0	No
Port 6	192.168.0.0	No

Network settings (Port2)

- Enable for compute:** Yes No
- Compute is enabled on this network interface.**
- Compute IPs:** For container based workloads (IoT/Kubernetes), specify the following IP ranges on this network:
10.57.48.60-10.57.48.61
- Kubernetes node IPs:** Enter a contiguous range of 2 static IPs for your device.
10.57.48.62-10.57.48.69
- Kubernetes external service IPs:** Specify the static IP range for services exposed outside of Kubernetes cluster.

Apply

3. Select **Apply**. After the IPs are applied, your device does not need a restart or a reboot. The new IPs take effect immediately.

Next steps

- Learn how to [troubleshoot IoT Edge issues on your Azure Stack Edge Pro GPU device](#).

Enable Edge container registry on your Azure Stack Edge Pro GPU device

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to enable the Edge container registry and use it from within the Kubernetes cluster on your Azure Stack Edge Pro device. The example used in the article details how to push an image from a source registry, in this case, Microsoft Container registry, to the registry on the Azure Stack Edge device, the Edge container registry.

About Edge container registry

Containerized compute applications run on container images and these images are stored in registries. Registries can be public such as Docker Hub, private, or cloud provider managed such as Azure Container Registry. For more information, see [About registries, repositories, and images](#).

An Edge container registry provides a repository at the Edge, on your Azure Stack Edge Pro device. You can use this registry to store and manage your private container images.

In a multi-node environment, container images can be downloaded and pushed to the Edge container registry once. All Edge applications can use the Edge container registry for subsequent deployments.

Prerequisites

Before you begin, make sure that:

1. You've access to an Azure Stack Edge Pro device.
2. You've activated your Azure Stack Edge Pro device as described in [Activate Azure Stack Edge Pro](#).
3. You've enabled compute role on the device. A Kubernetes cluster was also created on the device when you configured compute on the device as per the instructions in [Configure compute on your Azure Stack Edge Pro device](#).
4. You have the Kubernetes API endpoint from the **Device** page of your local web UI. For more information, see the instructions in [Get Kubernetes API endpoint](#).
5. You've access to a client system with a [Supported operating system](#). If using a Windows client, the system should run PowerShell 5.0 or later to access the device.
 - a. If you want to pull and push your own container images, make sure that the system has Docker client installed. If using a Windows client, [Install Docker Desktop on Windows](#).

Enable container registry as add-on

The first step is to enable the Edge container registry as an add-on.

1. [Connect to the PowerShell interface of the device](#).
2. To enable the container registry as an add-on, type:

```
Set-HcsKubernetesContainerRegistry
```

This operation may take several minutes to complete.

Here is the sample output of this command:

```
[10.128.44.40]: PS>Set-HcsKubernetesContainerRegistry  
Operation completed successfully. Use Get-HcsKubernetesContainerRegistryInfo for credentials
```

3. To get the container registry details, type:

```
Get-HcsKubernetesContainerRegistryInfo
```

Here is the sample out of this command:

```
[10.128.44.40]: PS> Get-HcsKubernetesContainerRegistryInfo  
  
Endpoint IPAddress Username Password  
----- -----  
ecr.dbe-hw6h1t2.microsoftdatabox.com:31001 10.128.44.41 ase-ecr-user i3eTsU4zGYyIgxV
```

4. Make a note of the username and the password from the output of

`Get-HcsKubernetesContainerRegistryInfo`. These credentials are used to sign in to the Edge container registry while pushing images.

Manage container registry images

You may want to access the container registry from outside of your Azure Stack Edge device. You may also want to push or pull images in the registry.

Follow these steps to access Edge container registry:

1. Get the endpoint details for the Edge container registry.

a. In the local UI of the device, go to **Device**.

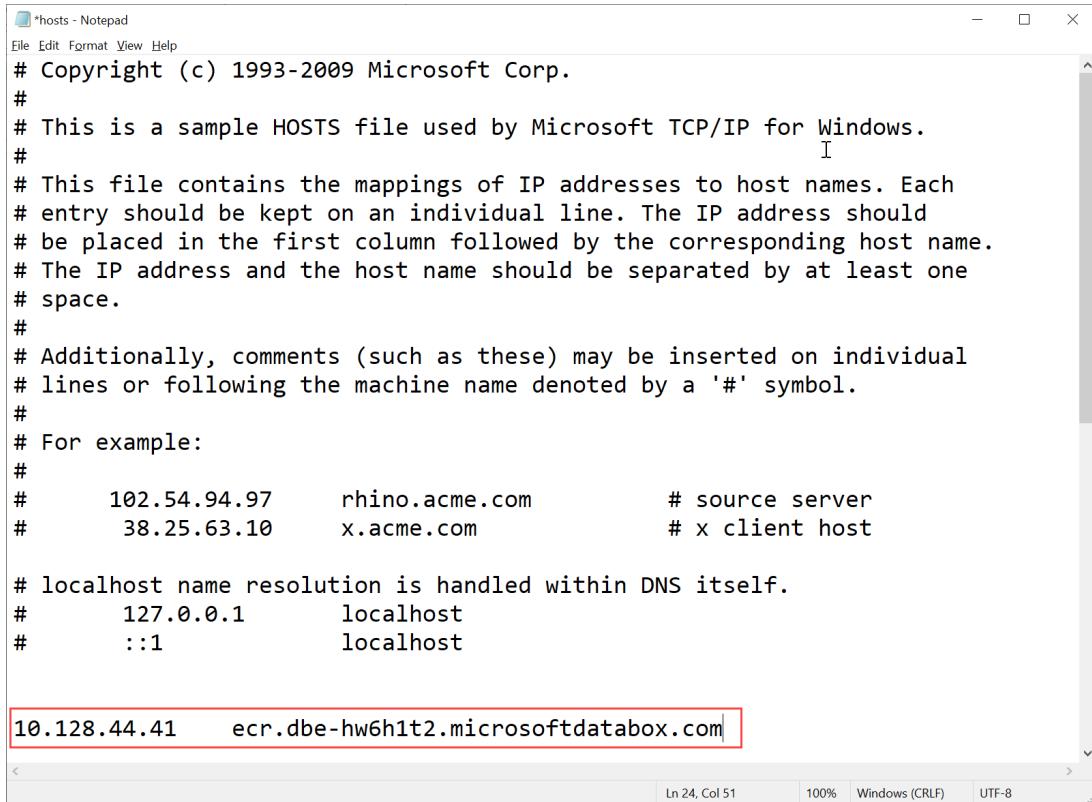
b. Locate the **Edge container registry endpoint**.

Service	Certificate Required	Endpoint
SMB server	No	\dbe-hw6h1t2.microsoftdatabox.com\{Share name}
NFS server	No	\{Device IP address\}\{Share name\}
Azure Resource Manager login	Yes	https://login.dbe-hw6h1t2.microsoftdatabox.com
Azure Resource Manager	Yes	https://management.dbe-hw6h1t2.microsoftdatabox.com
Blob Storage	Yes	https://[Account name].blob.dbe-hw6h1t2.microsoftdatabox.com
Kubernetes API	No	compute.dbe-hw6h1t2.microsoftdatabox.com [10.128.44.41] Advanced config
Kubernetes dashboard	No	https://10.128.44.41:31000 Download config
Edge IoT hub	Yes	diptipai-update-2011b-2-edge [10.128.44.43]
Edge container registry	Yes	ecr.dbe-hw6h1t2.microsoftdatabox.com:31001 [10.128.44.41]

- c. Copy this endpoint and create a corresponding DNS entry into the

`C:\Windows\System32\Drivers\etc\hosts` file of your client to connect to the Edge container registry endpoint.

<IP address of the Kubernetes main node> <Edge container registry endpoint>

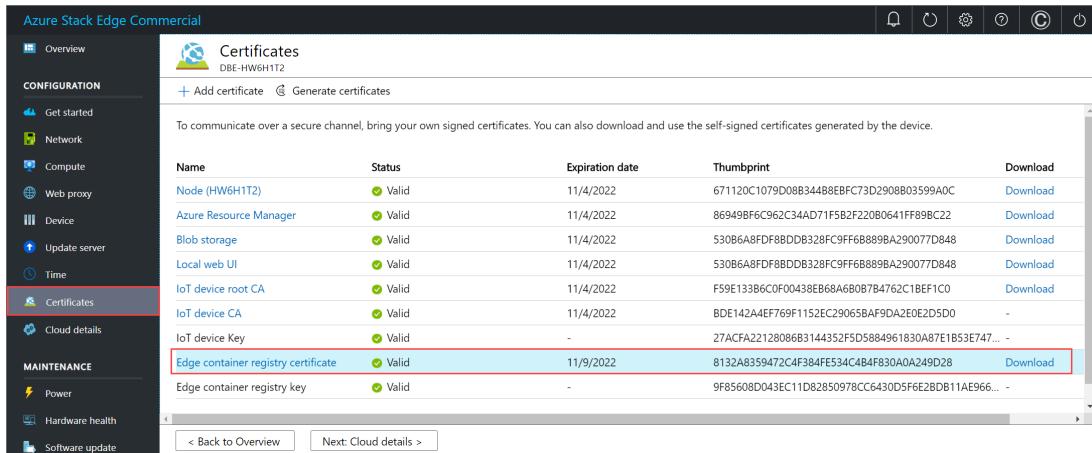


```
*hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com          # source server
#      38.25.63.10       x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost

10.128.44.41      ecr.dbe-hw6h1t2.microsoftdatabox.com
```

2. Download the Edge container registry certificate from Local UI.

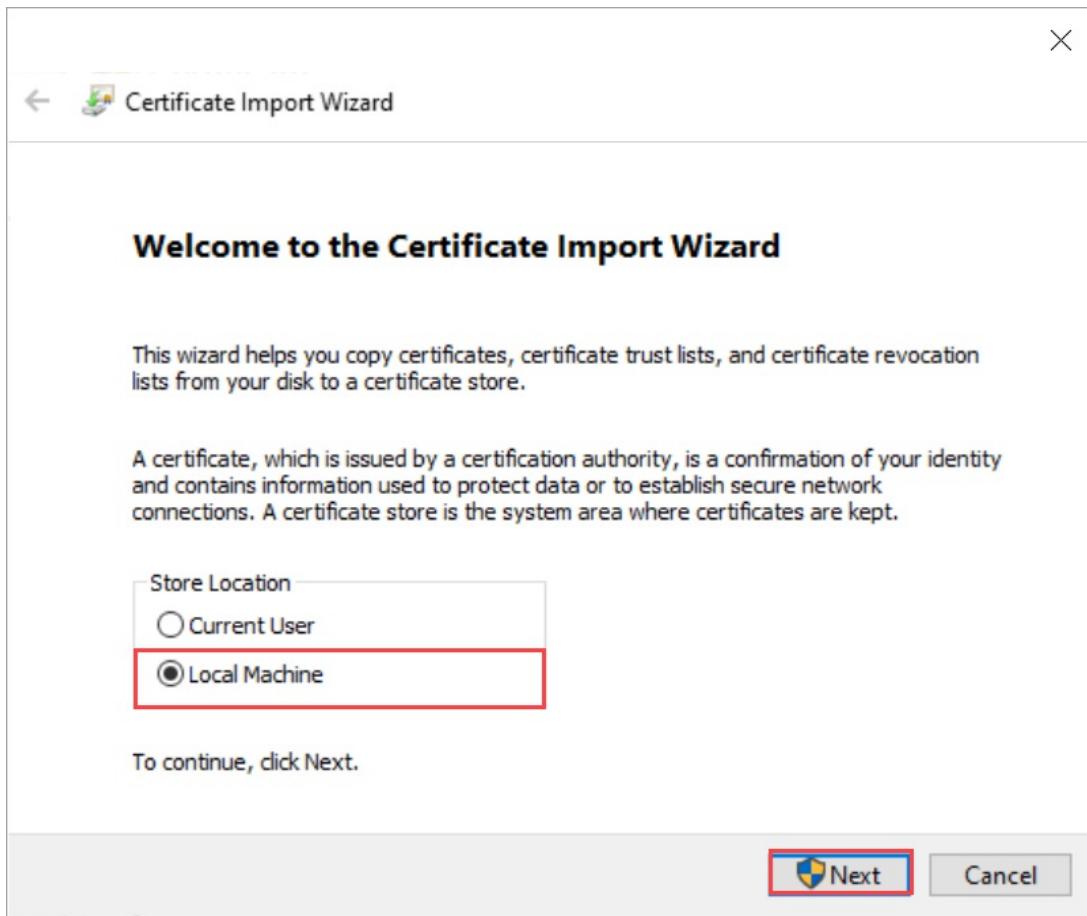
- In the local UI of the device, go to **Certificates**.
- Locate the entry for **Edge container registry certificate**. To the right of this entry, select the **Download** to download the Edge container registry certificate on your client system that you'll use to access your device.



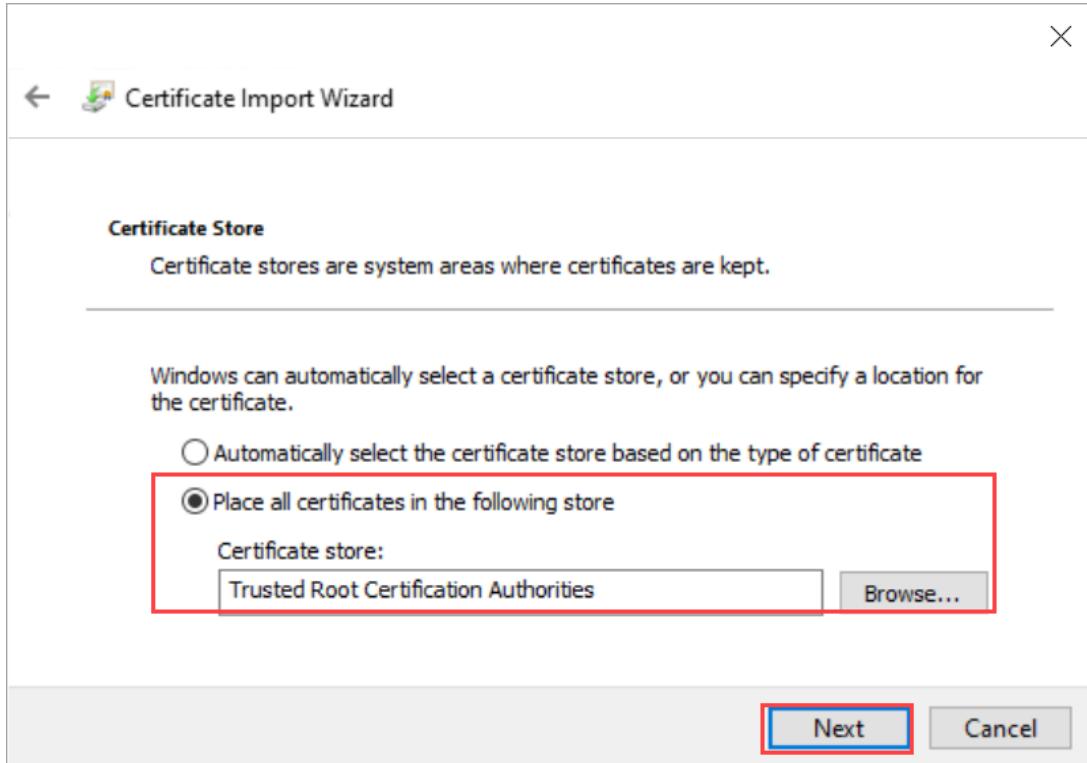
Name	Status	Expiration date	Thumbprint	Download
Node (HW6H1T2)	Valid	11/4/2022	671120C1079D08B344B8EBFC73D2908B03599A0C	Download
Azure Resource Manager	Valid	11/4/2022	86949BF6C962C34AD71F5B2F220B0641FF89BC22	Download
Blob storage	Valid	11/4/2022	530B6A8DF8BDB328FC9FF6B889BA290077D848	Download
Local web UI	Valid	11/4/2022	530B6A8DF8BDB328FC9FF6B889BA290077D848	Download
IoT device root CA	Valid	11/4/2022	F59E133B6C0F00438EB68A6B0B7B4762C1BEF1C0	Download
IoT device CA	Valid	11/4/2022	BDE142A4EF769F1152EC29065BA9D2E0E2D5D0	-
IoT device Key	Valid	-	27ACFA22128086B314435F5D5884961830A87E1B53E747...	-
Edge container registry certificate	Valid	11/9/2022	8132A8359472C4F384FE534C4BAFB30A0A249D28	Download
Edge container registry key	Valid	-	9F85608D043EC11D82850978CC6430D5F6E2BD11AE966...	-

3. Install the downloaded certificate on the client. If using a Windows client, follow these steps:

- Select the certificate and in the **Certificate Import Wizard**, select store location as **Local machine**.



- b. Install the certificate on your Local machine in the trusted root store.



4. After the certificate is installed, restart the Docker client on your system.

5. Sign into the Edge container registry. Type:

```
docker login <Edge container registry endpoint> -u <username> -p <password>
```

Provide the Edge container registry endpoint from the Devices page, and the username and password that you got from the output of `Get-HcsKubernetesContainerRegistryInfo`.

6. Use docker push or pull commands to push or pull container images from the container registry.

- Pull an image from the Microsoft Container Registry image. Type:

```
docker pull <Full path to the container image in the Microsoft Container Registry>
```

- Create an alias of the image you pulled with the fully qualified path to your registry.

```
docker tag <Path to the image in the Microsoft container registry> <Path to the image in the Edge container registry/Image name with tag>
```

- Push the image to your registry.

```
docker push <Path to the image in the Edge container registry/Image name with tag>
```

- Run the image you pushed into your registry.

```
docker run -it --rm -p 8080:80 <Path to the image in the Edge container registry/Image name with tag>
```

Here is a sample output of the pull and push commands:

```
PS C:\WINDOWS\system32> docker login ecr.dbe-hw6h1t2.microsoftdatabox.com:31001 -u ase-ecr-user -p 3bb02s0tDe8FouD
WARNING! Using --password via the CLI is insecure. Use --password-stdin.
Login Succeeded
PS C:\WINDOWS\system32> docker pull mcr.microsoft.com/oss/nginx/nginx:1.17.5-alpine
1.17.5-alpine: Pulling from oss/nginx/nginx
Digest: sha256:5466bbc0a989bd1cd283c0ba86d9c2fc133491ccfaea63160089f47b32ae973b
Status: Image is up to date for mcr.microsoft.com/oss/nginx/nginx:1.17.5-alpine
mcr.microsoft.com/oss/nginx/nginx:1.17.5-alpine
PS C:\WINDOWS\system32> docker tag mcr.microsoft.com/oss/nginx/nginx:1.17.5-alpine ecr.dbe-hw6h1t2.microsoftdatabox.com:31001/nginx:2.0
PS C:\WINDOWS\system32> docker push ecr.dbe-hw6h1t2.microsoftdatabox.com:31001/nginx:2.0
The push refers to repository [ecr.dbe-hw6h1t2.microsoftdatabox.com:31001/nginx]
bba7d2385bc1: Pushed
77cae8ab23bf: Pushed
2.0: digest: sha256:b4c0378c841cd76f0b75bc63454bfc6fe194a5220d4eab0d75963bccdbc327ff size: 739
PS C:\WINDOWS\system32> docker run -it --rm -p 8080:80 ecr.dbe-hw6h1t2.microsoftdatabox.com:31001/nginx:2.0
2020/11/10 00:00:49 [error] 6#6: *1 open() "/usr/share/nginx/html/favicon.ico" failed (2: No such file or directory), client: 172.17.0.1, server: localhost, request: "GET /favicon.ico HTTP/1.1", host: "localhost:8080", referrer: "http://localhost:8080/"
172.17.0.1 - - [10/Nov/2020:00:00:49 +0000] "GET /favicon.ico HTTP/1.1" 404 555
"http://localhost:8080/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36" "-"
^C
PS C:\WINDOWS\system32>
```

7. Browse to <http://localhost:8080> to view the running container. In this case, you will see the nginx webserver running.



To stop and remove the container, press `Control+C`.

Use Edge container registry images via Kubernetes pods

You can now deploy the image that you pushed in your Edge container registry from within the Kubernetes pods.

1. To deploy the image, you need to configure cluster access via `kubectl`. Create a namespace, a user, grant user access to the namespace, and get a `config` file. Make sure that you can connect to the Kubernetes pods.

Follow all the steps in [Connect to and manage a Kubernetes cluster via kubectl on your Azure Stack Edge Pro GPU device](#).

Here is a sample output for a namespace on your device from where the user can access the Kubernetes cluster.

```
[10.128.44.40]: PS>New-HcsKubernetesNamespace -Namespace myecr
[10.128.44.40]: PS>New-HcsKubernetesUser -UserName ecruser
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data:
LS0tLS1CRUDJTibDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ01CQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTJVJNd
0VRWURWUWFERXdwcmRXsmwKY201bGRHVnpNQjRYRFRJd01URxdOVEF6TkRJe1Gb1hEVE13TVRFd016QXpORE16TUZvd0ZURVRNQk
VnNjOVRLWndCQ042cm1XQms2eXFwcXI1MUx6bApTaXMyTy91UEJ2YXNSSUUzdzgrbmEwdG1aTERZZ2F6MkQwMm42Q29mUmtyUTR2d
11LTnR1M1pzR3pUdz0KLS0tLS1FTkQgQ0VSVE1GSUNBVEutLS0tLQo=
  server: https://compute.dbe-hw6h1t2.microsoftdatabox.com:6443
  name: kubernetes
=====CUT=====
  client-certificate-data:
LS0tLS1CRUDJTibDRVJUSUZJQ0FURS0tLS0tCk1JSUNwRENDQWJpZ0F3SUJBZ01JYmVWRGJSTzZ3e113RFFZSkvWk1odmNOQVFfT
EJRQXdGVEVUTUJFR0ExVUUKQXhNS2EzVm1aWEp1WhSbGN6QnVGdzB5TURFe1EVXdne1F5TxpCYUZ3Mh1nVEV4TURreU16UTRNal
=====CUT=====

DMVUvN31FOG5UU3k3b2VPWitUeHdzCjF1UDByMjhDZ11CdHdRY0ZpcFh1b1N5ak16dTNIYjhveFI2V3VwWmZ1dFFKNE1KWEFXOSTv
WGhKTfhyQ2x4bUckWHRtbCt4U05UTzFjQVNKRVZWVWdd6Tjg2ay9kSu43S3JIvkdUdUx1UDd4eGVjV2VRcWJrZEVSscUsxN01iTxpiV
ApmbnNx0dobEdmLzdM21kTGty0ENrcWs5TU5aM3MvUVIwR1FCdk94ZVpuUlptTeVgbUR5S1E9PQotLS0tLUVORCBSU0EgUFJJVk
FURSBLRVktLS0tLQo=


[10.128.44.40]: PS>Grant-HcsKubernetesNamespaceAccess -Namespace myecr -UserName ecruser
[10.128.44.40]: PS>kubectl get pods -n "myecr"
No resources found.
PS C:\WINDOWS\system32>
```

2. The image pull secrets are already set in all the Kubernetes namespaces on your device. You can get secrets by using the `get secrets` command. Here is a sample output:

```

PS C:\WINDOWS\system32> .\kubectl.exe get secrets -n myecr
NAME          TYPE           DATA   AGE
ase-ecr-credentials  kubernetes.io/dockerconfigjson  1      99m
default-token-c7kww  kubernetes.io/service-account-token  3      107m
sec-smbcredentials  microsoft.com/smb                2      99m
PS C:\WINDOWS\system32>

```

3. Deploy a pod to your namespace using kubectl. Use the following `yaml`.

Replace the image: `<image-name>` with the image pushed to the container registry. Refer to the secrets in your namespaces using `imagePullSecrets` with a name: `ase-ecr-credentials`.

```

apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - name: nginx
    image: ecr.dbe-hw6h1t2.microsoftdatobox.com:31001/nginx:2.0
    imagePullPolicy: Always
  imagePullSecrets:
  - name: ase-ecr-credentials

```

4. Apply the deployment in the namespace you created using the `apply` command. Verify that the container is running. Here is a sample output:

```

PS C:\Windows\System32> .\kubectl.exe apply -f ./deployment.yaml -n myecr
pod/nginx configured
PS C:\Windows\System32> .\kubectl.exe get pods -n myecr
NAME     READY   STATUS    RESTARTS   AGE
nginx   1/1     Running   0          27m
PS C:\Windows\System32>

```

Delete container registry images

Edge Container Registry storage is hosted on a local share within your Azure Stack Edge Pro device which is limited by the available storage on the device. It is your responsibility to delete unused docker images from the container registry using Docker HTTP v2 API (<https://docs.docker.com/registry/spec/api/>).

To remove one or more container images, follow these steps:

1. Set the image name to the image you want to delete.

```

PS C:\WINDOWS\system32> $imageName="nginx"

```

2. Set the username and password of the container registry as a PS credential

```

PS C:\WINDOWS\system32> $username="ase-ecr-user"
PS C:\WINDOWS\system32> $password="3bbo2s0tDe8FouD"
PS C:\WINDOWS\system32> $securePassword = ConvertTo-SecureString $password -AsPlainText -Force
PS C:\WINDOWS\system32> $credential = New-Object System.Management.Automation.PSCredential
($username, $securePassword)

```

3. List the tags associated with the image

```
PS C:\WINDOWS\system32> $tags = Invoke-RestMethod -Credential $credential -Uri "https://ecr.dbe-hw6h1t2.microsoftdatobox.com:31001/v2/nginx/tags/list" | Select-Object -ExpandProperty tags
PS C:\WINDOWS\system32> $tags
2.0
PS C:\WINDOWS\system32> $tags = Invoke-RestMethod -Credential $credential -Uri "https://ecr.dbe-hw6h1t2.microsoftdatobox.com:31001/v2/$imageName/tags/list" | Select-Object -ExpandProperty tags
PS C:\WINDOWS\system32> $tags
2.0
PS C:\WINDOWS\system32>
```

4. List the digest associated with the tag you would like to delete. This uses \$tags from the output of above command. If you have multiple tags, select one of them and use in the next command.

```
PS C:\WINDOWS\system32> $response = Invoke-WebRequest -Method Head -Credential $credential -Uri "https://ecr.dbe-hw6h1t2.microsoftdatobox.com:31001/v2/$imageName/manifests/$tags" -Headers @{
    'Accept' = 'application/vnd.docker.distribution.manifest.v2+json' }
PS C:\WINDOWS\system32> $digest = $response.Headers['Docker-Content-Digest']
PS C:\WINDOWS\system32> $digest
sha256:b4c0378c841cd76f0b75bc63454bfc6fe194a5220d4eab0d75963bccdbc327ff
PS C:\WINDOWS\system32>
```

5. Delete the image using the digest of the image:tag

```
PS C:\WINDOWS\system32> Invoke-WebRequest -Method Delete -Credential $credential -Uri "https://ecr.dbe-hw6h1t2.microsoftdatobox.com:31001/v2/$imageName/manifests/$digest" | Select-Object -ExpandProperty StatusDescription
```

After you delete the unused images, the space associated with the unreferenced images is automatically reclaimed by a process that runs nightly.

Next steps

- [Deploy a stateless application on your Azure Stack Edge Pro.](#)

Manage access, power, and connectivity mode for your Azure Stack Edge Pro GPU

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to manage the access, power, and connectivity mode for your Azure Stack Edge Pro with GPU device. These operations are performed via the local web UI or the Azure portal.

In this article, you learn how to:

- Manage device access
- Enable device access via remote PowerShell over HTTP
- Enable device access from outside network
- Manage resource access
- Manage connectivity mode
- Manage power

Manage device access

The access to your Azure Stack Edge Pro device is controlled by the use of a device password. You can change the password via the local web UI. You can also reset the device password in the Azure portal.

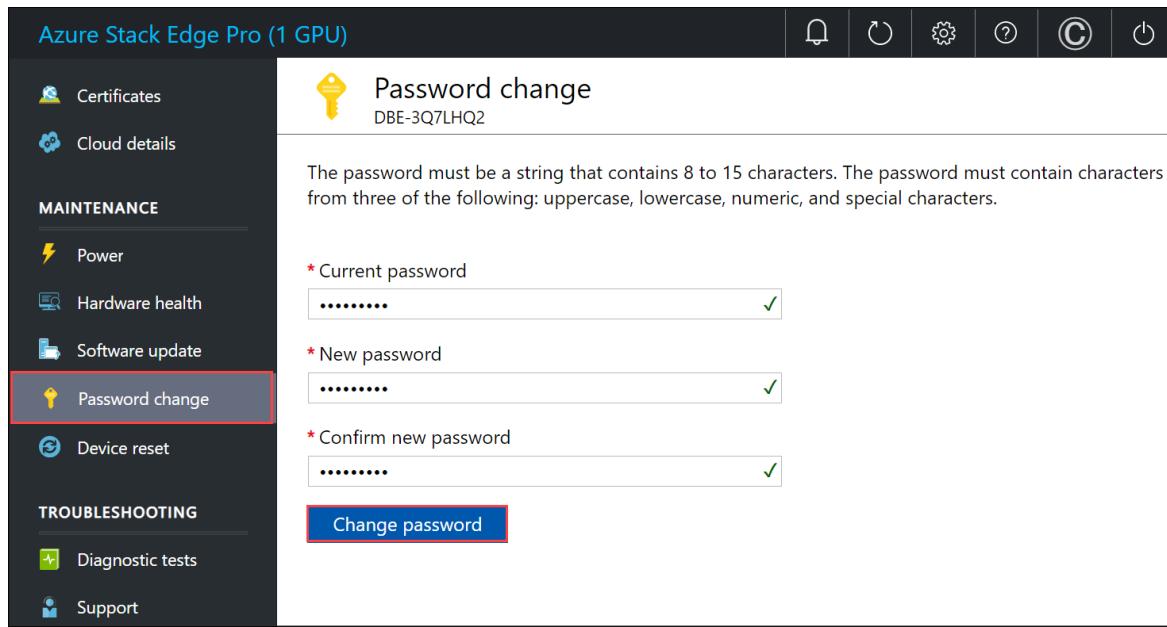
The access to data on the device disks is also controlled by encryption-at-rest keys.

You can access the device by opening a remote PowerShell session over HTTP or HTTPS from the local web UI of the device.

Change device password

Follow these steps in the local UI to change the device password.

1. In the local web UI, go to **Maintenance > Password**.
2. Enter the current password and then the new password. The supplied password must be between 8 and 16 characters. The password must have 3 of the following characters: uppercase, lowercase, numeric, and special characters. Confirm the new password.



3. Select Change password.

Reset device password

The reset workflow does not require the user to recall the old password and is useful when the password is lost. This workflow is performed in the Azure portal.

1. In the Azure portal, go to Overview > Reset admin password.

The screenshot shows the Azure portal's 'Overview' page for a device named 'myasegpudev'. The left sidebar has sections like Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Properties, Order details, Edge services, Virtual machines, IoT Edge, Cloud storage gateway, and Monitoring. The main area shows a message 'Your device is running fine!' and a table for 'Deployed edge services' with one entry: 'IoT Edge' status 'Running'. Below that is a section for 'Edge services' with three cards: 'Virtual machines' (New), 'IoT Edge' (How to get started?), and 'Cloud storage gateway' (How to get started?). At the top, there's a navigation bar with 'Update device', 'Reset device password' (highlighted with a red box), 'Return device', 'Feedback', 'Delete', and 'Refresh' buttons. There are also 'View Cost' and 'JSON View' links.

2. Enter the new password and then confirm it. The supplied password must be between 8 and 16 characters. The password must have 3 of the following characters: uppercase, lowercase, numeric, and special characters. Select Reset.

The screenshot shows a 'Reset device password' dialog box. It has a title 'Reset device password' and a subtitle 'MyAzureStackEdge1'. It contains two input fields: 'New password' (containing '*****') and 'Confirm password' (containing '*****'). Both fields have green checkmarks indicating they are valid. At the bottom is a large blue 'Reset' button.

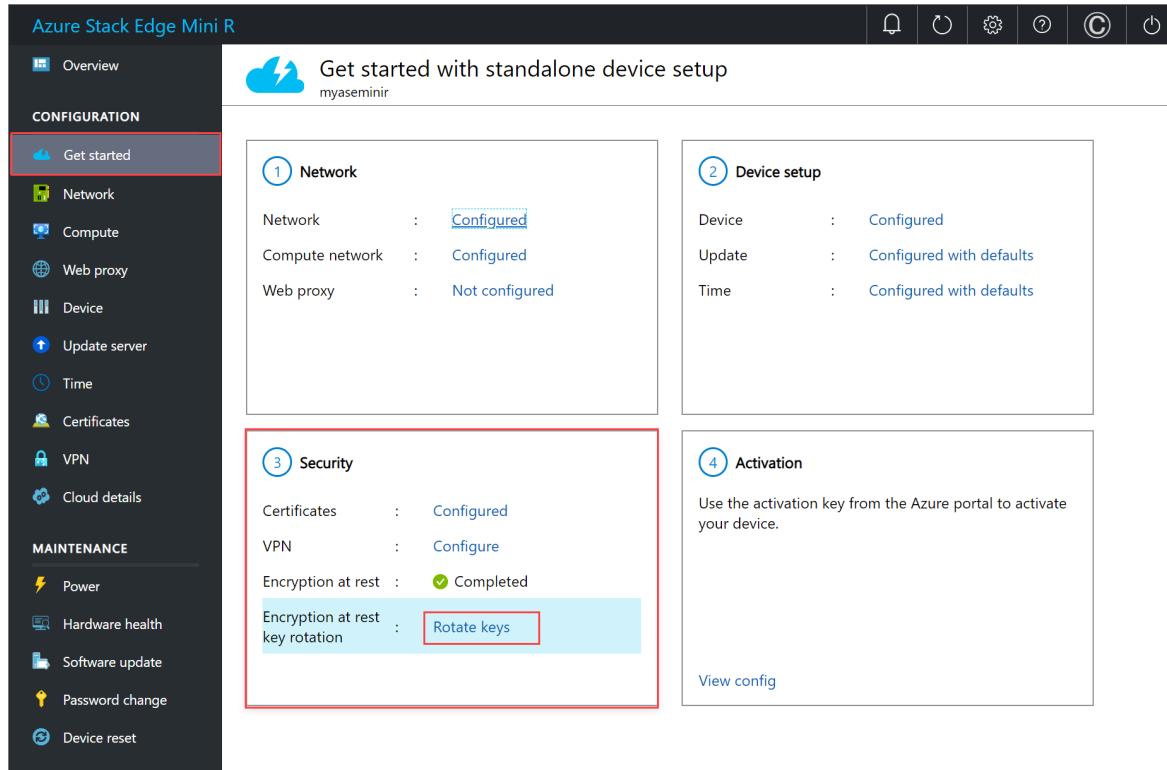
Manage access to device data

For the Azure Stack Edge Pro R and Azure Stack Edge Mini R devices, the access to device data is controlled by using encryption-at-rest keys for the device drives. After you have successfully configured the device for encryption-at-rest, the rotate encryption-at-rest keys option becomes available in the local UI of the device.

This operation lets you change the keys for BitLocker volumes `HcsData` and `HcsInternal` and all the self-encrypting drives on your device.

Follow these steps to rotate the encryption-at-rest keys.

1. In the local UI of the device, go to the **Get started** page. On the **Security** tile, select **Encryption-at-rest: Rotate keys** option. This option is only available after you have successfully configured the encryption-at-rest keys.



2. You can use your own BitLocker keys or use the system-generated keys.

To provide your own key, enter a 32 character long Base-64 encoded string. The input is similar to what you would provide when you configure the encryption-at-rest for the first time.

X

Encryption at rest key rotation

You can bring your own encryption at rest key or generate one here.

* Select an option

Bring your own key ▾

* To provide your own key, enter a Base-64 encoded AES-256 bit encryption key.

..... ✓

* Enter the encryption key again.

..... ✓

Apply

You can also choose to use a system generated key.



Encryption at rest key rotation

You can bring your own encryption at rest key or generate one here.

* Select an option

Use system generated key ▾

System generated encryption key

.....

Apply

3. Select **Apply**. The key protectors are rotated.

▪ Encryption at rest key rotation 14:43:46
Triggering key rotation

4. When prompted to download and save the key file, select **Download and continue**.

Encryption at rest keys rotated

Successfully rotated the keys for your device. Download the device key file to a secure location. These keys may be needed to facilitate a future system recovery.

Download and continue

Save the `.json` key file in a secure location. This file is used to facilitate a potential future recovery of the device.

Reset device password

MyAzureStackEdge1

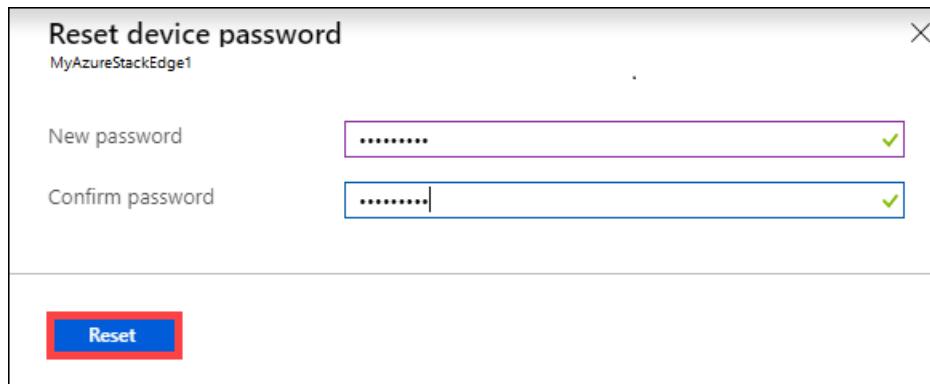
New password

.....

Confirm password

.....

Reset

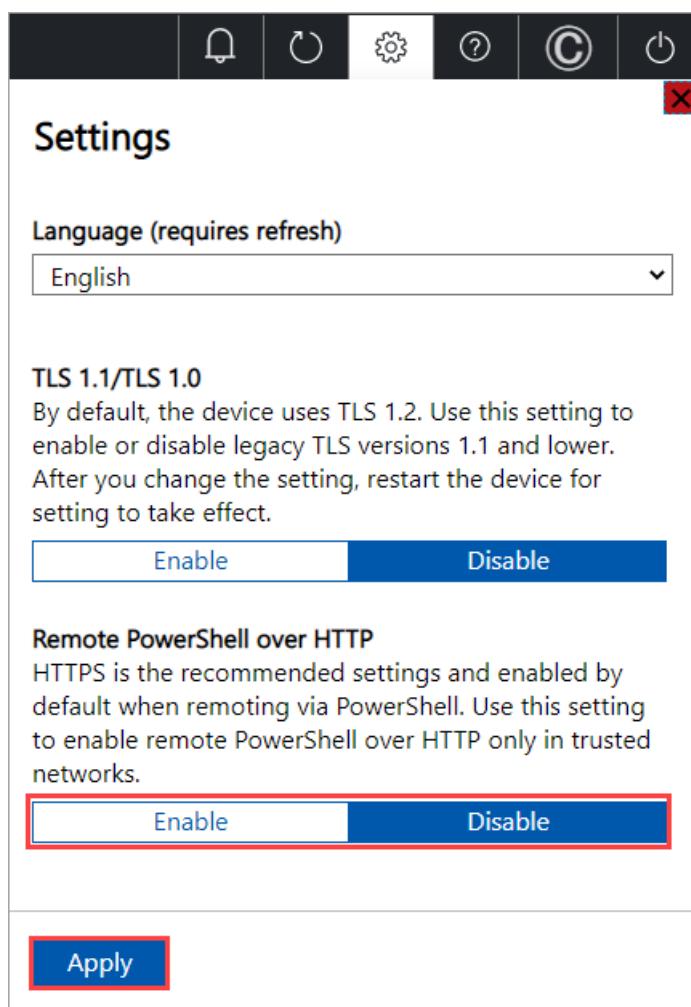


Enable device access via remote PowerShell over HTTP

You can open a remote PowerShell session to your device over HTTP or HTTPS. By default, you access the device via a PowerShell session over HTTPS. However, in trusted networks, it is acceptable to enable remote PowerShell over HTTP.

Follow these steps in the local UI to enable remote PowerShell over HTTP:

1. In the local UI of your device, go to **Settings** from the top right corner of the page.
2. Select **Enable** to allow you to open a remote PowerShell session for your device over HTTP. This setting should be enabled only in trusted networks.



3. Select **Apply**.

You can now connect to the PowerShell interface of the device over HTTP. For details, see [Connect to the PowerShell interface of your device](#).

Enable device access from outside network

To be able to connect to your Azure Stack Edge device from an outside network, make sure the network for your laptop and the network for the device meet the following requirements.

TRAFFIC DIRECTION	OUT-OF-NETWORK REQUIREMENTS
Outbound to laptop	<p>On the network for the Azure Stack Edge device:</p> <ul style="list-style-type: none">Configure the correct gateways on the device to enable traffic to reach the laptop's network.If you configure multiple gateways on the device, ensure that traffic can reach your laptop's network on all gateways. <p>A device ideally tries to use the network interface card (NIC) with the lowest route metric. However, there's no clear way for an Azure Stack Edge device to identify the NIC with the lowest metric. So it's best to make your laptop network reachable on all configured gateways.</p>
Inbound to device	<p>On the network for your laptop:</p> <ul style="list-style-type: none">Configure a clear network route from the laptop to the network for the device, possibly through defined gateways.

NOTE

Diagnostic tests for Azure Stack Edge return a warning if all gateways don't have internet connectivity. For diagnostics information, see [Run diagnostics](#).

Manage resource access

To create your Azure Stack Edge / Data Box Gateway, IoT Hub, and Azure Storage resource, you need permissions as a contributor or higher at a resource group level. You also need the corresponding resource providers to be registered. For any operations that involve activation key and credentials, permissions to the Microsoft Graph API are also required. These requirements are described in the following sections.

Manage Microsoft Graph API permissions

When generating the activation key for the Azure Stack Edge Pro device, or performing any operations that require credentials, you need permissions to Azure Active Directory Graph API. The operations that need credentials could be:

- Creating a share with an associated storage account.
- Creating a user who can access the shares on the device.

You should have a `User` access on Active Directory tenant as you need to be able to

`Read all directory objects`. You can't be a Guest user as they don't have permissions to

`Read all directory objects`. If you're a guest, then the operations such as generation of an activation key, creation of a share on your Azure Stack Edge Pro device, creation of a user, configuration of Edge compute role, reset device password will all fail.

For more information on how to provide access to users to Microsoft Graph API, see [Microsoft Graph permissions reference](#).

Register resource providers

To provision a resource in Azure (in the Azure Resource Manager model), you need a resource provider that supports the creation of that resource. For example, to provision a virtual machine, you should have a 'Microsoft.Compute' resource provider available in the subscription.

Resource providers are registered on the level of the subscription. By default, any new Azure subscription is pre-registered with a list of commonly used resource providers. The resource provider for 'Microsoft.DataBoxEdge' is not included in this list.

You don't need to grant access permissions to the subscription level for users to be able to create resources like 'Microsoft.DataBoxEdge' within their resource groups that they have owner rights on, as long as the resource providers for these resources is already registered.

Before you attempt to create any resource, make sure that the resource provider is registered in the subscription. If the resource provider is not registered, you'll need to make sure that the user creating the new resource has enough rights to register the required resource provider on the subscription level. If you haven't done this as well, then you'll see the following error:

The subscription <Subscription name> doesn't have permissions to register the resource provider(s): Microsoft.DataBoxEdge.

To get a list of registered resource providers in the current subscription, run the following command:

```
Get-AzResourceProvider -ListAvailable |where {$_._Registrationstate -eq "Registered"}
```

For Azure Stack Edge Pro device, `Microsoft.DataBoxEdge` should be registered. To register `Microsoft.DataBoxEdge`, subscription admin should run the following command:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.DataBoxEdge
```

For more information on how to register a resource provider, see [Resolve errors for resource provider registration](#).

Manage connectivity mode

Apart from the default fully connected mode, your device can also run in partially connected, or fully disconnected mode. Each of these modes is described as below:

- **Fully connected** - This is the normal default mode in which the device operates. Both the cloud upload and download of data is enabled in this mode. You can use the Azure portal or the local web UI to manage the device.

NOTE

For the Network Function Manager deployments, the Azure Stack Edge device must be **Online** and operating in fully connected mode.

- **Partially disconnected** – In this mode, the device cannot upload or download any share data though you can manage the device via the Azure portal.

This mode is typically used when on a metered satellite network and the goal is to minimize network bandwidth consumption. Minimal network consumption may still occur for device monitoring operations.

- **Disconnected** – In this mode, the device is fully disconnected from the cloud and both the cloud uploads and downloads are disabled. The device can only be managed via the local web UI.

This mode is typically used when you want to take your device offline.

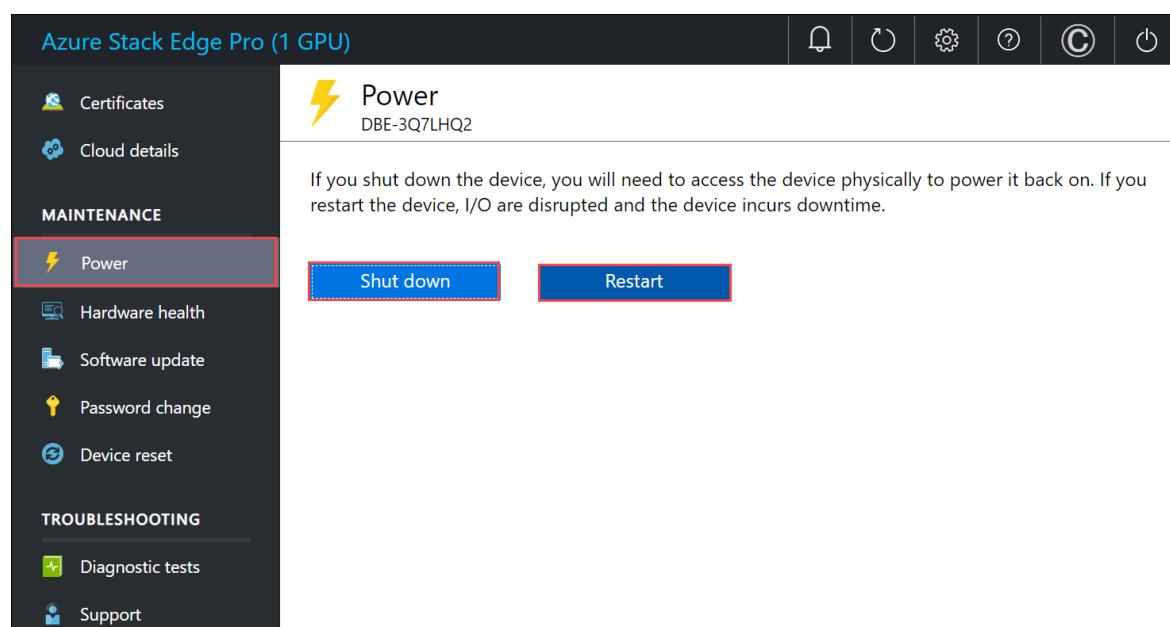
To change device mode, follow these steps:

1. In the local web UI of your device, go to **Configuration > Cloud**.
2. From the dropdown list, select the mode that you want to operate the device in. You can select from **Fully connected**, **Partially connected**, and **Fully disconnected**. To run the device in partially disconnected mode, enable **Azure portal management**.

Manage power

You can shut down or restart your physical device using the local web UI. We recommend that before you restart, take the shares offline on the data server and then the device. This action minimizes any possibility of data corruption.

1. In the local web UI, go to **Maintenance > Power**.
2. Select **Shutdown** or **Restart** depending on what you intend to do.



3. When prompted for confirmation, select **Yes** to proceed.

NOTE

If you shut down the physical device, you will need to push the power button on the device to turn it on.

Next steps

- Learn how to [Manage shares](#).

Manage an Azure Stack Edge Pro GPU device via Windows PowerShell

9/21/2022 • 20 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

Azure Stack Edge Pro GPU solution lets you process data and send it over the network to Azure. This article describes some of the configuration and management tasks for your Azure Stack Edge Pro GPU device. You can use the Azure portal, local web UI, or the Windows PowerShell interface to manage your device.

This article focuses on how you can connect to the PowerShell interface of the device and the tasks you can do using this interface.

Connect to the PowerShell interface

Depending on the operating system of client, the procedures to remotely connect to the device are different.

Remotely connect from a Windows client

Prerequisites

Before you begin, make sure that:

- Your Windows client is running Windows PowerShell 5.0 or later.
- Your Windows client has the signing chain (root certificate) corresponding to the node certificate installed on the device. For detailed instructions, see [Install certificate on your Windows client](#).
- The `hosts` file located at `C:\Windows\System32\drivers\etc` for your Windows client has an entry corresponding to the node certificate in the following format:

```
<Device IP> <Node serial number>.<DNS domain of the device>
```

Here is an example entry for the `hosts` file:

```
10.100.10.10 1HXQG13.wdshcsso.com
```

Detailed steps

Follow these steps to remotely connect from a Windows client.

1. Run a Windows PowerShell session as an administrator.
2. Make sure that the Windows Remote Management service is running on your client. At the command prompt, type:

```
winrm quickconfig
```

For more information, see [Installation and configuration for Windows Remote Management](#).

3. Assign a variable to the connection string used in the `hosts` file.

```
$Name = "<Node serial number>.<DNS domain of the device>"
```

Replace <Node serial number> and <DNS domain of the device> with the node serial number and DNS domain of your device. You can get the values for node serial number from the **Certificates** page and DNS domain from the **Device** page in the local web UI of your device.

4. To add this connection string for your device to the client's trusted hosts list, type the following command:

```
Set-Item WSMAN:\localhost\Client\TrustedHosts $Name -Concatenate -Force
```

5. Start a Windows PowerShell session on the device:

```
Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName Minishell -UseSSL
```

If you see an error related to trust relationship, then check if the signing chain of the node certificate uploaded to your device is also installed on the client accessing your device.

6. Provide the password when prompted. Use the same password that is used to sign into the local web UI. The default local web UI password is *Password1*. When you successfully connect to the device using remote PowerShell, you see the following sample output:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> winrm quickconfig
WinRM service is already running on this machine.
PS C:\WINDOWS\system32> $Name = "1HXQG13.wdshcsso.com"
PS C:\WINDOWS\system32> Set-Item WSMAN:\localhost\Client\TrustedHosts $Name -Concatenate -Force
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName
Minishell -UseSSL

WARNING: The Windows PowerShell interface of your device is intended to be used only for the initial
network configuration. Please engage Microsoft Support if you need to access this interface to
troubleshoot any potential issues you may be experiencing. Changes made through this interface
without involving Microsoft Support could result in an unsupported configuration.

[1HXQG13.wdshcsso.com]: PS>
```

When you use the `-UseSSL` option, you are remoting via PowerShell over *https*. We recommend that you always use *https* to remotely connect via PowerShell. Within trusted networks, remoting via PowerShell over http is acceptable. You first enable remote PowerShell over http in the local UI. Then you can connect to PowerShell interface of the device by using the preceding procedure without the `-UseSSL` option.

If you are not using the certificates (we recommend that you use the certificates!), you can skip the certificate validation check by using the session options: `-SkipCACheck -SkipCNCheck -SkipRevocationCheck`.

```
$sessOptions = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName Minishell -UseSSL -
SessionOption $sessOptions
```

Here is an example output when skipping the certificate check:

```

PS C:\WINDOWS\system32> $Name = "1HXQG13.wdshcsso.com"
PS C:\WINDOWS\system32> $sessOptions = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
PS C:\WINDOWS\system32> $sessOptions

MaximumConnectionRedirectionCount : 5
NoCompression : False
NoMachineProfile : False
ProxyAccessType : None
ProxyAuthentication : Negotiate
ProxyCredential :
SkipCACheck : True
SkipCNCheck : True
SkipRevocationCheck : True
OperationTimeout : 00:03:00
NoEncryption : False
UseUTF16 : False
IncludePortInSPN : False
OutputBufferingMode : None
MaxConnectionRetryCount : 0
Culture :
UICulture :
MaximumReceivedDataSizePerCommand :
MaximumReceivedObjectSize :
ApplicationArguments :
OpenTimeout : 00:03:00
CancelTimeout : 00:01:00
IdleTimeout : -00:00:00.0010000

PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $Name -Credential ~\EdgeUser -ConfigurationName
Minishell -UseSSL -SessionOption $sessOptions
WARNING: The Windows PowerShell interface of your device is intended to be used only for the initial network
configuration. Please
engage Microsoft Support if you need to access this interface to troubleshoot any potential issues you may
be experiencing.
Changes made through this interface without involving Microsoft Support could result in an unsupported
configuration.
[1HXQG13.wdshcsso.com]: PS>

```

IMPORTANT

In the current release, you can connect to the PowerShell interface of the device only via a Windows client. The `-UseSSL` option does not work with the Linux clients.

Create a support package

If you experience any device issues, you can create a support package from the system logs. Microsoft Support uses this package to troubleshoot the issues. Follow these steps to create a support package:

1. [Connect to the PowerShell interface of your device.](#)
2. Use the `Get-HcsNodeSupportPackage` command to create a support package. The usage of the cmdlet is as follows:

```

Get-HcsNodeSupportPackage [-Path] <string> [-Zip] [-ZipFileName <string>] [-Include {None | RegistryKeys | EtwLogs | PeriodicEtwLogs | LogFiles | DumpLog | Platform | FullDumps | MiniDumps | ClusterManagementLog | ClusterLog | UpdateLogs | CbsLogs | StorageCmdlets | ClusterCmdlets | ConfigurationCmdlets | KernelDump | RollbackLogs | Symbols | NetworkCmdlets | NetworkCmds | Fltmc | ClusterStorageLogs | UTElement | UTFlag | SmbWmiProvider | TimeCmds | LocalUILogs | ClusterHealthLogs | BcdeditCommand | BitLockerCommand | DirStats | ComputeRolesLogs | ComputeCmdlets | DeviceGuard | Manifests | MeasuredBootLogs | Stats | PeriodicStatLogs | MigrationLogs | RollbackSupportPackage | ArchivedLogs | Default}] [-MinimumTimestamp <datetime>] [-MaximumTimestamp <datetime>] [-IncludeArchived] [-IncludePeriodicStats] [-Credential <pscredential>] [<CommonParameters>]

```

The cmdlet collects logs from your device and copies those logs to a specified network or local share.

The parameters used are as follows:

- `-Path` - Specify the network or the local path to copy support package to. (required)
- `-Credential` - Specify the credentials to access the protected path.
- `-Zip` - Specify to generate a zip file.
- `-Include` - Specify to include the components to be included in the support package. If not specified, `Default` is assumed.
- `-IncludeArchived` - Specify to include archived logs in the support package.
- `-IncludePeriodicStats` - Specify to include periodic stat logs in the support package.

View device information

1. [Connect to the PowerShell interface](#).

2. Use the `Get-HcsApplianceInfo` to get the information for your device.

The following example shows the usage of this cmdlet:

```

[10.100.10.10]: PS>Get-HcsApplianceInfo

Id : b2044bdb-56fd-4561-a90b-407b2a67bdfc
FriendlyName : DBE-NBSVFQR94S6
Name : DBE-NBSVFQR94S6
SerialNumber : HCS-NBSVFQR94S6
DeviceId : 40d7288d-cd28-481d-a1ea-87ba9e71ca6b
Model : Virtual
FriendlySoftwareVersion : Data Box Gateway 1902
HcsVersion : 1.4.771.324
IsClustered : False
IsVirtual : True
LocalCapacityInMb : 1964992
SystemState : Initialized
SystemStatus : Normal
Type : DataBoxGateway
CloudReadRateBytesPerSec : 0
CloudWriteRateBytesPerSec : 0
IsInitialPasswordSet : True
FriendlySoftwareVersionNumber : 1902
UploadPolicy : All
DataDiskResiliencySettingName : Simple
ApplianceTypeFriendlyName : Data Box Gateway
IsRegistered : False

```

Here is a table summarizing some of the important device information:

PARAMETER	DESCRIPTION
FriendlyName	The friendly name of the device as configured through the local web UI during device deployment. The default friendly name is the device serial number.
SerialNumber	The device serial number is a unique number assigned at the factory.
Model	The model for your Azure Stack Edge or Data Box Gateway device. The model is physical for Azure Stack Edge and virtual for Data Box Gateway.
FriendlySoftwareVersion	The friendly string that corresponds to the device software version. For a system running preview, the friendly software version would be Data Box Edge 1902.
HcsVersion	The HCS software version running on your device. For instance, the HCS software version corresponding to Data Box Edge 1902 is 1.4.771.324.
LocalCapacityInMb	The total local capacity of the device in Megabits.
IsRegistered	This value indicates if your device is activated with the service.

View GPU driver information

If the compute role is configured on your device, you can also get the GPU driver information via the PowerShell interface.

1. [Connect to the PowerShell interface](#).
2. Use the `Get-HcsGpuNvidiaSmi` to get the GPU driver information for your device.

The following example shows the usage of this cmdlet:

```
Get-HcsGpuNvidiaSmi
```

Make a note of the driver information from the sample output of this cmdlet.

```
+-----+
| NVIDIA-SMI 440.64.00    Driver Version: 440.64.00    CUDA Version: 10.2    |
+-----+-----+-----+
| GPU  Name      Persistence-M| Bus-Id      Disp.A | Volatile Uncorr. ECC |
| Fan  Temp     Perf  Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
|=====+=====+=====+=====+=====+=====+=====+=====+=====+=====+=====+=====|
|  0  Tesla T4          On     | 000029CE:00:00.0 Off |                0 |
| N/A   60C   P0    29W /  70W |    1539MiB / 15109MiB |      0%     Default |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|  1  Tesla T4          On     | 0000AD50:00:00.0 Off |                0 |
| N/A   58C   P0    29W /  70W |    330MiB / 15109MiB |      0%     Default |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Enable Multi-Process Service (MPS)

A Multi-Process Service (MPS) on Nvidia GPUs provides a mechanism where GPUs can be shared by multiple jobs, where each job is allocated some percentage of the GPU's resources. MPS is a preview feature on your Azure Stack Edge Pro GPU device. To enable MPS on your device, follow these steps:

1. Before you begin, make sure that:
 - a. You've configured and [Activated your Azure Stack Edge Pro device](#) with an Azure Stack Edge resource in Azure.
 - b. You've [Configured compute on this device in the Azure portal](#).
2. [Connect to the PowerShell interface](#).
3. Use the following command to enable MPS on your device.

```
Start-HcsGpuMPS
```

NOTE

When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads. You'll need to enable MPS again.

Reset your device

To reset your device, you need to securely wipe out all the data on the data disk and the boot disk of your device.

Use the `Reset-HcsAppliance` cmdlet to wipe out both the data disks and the boot disk or just the data disks. The `SecureWipeBootDisk` and `SecureWipeDataDisks` switches allow you to wipe the boot disk and the data disks respectively.

The `SecureWipeBootDisk` switch wipes the boot disk and makes the device unusable. It should be used only when the device needs to be returned to Microsoft. For more information, see [Return the device to Microsoft](#).

If you use the device reset in the local web UI, only the data disks are securely wiped but the boot disk is kept intact. The boot disk contains the device configuration.

1. [Connect to the PowerShell interface](#).
2. At the command prompt, type:

```
Reset-HcsAppliance -SecureWipeBootDisk -SecureWipeDataDisks
```

The following example shows how to use this cmdlet:

```
[10.128.24.33]: PS>Reset-HcsAppliance -SecureWipeBootDisk -SecureWipeDataDisks

Confirm
Are you sure you want to perform this action?
Performing the operation "Reset-HcsAppliance" on target "ShouldProcess appliance".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"): N
```

Get compute logs

If the compute role is configured on your device, you can also get the compute logs via the PowerShell interface.

1. [Connect to the PowerShell interface](#).

2. Use the `Get-AzureDataBoxEdgeComputeRoleLogs` cmdlet to get the compute logs for your device.

The following example shows the usage of this cmdlet:

```
Get-AzureDataBoxEdgeComputeRoleLogs -Path "\\\hcsfs\logs\myacct" -Credential "username" -  
FullLogCollection
```

Here is a description of the parameters used for the cmdlet:

- `Path`: Provide a network path to the share where you want to create the compute log package.
- `Credential`: Provide the username for the network share. When you run this cmdlet, you will need to provide the share password.
- `FullLogCollection`: This parameter ensures that the log package will contain all the compute logs. By default, the log package contains only a subset of logs.

Change Kubernetes pod and service subnets

By default, Kubernetes on your Azure Stack Edge device uses subnets 172.27.0.0/16 and 172.28.0.0/16 for pod and service respectively. If these subnets are already in use in your network, then you can run the `Set-HcsKubeClusterNetworkInfo` cmdlet to change these subnets.

You want to perform this configuration before you configure compute from the Azure portal as the Kubernetes cluster is created in this step.

1. [Connect to the PowerShell interface of the device](#).

2. From the PowerShell interface of the device, run:

```
Set-HcsKubeClusterNetworkInfo -PodSubnet <subnet details> -ServiceSubnet <subnet details>
```

Replace the <subnet details> with the subnet range that you want to use.

3. Once you have run this command, you can use the `Get-HcsKubeClusterNetworkInfo` command to verify that the pod and service subnets have changed.

Here is a sample output for this command.

```
[10.100.10.10]: PS>Set-HcsKubeClusterNetworkInfo -PodSubnet 10.96.0.1/16 -ServiceSubnet 10.97.0.1/16  
[10.100.10.10]: PS>Get-HcsKubeClusterNetworkInfo  
  
Id          PodSubnet      ServiceSubnet  
--          -----          -----  
6dbf23c3-f146-4d57-bdfc-76cad714cf1 10.96.0.1/16 10.97.0.1/16  
[10.100.10.10]: PS>
```

Debug Kubernetes issues related to IoT Edge

Before you begin, you must have:

- Compute network configured. See [Tutorial: Configure network for Azure Stack Edge Pro with GPU](#).
- Compute role configured on your device.

On an Azure Stack Edge Pro GPU device that has the compute role configured, you can troubleshoot or monitor the device using two different sets of commands.

- Using `iotedge` commands. These commands are available for basic operations for your device.
- Using `kubectl` commands. These commands are available for an extensive set of operations for your device.

To execute either of the above set of commands, you need to [Connect to the PowerShell interface](#).

Use `iotedge` commands

To see a list of available commands, [connect to the PowerShell interface](#) and use the `iotedge` function.

```
[10.100.10.10]: PS>iotedge -?  
Usage: iotedge COMMAND
```

Commands:

- list
- logs
- restart

```
[10.100.10.10]: PS>
```

The following table has a brief description of the commands available for `iotedge`:

COMMAND	DESCRIPTION
<code>list</code>	List modules
<code>logs</code>	Fetch the logs of a module
<code>restart</code>	Stop and restart a module

List all IoT Edge modules

To list all the modules running on your device, use the `iotedge list` command.

Here is a sample output of this command. This command lists all the modules, associated configuration, and the external IPs associated with the modules. For example, you can access the **webserver** app at

<https://10.128.44.244>.

```
[10.100.10.10]: PS>iotedge list  
  
NAME          STATUS  DESCRIPTION CONFIG           EXTERNAL-IP  
----          -----  -----  
gettingstartedwithgpus  Running Up 10 days  mcr.microsoft.com/intelligentedge/solutions:latest  
iotedged      Running Up 10 days  azureiotedge/azureiotedge-iotedged:0.1.0-beta10  <none>  
edgehub        Running Up 10 days  mcr.microsoft.com/azureiotedge-hub:1.0          10.128.44.243  
edgeagent      Running Up 10 days  azureiotedge/azureiotedge-agent:0.1.0-beta10  
webserverapp   Running Up 10 days  nginx:stable                         10.128.44.244  
  
[10.100.10.10]: PS>
```

Restart modules

You can use the `list` command to list all the modules running on your device. Then identify the name of the module that you want to restart and use it with the `restart` command.

Here is a sample output of how to restart a module. Based on the description of how long the module is running for, you can see that `cuda-sample1` was restarted.

```
[10.100.10.10]: PS>iotedge list

NAME      STATUS  DESCRIPTION CONFIG                                EXTERNAL-IP PORT(S)
----      -----  -----  -----
edgehub    Running Up 5 days   mcr.microsoft.com/azureiotedge-hub:1.0  10.57.48.62
443:31457/TCP,5671:308

81/TCP,8883:31753/TCP
iotedged   Running Up 7 days  azureiotedge/azureiotedge-iotedged:0.1.0-beta13 <none>
35000/TCP,35001/TCP
cuda-sample2 Running Up 1 days  nvidia/samples:nbody
edgeagent    Running Up 7 days  azureiotedge/azureiotedge-agent:0.1.0-beta13
cuda-sample1 Running Up 1 days  nvidia/samples:nbody

[10.100.10.10]: PS>iotedge restart cuda-sample1
[10.100.10.10]: PS>iotedge list

NAME      STATUS  DESCRIPTION CONFIG                                EXTERNAL-IP PORT(S)
----      -----  -----  -----
edgehub    Running Up 5 days   mcr.microsoft.com/azureiotedge-hub:1.0  10.57.48.62
443:31457/TCP,5671:30

881/TCP,8883:31753/TC

P
iotedged   Running Up 7 days  azureiotedge/azureiotedge-iotedged:0.1.0-beta13 <none>
35000/TCP,35001/TCP
cuda-sample2 Running Up 1 days  nvidia/samples:nbody
edgeagent    Running Up 7 days  azureiotedge/azureiotedge-agent:0.1.0-beta13
cuda-sample1 Running Up 4 minutes nvidia/samples:nbody

[10.100.10.10]: PS>
```

Get module logs

Use the `logs` command to get logs for any IoT Edge module running on your device.

If there was an error in creation of the container image or while pulling the image, run `logs edgeagent`.

`edgeagent` is the IoT Edge runtime container that is responsible for provisioning other containers. Because

`logs edgeagent` dumps all the logs, a good way to see the recent errors is to use the option `--tail 0``.

Here is a sample output.

```
[10.100.10.10]: PS>iotedge logs cuda-sample2 --tail 10
[10.100.10.10]: PS>iotedge logs edgeagent --tail 10
<6> 2021-02-25 00:52:54.828 +00:00 [INF] - Executing command: "Report EdgeDeployment status: [Success]"
<6> 2021-02-25 00:52:54.829 +00:00 [INF] - Plan execution ended for deployment 11
<6> 2021-02-25 00:53:00.191 +00:00 [INF] - Plan execution started for deployment 11
<6> 2021-02-25 00:53:00.191 +00:00 [INF] - Executing command: "Create an EdgeDeployment with modules: [cuda-
sample2, edgeAgent, edgeHub, cuda-sample1]"
<6> 2021-02-25 00:53:00.212 +00:00 [INF] - Executing command: "Report EdgeDeployment status: [Success]"
<6> 2021-02-25 00:53:00.212 +00:00 [INF] - Plan execution ended for deployment 11
<6> 2021-02-25 00:53:05.319 +00:00 [INF] - Plan execution started for deployment 11
<6> 2021-02-25 00:53:05.319 +00:00 [INF] - Executing command: "Create an EdgeDeployment with modules: [cuda-
sample2, edgeAgent, edgeHub, cuda-sample1]"
<6> 2021-02-25 00:53:05.412 +00:00 [INF] - Executing command: "Report EdgeDeployment status: [Success]"
<6> 2021-02-25 00:53:05.412 +00:00 [INF] - Plan execution ended for deployment 11
[10.100.10.10]: PS>
```

NOTE

The direct methods such as GetModuleLogs or UploadModuleLogs are not supported on IoT Edge on Kubernetes on your Azure Stack Edge.

Use kubectl commands

On an Azure Stack Edge Pro GPU device that has the compute role configured, all the `kubectl` commands are available to monitor or troubleshoot modules. To see a list of available commands, run `kubectl --help` from the command window.

```
C:\Users\myuser>kubectl --help

kubectl controls the Kubernetes cluster manager.

Find more information at: https://kubernetes.io/docs/reference/kubectl/overview/

Basic Commands (Beginner):
  create      Create a resource from a file or from stdin.
  expose      Take a replication controller, service, deployment or pod and expose it as a new
Kubernetes Service
  run         Run a particular image on the cluster
  set         Set specific features on objects
  run-container Run a particular image on the cluster. This command is deprecated, use "run" instead
=====
=====CUT=====CUT=====CUT=====

Usage:
  kubectl [flags] [options]

Use "kubectl <command> --help" for more information about a given command.
Use "kubectl options" for a list of global command-line options (applies to all commands).

C:\Users\myuser>
```

For a comprehensive list of the `kubectl` commands, go to [kubectl cheatsheet](#).

To get IP of service or module exposed outside of Kubernetes cluster

To get the IP of a load-balancing service or modules exposed outside of the Kubernetes, run the following command:

```
kubectl get svc -n iotedge
```

Following is a sample output of the all the services or modules that are exposed outside of the Kubernetes cluster:

```
[10.100.10.10]: PS>kubectl get svc -n iotedge
NAME          TYPE        CLUSTER-IP   EXTERNAL-IP      PORT(S)
AGE
edgehub       LoadBalancer 10.103.52.225  10.128.44.243  443:31987/TCP,5671:32336/TCP,8883:30618/TCP
34h
iotedged     ClusterIP    10.107.236.20  <none>           35000/TCP,35001/TCP
3d8h
webserverapp LoadBalancer 10.105.186.35  10.128.44.244  8080:30976/TCP
16h
```

The IP address in the External IP column corresponds to the external endpoint for the service or the module. You can also [Get the external IP in the Kubernetes dashboard](#).

To check if module deployed successfully

Compute modules are containers that have a business logic implemented. A Kubernetes pod can have multiple containers running.

To check if a compute module is deployed successfully, connect to the PowerShell interface of the device. Run the `get pods` command and check if the container (corresponding to the compute module) is running.

To get the list of all the pods running in a specific namespace, run the following command:

```
get pods -n <namespace>
```

To check the modules deployed via IoT Edge, run the following command:

```
get pods -n iotedge
```

Following is a sample output of all the pods running in the `iotedge` namespace.

```
[10.100.10.10]: PS>kubectl get pods -n iotedge
NAME           READY   STATUS    RESTARTS   AGE
edgeagent-cf6d4ffd4-q512k   2/2     Running   0          20h
edgehub-8c9dc8788-2mvwv    2/2     Running   0          56m
filemove-66c49984b7-h8lxc   2/2     Running   0          56m
iotedged-675d7f4b5f-9nml4  1/1     Running   0          20h
```

```
[10.100.10.10]: PS>
```

The status **Status** indicates that all the pods in the namespace are running and the **Ready** indicates the number of containers deployed in a pod. In the preceding sample, all the pods are running and all the modules deployed in each of the pods are running.

To check the modules deployed via Azure Arc, run the following command:

```
get pods -n azure-arc
```

Alternatively, you can [Connect to Kubernetes dashboard to see IoT Edge or Azure Arc deployments](#).

For a more verbose output of a specific pod for a given namespace, you can run the following command:

```
kubectl describe pod <pod name> -n <namespace>
```

The sample output is shown here.

```
[10.100.10.10]: PS>kubectl describe pod fileremove-66c49984b7 -n iotedge
Name:           fileremove-66c49984b7-h8lxc
Namespace:      iotedge
Priority:       0
Node:           k8s-1hwf613cl-1hwf613/10.139.218.12
Start Time:     Thu, 14 May 2020 12:46:28 -0700
Labels:         net.azure-devices.edge.deviceid=myasgpu-edge
                net.azure-devices.edge.hub=myasgpu2iothub.azure-devices.net
                net.azure-devices.edge.module=fileremove
                pod-template-hash=66c49984b7
Annotations:    net.azure-devices.edge.original-moduleid: fileremove
Status:         Running
IP:             172.17.75.81
IPs:            <none>
Controlled By: ReplicaSet/fileremove-66c49984b7
Containers:
  proxy:
    Container ID: docker://fd7975ca78209a633a1f314631042a0892a833b7e942db2e7708b41f03e8daaf
    Image:         azureiotedge/azureiotedge-proxy:0.1.0-beta8
    Image ID:     docker://sha256:5efbf6238f13d24bab9a2b499e5e05bc0c33ab1587d6cf6f289cdbe7aa667563
    Port:          <none>
    Host Port:    <none>
    State:        Running
      Started:    Thu, 14 May 2020 12:46:30 -0700
    Ready:         True
    Restart Count: 0
    Environment:
      PROXY_LOG: Debug
=====
Volumes:
  config-volume:
    Type:      ConfigMap (a volume populated by a ConfigMap)
    Name:      iotedgeproxy-config
    Optional:  false
  trust-bundle-volume:
    Type:      ConfigMap (a volume populated by a ConfigMap)
    Name:      iotedgeproxy-trust-bundle
    Optional:  false
  myasesmb1local:
    Type:      PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
    ClaimName: myasesmb1local
    ReadOnly:   false
  myasesmb1:
    Type:      PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
    ClaimName: myasesmb1
    ReadOnly:   false
  fileremove-token-pzvw8:
    Type:      Secret (a volume populated by a Secret)
    SecretName: fileremove-token-pzvw8
    Optional:  false
  QoS Class:  BestEffort
  Node-Selectors: <none>
  Tolerations: node.kubernetes.io/not-ready:NoExecute for 300s
                node.kubernetes.io/unreachable:NoExecute for 300s
  Events:     <none>

[10.100.10.10]: PS>
```

To get container logs

To get the logs for a module, run the following command from the PowerShell interface of the device:

```
kubectl logs <pod_name> -n <namespace> --all-containers
```

Because `all-containers` flag dumps all the logs for all the containers, a good way to see the recent errors is to use the option `--tail 10`.

Following is a sample output.

```
[10.100.10.10]: PS>kubectl logs filemove-66c49984b7-h8lxc -n iotedge --all-containers --tail 10
DEBUG 2020-05-14T20:40:42Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:40:44Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:40:44Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:40:44Z: loop process - 1 events, 0.000s
DEBUG 2020-05-14T20:40:44Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:42:12Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:42:14Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:42:14Z: loop process - 0 events, 0.000s
DEBUG 2020-05-14T20:42:14Z: loop process - 1 events, 0.000s
DEBUG 2020-05-14T20:42:14Z: loop process - 0 events, 0.000s
05/14/2020 19:46:44: Info: Opening module client connection.
05/14/2020 19:46:45: Info: Open done.
05/14/2020 19:46:45: Info: Initializing with input: /home/input, output: /home/output, protocol: Amqp.
05/14/2020 19:46:45: Info: IoT Hub module client initialized.

[10.100.10.10]: PS>
```

Change memory, processor limits for Kubernetes worker node

To change the memory or processor limits for Kubernetes worker node, do the following steps:

1. [Connect to the PowerShell interface of the device.](#)
2. To get the current resources for the worker node and the role options, run the following command:

```
Get-AzureDataBoxEdgeRole
```

Here is a sample output. Note the values for `Name` and `Compute` under `Resources` section.

`MemoryInBytes` and `ProcessorCount` denote the currently assigned values memory and processor count for the Kubernetes worker node.

```
[10.100.10.10]: PS>Get-AzureDataBoxEdgeRole
ImageDetail           : Name:mcr.microsoft.com/azureiotedge-agent
                        Tag:1.0
                        PlatformType:Linux
EdgeDeviceConnectionString :
IotDeviceConnectionString :
HubHostName          : ase-srp-007.azure-devices.net
IotDeviceId           : srp-007-storagegateway
EdgeDeviceId           : srp-007-edge
Version               :
Id                    : 6ebeff9f-84c5-49a7-890c-f5e05520a506
Name                 : IoTRole
Type                 : IOT
Resources             : Compute:
                        MemoryInBytes:34359738368
                        ProcessorCount:12
                        VMProfile:

                        Storage:
                        EndpointMap:
                        EndpointId:c0721210-23c2-4d16-bca6-c80e171a0781
                        TargetPath:mysmbedgecloudshare1
                        Name:mysmbedgecloudshare1
                        Protocol:SMB

                        EndpointId:6557c3b6-d3c5-4f94-aaa0-6b7313ab5c74
                        TargetPath:mysmbedgegelocalshare
                        Name:mysmbedgegelocalshare
                        Protocol:SMB
                        RootFileSystemStorageSizeInBytes:0

HostPlatform          : KubernetesCluster
State                : Created
PlatformType          : Linux
HostPlatformInstanceId : 994632cb-853e-41c5-a9cd-05b36ddbb190
IsHostPlatformOwner   : True
IsCreated             :
[10.100.10.10]: PS>
```

3. To change the values of memory and processors for the worker node, run the following command:

```
Set-AzureDataBoxEdgeRoleCompute -Name <Name value from the output of Get-AzureDataBoxEdgeRole> -
Memory <Value in Bytes> -ProcessorCount <No. of cores>
```

Here is a sample output.

```
[10.100.10.10]: PS>Set-AzureDataBoxEdgeRoleCompute -Name IoTRole -MemoryInBytes 32GB -ProcessorCount 16

ImageDetail          : Name:mcr.microsoft.com/azureiotedge-agent
                        Tag:1.0
                        PlatformType:Linux

EdgeDeviceConnectionString :
IoTDeviceConnectionString :
HubHostName          : ase-srp-007.azure-devices.net
IoTDeviceId           : srp-007-storagegateway
EdgeDeviceId          : srp-007-edge
Version               :
Id                   : 6ebeff9f-84c5-49a7-890c-f5e05520a506
Name                 : IoTRole
Type                 : IOT
Resources             :
                        Compute:
                        MemoryInBytes:34359738368
                        ProcessorCount:16
                        VMProfile:

                        Storage:
                        EndpointMap:
                        EndpointId:c0721210-23c2-4d16-bca6-c80e171a0781
                        TargetPath:mysmbedgecloudshare1
                        Name:mysmbedgecloudshare1
                        Protocol:SMB

                        EndpointId:6557c3b6-d3c5-4f94-aaa0-6b7313ab5c74
                        TargetPath:mysmbedgelocalshare
                        Name:mysmbedgelocalshare
                        Protocol:SMB

                        RootFileSystemStorageSizeInBytes:0

HostPlatform          : KubernetesCluster
State                : Created
PlatformType          : Linux
HostPlatformInstanceId : 994632cb-853e-41c5-a9cd-05b36ddb190
IsHostPlatformOwner   : True
IsCreated             :

[10.100.10.10]: PS>
```

While changing the memory and processor usage, follow these guidelines.

- Default memory is 25% of device specification.
- Default processor count is 30% of device specification.
- When changing the values for memory and processor counts, we recommend that you vary the values between 15% to 60% of the device memory and the processor count.
- We recommend an upper limit of 60% is so that there are enough resources for system components.

Connect to BMC

Baseboard management controller (BMC) is used to remotely monitor and manage your device. This section describes the cmdlets that can be used to manage BMC configuration. Prior to running any of these cmdlets, [Connect to the PowerShell interface of the device](#).

- `Get-HcsNetBmcInterface` : Use this cmdlet to get the network configuration properties of the BMC, for example, `IPv4Address`, `IPv4Gateway`, `IPv4SubnetMask`, `DhcpEnabled`.

Here is a sample output:

```
[10.100.10.10]: PS>Get-HcsNetBmcInterface  
IPv4Address IPv4Gateway IPv4SubnetMask DhcpEnabled  
-----  
10.128.53.186 10.128.52.1 255.255.252.0 False  
[10.100.10.10]: PS>
```

- `Set-HcsNetBmcInterface` : You can use this cmdlet in the following two ways.
 - Use the cmdlet to enable or disable DHCP configuration for BMC by using the appropriate value for `UseDhcp` parameter.

```
Set-HcsNetBmcInterface -UseDhcp $true
```

Here is a sample output:

```
[10.100.10.10]: PS>Set-HcsNetBmcInterface -UseDhcp $true  
[10.100.10.10]: PS>Get-HcsNetBmcInterface  
IPv4Address IPv4Gateway IPv4SubnetMask DhcpEnabled  
-----  
10.128.54.8 10.128.52.1 255.255.252.0 True  
[10.100.10.10]: PS>
```

- Use this cmdlet to configure the static configuration for the BMC. You can specify the values for `IPv4Address` , `IPv4Gateway` , and `IPv4SubnetMask` .

```
Set-HcsNetBmcInterface -IPv4Address "<IPv4 address of the device>" -IPv4Gateway "<IPv4 address of the gateway>" -IPv4SubnetMask "<IPv4 address for the subnet mask>"
```

Here is a sample output:

```
[10.100.10.10]: PS>Set-HcsNetBmcInterface -IPv4Address 10.128.53.186 -IPv4Gateway 10.128.52.1  
-IPv4SubnetMask 255.255.252.0  
[10.100.10.10]: PS>Get-HcsNetBmcInterface  
IPv4Address IPv4Gateway IPv4SubnetMask DhcpEnabled  
-----  
10.128.53.186 10.128.52.1 255.255.252.0 False  
[10.100.10.10]: PS>
```

- `Set-HcsBmcPassword` : Use this cmdlet to modify the BMC password for `EdgeUser` . The user name - `EdgeUser` - is case-sensitive.

Here is a sample output:

```
[10.100.10.10]: PS> Set-HcsBmcPassword -NewPassword "Password1"  
[10.100.10.10]: PS>
```

Exit the remote session

To exit the remote PowerShell session, close the PowerShell window.

Next steps

- Deploy [Azure Stack Edge Pro GPU](#) in Azure portal.

Update your Azure Stack Edge Pro GPU

9/21/2022 • 9 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes the steps required to install update on your Azure Stack Edge Pro with GPU via the local web UI and via the Azure portal. You apply the software updates or hotfixes to keep your Azure Stack Edge Pro device and the associated Kubernetes cluster on the device up-to-date.

The procedure described in this article was performed using a different version of software, but the process remains the same for the current software version.

About latest update

The current update is Update 2207. This update installs two updates, the device update followed by Kubernetes updates. The associated versions for this update are:

- Device software version - **2.2.2037.5375**
- Device Kubernetes version - **2.2.2037.5375**
- Kubernetes server version - **v1.22.6**
- IoT Edge version: **0.1.0-beta15**
- Azure Arc version: **1.6.6**
- GPU driver version: **515.48.07**
- CUDA version: **11.7**

For information on what's new in this update, go to [Release notes](#).

To apply 2207 update, your device must be running 2106 or later.

- If you are not running the minimal supported version, you'll see this error: *Update package cannot be installed as its dependencies are not met.*
- You can update to 2106 from an older version and then install 2207.

Updates for a single-node vs two-node

The procedure to update an Azure Stack Edge is the same whether it is a single-node device or a two-node cluster. This applies both to the Azure portal or the local UI procedure.

- **Single node** - For a single node device, installing an update or hotfix is disruptive and will restart your device. Your device will experience a downtime for the entire duration of the update.
- **Two-node** - For a two-node cluster, this is an optimized update. The two-node cluster may experience short, intermittent disruptions while the update is in progress. We recommend that you shouldn't perform any operations on the device node when update is in progress.

The Kubernetes worker VMs will go down when a node goes down. The Kubernetes master VM will fail over to the other node. Workloads will continue to run. For more information, see [Kubernetes failover scenarios for Azure Stack Edge](#).

Provisioning actions such as creating shares or virtual machines are not supported during update. The update takes approximately 60 to 75 minutes per node to complete.

To install updates on your device, you need to follow these steps:

1. Configure the location of the update server.
2. Apply the updates via the Azure portal UI or the local web UI.

Each of these steps is described in the following sections.

Configure update server

1. In the local web UI, go to **Configuration > Update server**.
2. In **Select update server type**, from the dropdown list, choose from Microsoft Update server (default) or Windows Server Update Services.

If updating from the Windows Server Update Services, specify the server URI. The server at that URI will deploy the updates on all the devices connected to this server.

The WSUS server is used to manage and distribute updates through a management console. A WSUS server can also be the update source for other WSUS servers within the organization. The WSUS server that acts as an update source is called an upstream server. In a WSUS implementation, at least one WSUS server on your network must be able to connect to Microsoft Update to get available update information. As an administrator, you can determine - based on network security and configuration - how many other WSUS servers connect directly to Microsoft Update.

For more information, go to [Windows Server Update Services \(WSUS\)](#)

Use the Azure portal

We recommend that you install updates through the Azure portal. The device automatically scans for updates once a day. Once the updates are available, you see a notification in the portal. You can then download and install the updates.

NOTE

- Make sure that the device is healthy and status shows as **Your device is running fine!** before you proceed to install the updates.

Depending on the software version that you are running, install process may differ slightly.

- If you are updating from 2106 to 2110 or later, you will have a one-click install. See the **version 2106 and later** tab for instructions.
- If you are updating to versions prior to 2110, you will have a two-click install. See **version 2105 and earlier** tab for instructions.
- [version 2106 and later](#)
- [version 2105 and earlier](#)

1. When the updates are available for your device, you see a notification in the **Overview** page of your Azure Stack Edge resource. Select the notification or from the top command bar, **Update device**. This will allow you to apply device software updates.

The screenshot shows the Azure Stack Edge device overview page. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Security, Order details, Diagnostics), Edge services (Virtual machines, IoT Edge, Cloud storage gateway), and Monitoring (Device events). The main area has tabs for Update device, Reset device password, Return device, Feedback, Delete, and Refresh. A message at the top says 'New device update available. Your device will experience downtime when these updates are installed.' Below this, there's a section for 'Your device is online' and 'Deployed edge services' (which is currently empty). Under 'Edge services', there are three cards: 'Virtual machines' (New), 'IoT Edge', and 'Cloud storage gateway'. Each card has a 'How to get started?' link.

2. In the **Device updates** blade, check that you have reviewed the license terms associated with new features in the release notes.

Once the updates are downloaded on the device, you can choose to **Automatically install** the updates.

The screenshot shows the 'Device updates' blade for the device 'asedevice'. It displays information about available updates:

Installed software version	Azure Stack Edge 2106 (2.2.1636.3457)
Last successful update	-
Last successful scan	9/27/2021, 03:00:19
Update details	2 updates, 7.47 GB
Estimated duration	60 mins (after download)
Updates started on	-

Below this, a table lists the update types and their details:

Type	Version	Size	Installation impact
Software	2109(2.2.1726.3923)	4.27 GB	⚠️ Device reboots automatically
Kubernetes	2109(2.2.1726.3923)	3.21 GB	⚠️ Kubernetes workloads will be down

At the bottom, there are two radio button options for update installation:

- Automatically install the updates
- Manually install updates later

A note below the radio buttons says: 'Once updates are downloaded on this device,' followed by a red box around the 'Automatically install the updates' option.

An info icon with the text 'To know more about installation, click on [Learn more](#)' is also present.

A checkbox labeled 'I accept the terms and conditions mentioned in the release notes. For more information about the updates and its impact, refer [release notes](#)' is checked and highlighted with a red box.

At the bottom, there are 'Install update' and 'Close' buttons.

You can also just download the updates and then **Manually install updates later**.

Device updates

asedevice

New updates available. You can choose to download the update now and install later.

Installed software version	Azure Stack Edge 2106 (2.2.1636.3457)
Last successful update	-
Last successful scan	9/27/2021, 03:00:19
Update details	2 updates, 7.47 GB
Estimated duration	60 mins (after download)
Updates started on	-

Type	Version	Size	Installation impact
Software	2109(2.2.1726.3923)	4.27 GB	⚠ Device reboots automatically
Kubernetes	2109(2.2.1726.3923)	3.21 GB	⚠ Kubernetes workloads will be down

Once updates are downloaded on this device,

Automatically install the updates

Manually install updates later

I accept the terms and conditions mentioned in the release notes. For more information about the updates and it's impact, refer [release notes](#).

Download **Close**

3. The download of updates starts. You see a notification that the download is in progress.

*** Triggering download and install updates X

The operation is in progress.

A notification banner is also displayed in the Azure portal. This indicates the download progress. You can select this notification or select **Update device** to see the detailed status of the update.

Device updates

asedevice

Type	Version	Size	Status
Software	2109(2.2.1726.3923)	4.27 GB	Download started
Kubernetes	2109(2.2.1726.3923)	3.21 GB	Download started

- After the download is complete, the notification banner updates to indicate the completion. If you chose to automatically install the updates, the installation begins automatically.

If you chose to manually install updates later, then select the notification to open the **Device updates** blade. Select **Install update**.

Device updates

asedevice

Type	Version	Size	Installation impact
Software	2109(2.2.1726.3923)	4.27 GB	Device reboots automatically
Kubernetes	2109(2.2.1726.3923)	3.21 GB	Kubernetes workloads will be down

- You see a notification that the install is in progress. The portal also displays an informational alert to indicate that the install is in progress. The device goes offline and is in maintenance mode.

The screenshot shows the Azure Stack Edge device management interface for a device named 'asedevice'. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties), and Essentials. The main content area displays a message: 'Updating device - (0 of 2 updates installed). The device is in maintenance mode. Some operations will not be available in this state.' Below this, it says 'Your device is in maintenance!' and lists 'Deployed edge services' with 'No deployed services'. A red box highlights the maintenance mode message.

6. As this is a 1-node device, the device restarts after the updates are installed.

The screenshot shows the Azure Stack Edge device management interface for the same device 'asedevice'. The left sidebar is identical. The main content area now displays a message: 'Restarting the device after installing the update. This will take a while. Some operations will not be available in this state.' Below this, it says 'Your device is offline' and lists 'Deployed edge services' with 'No deployed services'. A red box highlights the restart message.

7. After the restart, the device software will finish updating. The Kubernetes software update will start automatically. The device goes offline again and is in maintenance mode.

The screenshot shows the Azure Stack Edge device management interface for the device 'asedevice'. The left sidebar is identical. The main content area displays a message: 'Updating device - (1 of 2 updates installed). The device is in maintenance mode. Some operations will not be available in this state.' Below this, it says 'Your device is in maintenance!' and lists 'Deployed edge services' with 'No deployed services'. A red box highlights the maintenance mode message.

8. Once the device software and Kubernetes updates are successfully installed, the banner notification disappears. The device status updates to **Your device is online**.

The screenshot shows the Azure Stack Edge device management interface for the device 'asedevice'. The left sidebar is identical. The main content area displays a message: 'Your device is online'. Below this, it lists 'Deployed edge services' with 'No deployed services' and 'Edge services'. A red box highlights the 'Your device is online' message.

Go to the local web UI and then go to **Software update** page. Verify that the device software and Kubernetes are successfully updated and the software version reflects that.

Azure Stack Edge Pro (1 GPU)

Software update
DBE-3Q6QHQ2

Install updates and hotfixes only if you are not able to apply these through the Azure portal. An update or a hotfix installation could restart your device. If the device restarts, I/O are disrupted and your device incurs downtime.

Device software version : Azure Stack Edge 2207 (2.2.2037.5375)
Device Kubernetes version : Azure Stack Kubernetes Edge 2207 (2.2.2037.5375)
Kubernetes server version: v1.22.6
IoT Edge version: 0.1.0-beta15
Azure Arc version: 1.6.6
GPU driver version: 515.48.07
CUDA version: 11.7

* Update file path

Apply Update

OVERVIEW CONFIGURATION DEVICE MAINTENANCE

- Overview
- Get started
- Network
- Advanced networking
- Cluster (Preview)
- Kubernetes
- Web proxy
- Device
- Update server
- Time
- Certificates
- Cloud details

- Power
- Hardware health
- Software update**
- Password change

Your device now has the latest version of device software and Kubernetes.

Use the local web UI

There are two steps when using the local web UI:

- Download the update or the hotfix
- Install the update or the hotfix

Each of these steps is described in detail in the following sections.

Download the update or the hotfix

Perform the following steps to download the update. You can download the update from the Microsoft-supplied location or from the Microsoft Update Catalog.

Do the following steps to download the update from the Microsoft Update Catalog.

1. Start the browser and navigate to <https://catalog.update.microsoft.com>.

The screenshot shows the Microsoft Update Catalog website. At the top, there's a navigation bar with back, forward, and refresh buttons, followed by a URL bar containing 'https://www.catalog.update.microsoft.com/Home.aspx' with a red box around it. Below the URL bar is a large globe icon and the text 'Microsoft Update Catalog'. To the right of the globe is a search bar with the placeholder 'Azure Stack Edge' and a 'Search' button, also with a red box around it. On the left side of the main content area, there's a 'FAQ | help' link. On the right, there's a 'Welcome' section with text about providing feedback and a 'Welcome' message. At the bottom of the page, there's a footer with links to 'MU Blog', 'Newsgroup', and 'Send us your feedback', all within a red box.

2. In the search box of the Microsoft Update Catalog, enter the Knowledge Base (KB) number of the hotfix or terms for the update you want to download. For example, enter **Azure Stack Edge**, and then click **Search**.

The update listing appears as **Azure Stack Edge Update 2207**.

3. Select **Download**. There are two packages to download for the update. The first package will have two files for the device software updates (*SoftwareUpdatePackage.0.exe*, *SoftwareUpdatePackage.1.exe*) and the second package has three files for the Kubernetes updates (*Kubernetes_Package.0.exe*, *Kubernetes_Package.1.exe*, and *Kubernetes_Package.2.exe*), respectively. Download the packages to a folder on the local system. You can also copy the folder to a network share that is reachable from the device.

Install the update or the hotfix

Prior to the update or hotfix installation, make sure that:

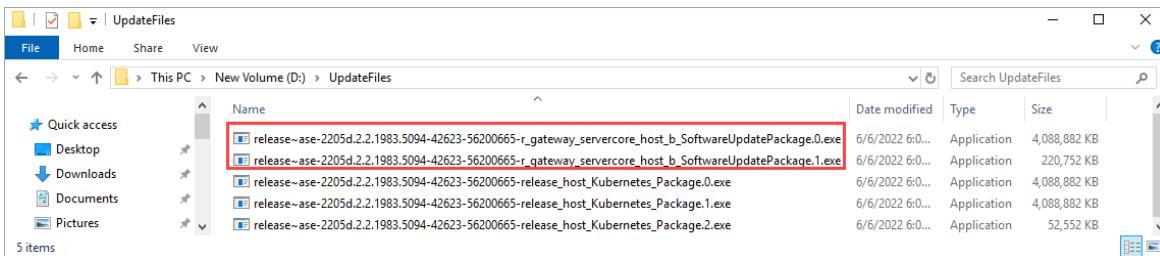
- You have the update or the hotfix downloaded either locally on your host or accessible via a network share.
- Your device status is healthy as shown in the **Overview** page of the local web UI.

The screenshot shows the Azure Stack Edge Pro local web interface. The top navigation bar includes a back arrow, a refresh button, and a search bar. The main content area is titled 'Azure Stack Edge Pro (1 GPU)' and has a 'Overview' tab selected, indicated by a red box. On the left, there's a sidebar with 'CONFIGURATION' and various icons for 'Get started', 'Network', 'Compute', 'Web proxy', 'Device', 'Update server', 'Time', and 'Certificates'. The main content area has two sections: 'System' and 'Device'. The 'System' section shows 'Health status' as 'Healthy' (highlighted with a red box), 'Software version' as '2.2.1636.3457', 'State' as 'Activated', and 'Azure portal' as 'asedevice'. The 'Device' section shows 'Device serial number' as '3Q6QHQ2', 'Node serial number' as '3Q6QHQ2', 'Available capacity' as '5.32 TB', and 'Compute acceleration' as '1 * GPU'.

This procedure takes around 20 minutes to complete. Perform the following steps to install the update or hotfix.

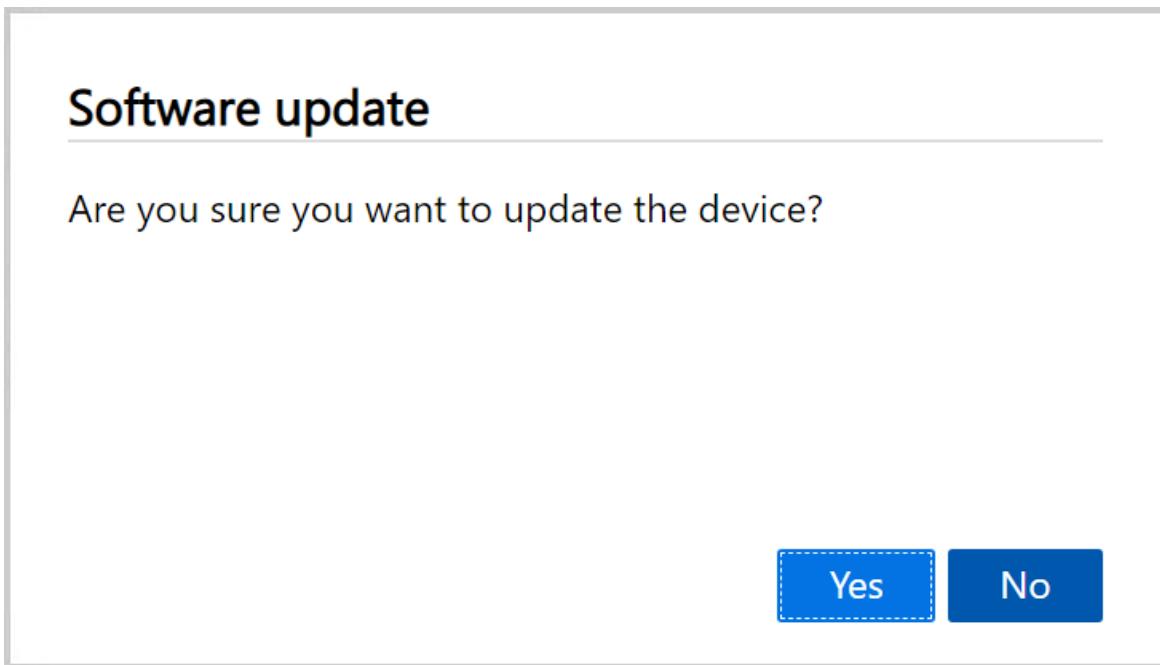
1. In the local web UI, go to **Maintenance > Software update**. Make a note of the software version that you are running.

- Provide the path to the update file. You can also browse to the update installation file if placed on a network share. Select the two software files (with *SoftwareUpdatePackage.0.exe* and *SoftwareUpdatePackage.1.exe* suffix) together.



- Select **Apply update**.

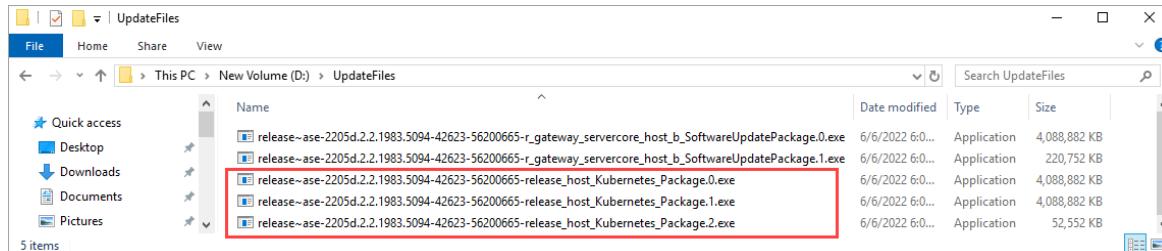
- When prompted for confirmation, select **Yes** to proceed. Given the device is a single node device, after the update is applied, the device restarts and there is downtime.



- The update starts. After the device is successfully updated, it restarts. The local UI is not accessible in this duration.
- After the restart is complete, you are taken to the **Sign in** page. To verify that the device software has

been updated, in the local web UI, go to **Maintenance > Software update**. For the current release, the displayed software version should be **Azure Stack Edge 2205**.

7. You will now update the Kubernetes software version. Select the remaining three Kubernetes files together (file with the *Kubernetes_Package.0.exe*, *Kubernetes_Package.1.exe*, and *Kubernetes_Package.2.exe* suffix) and repeat the above steps to apply update.



8. Select **Apply Update**.
9. When prompted for confirmation, select **Yes** to proceed.
10. After the Kubernetes update is successfully installed, there is no change to the displayed software in **Maintenance > Software update**.

A screenshot of the Azure Stack Edge Pro (1 GPU) maintenance interface. The left sidebar shows navigation options like Overview, Configuration (Get started, Network, Advanced networking, Cluster (Preview), Kubernetes, Web proxy, Device, Update server, Time, Certificates, Cloud details), Maintenance (Power, Hardware health, Software update, Password change), and a Help section. The 'Software update' section is currently selected and highlighted with a red box. It displays the following information:

- Device software version : Azure Stack Edge 2207 (2.2.2037.5375)
- Device Kubernetes version : Azure Stack Kubernetes Edge 2207 (2.2.2037.5375)
- Kubernetes server version: v1.22.6
- IoT Edge version: 0.1.0-beta15
- Azure Arc version: 1.6.6
- GPU driver version: 515.48.07
- CUDA version: 11.7

The 'Update file path' input field is also highlighted with a red box.

Next steps

Learn more about [administering your Azure Stack Edge Pro](#).

Reset and reactivate your Azure Stack Edge device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to reset, reconfigure, and reactivate an Azure Stack Edge device if you're having issues with the device or need to start fresh for some other reason.

After you reset the device to remove the data, you'll need to reactivate the device as a new resource. Resetting a device removes the device configuration, so you'll need to reconfigure the device via the local web UI.

For example, you might need to move an existing Azure Stack Edge resource to a new subscription. To do so, you would:

1. Reset data on the device by following the steps in [Reset device](#).
2. Create a new resource that uses the new subscription with your existing device, and then activate the device. Follow the steps in [Reactivate device](#).

Reset device

To wipe the data off the data disks of your device, you need to reset your device.

Before you reset, create a copy of the local data on the device if needed. You can copy the data from the device to an Azure Storage container.

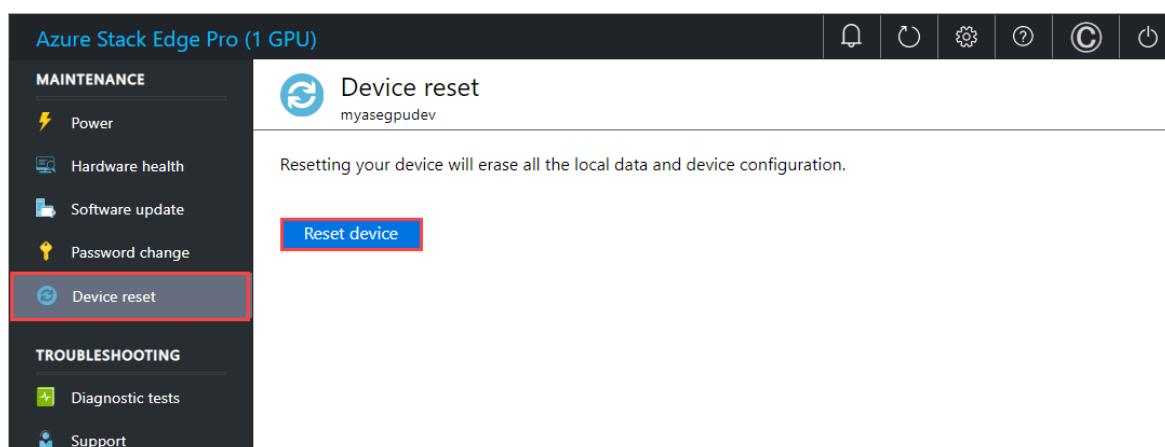
IMPORTANT

Resetting your device will erase all local data and workloads from your device, and that can't be reversed. Reset your device only if you want to start afresh with the device.

You can reset your device in the local web UI or in PowerShell. For PowerShell instructions, see [Reset your device](#).

To reset your device using the local web UI, take the following steps.

1. In the local web UI, go to **Maintenance > Device reset**.
2. Select **Reset device**.



3. When prompted for confirmation, review the warning. Type **Yes** and then select **Yes** to continue.

Confirm device reset

Are you sure you want to reset your device to factory settings? This action deletes all the local data on the device. To confirm, enter 'Yes' and click Yes.

* Enter 'Yes'



The reset erases the data off the device data disks. Depending on the amount of data on your device, this process takes about 30-40 minutes.

Reactivate device

After you reset the device, you'll need to reactivate the device as a new resource. After placing a new order, you'll need to reconfigure and then reactivate the new resource.

To reactivate your existing device, follow these steps:

1. Create a new order for the existing device by following the steps in [Create a new resource](#). On the **Shipping address** tab, select **I already have a device**.

Create a resource and order a device

X

Azure Stack Edge Pro R

Basics **Shipping address** Tags Review + create

I already have a device.

Enter the shipping address for the device.

Contact person * ⓘ

Company name *

Address *

Zip / Postal code *

City *

State / Province / Region *

Country / Region

Work phone * ⓘ

Email ID(s) * ⓘ

Review + create

Previous

Next: Tags



2. [Get the activation key.](#)
3. [Connect to the device.](#)
4. [Configure the network for the device.](#)
5. [Configure device settings.](#)
6. [Configure certificates.](#)
7. [Activate the device.](#)

Next steps

- Learn how to [Connect to an Azure Stack Edge device](#).

Return your Azure Stack Edge device

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R ✓ Azure Stack Edge Pro - FPGA

This article describes how to wipe the data and then return your Azure Stack Edge device. After you've returned the device, you can also delete the resource associated with the device.

In this article, you learn how to:

- Wipe the data off the data disks on the device
- Initiate device return in Azure portal
- Pack up the device and schedule a pickup
- Delete the resource in Azure portal

Erase data from the device

To wipe the data off the data disks of your device, you need to reset your device.

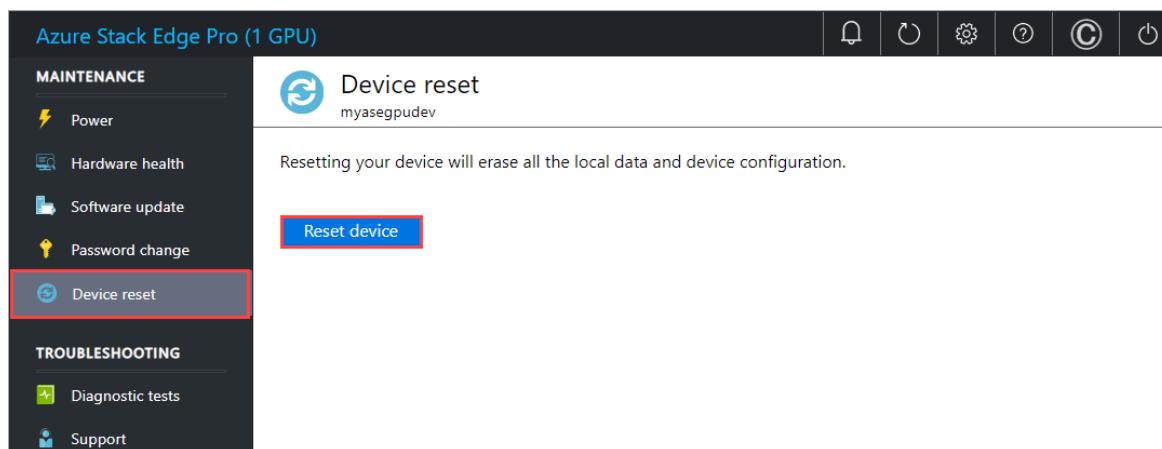
Before you reset, create a copy of the local data on the device if needed. You can copy the data from the device to an Azure Storage container.

You can initiate the device return even before the device is reset.

You can reset your device in the local web UI or in PowerShell. For PowerShell instructions, see [Reset your device](#).

To reset your device using the local web UI, take the following steps.

1. In the local web UI, go to **Maintenance > Device reset**.
2. Select **Reset device**.



3. When prompted for confirmation, review the warning. Type **Yes** and then select **Yes** to continue.

Confirm device reset

Are you sure you want to reset your device to factory settings? This action deletes all the local data on the device. To confirm, enter 'Yes' and click Yes.

* Enter 'Yes'



The reset erases the data off the device data disks. Depending on the amount of data on your device, this process takes about 30-40 minutes.

NOTE

- If you're exchanging or upgrading to a new device, we recommend that you reset your device only after you've received the new device.
- The device reset only deletes all the local data off the device. The data that is in the cloud isn't deleted and collects charges. This data needs to be deleted separately using a cloud storage management tool like [Azure Storage Explorer](#).

Initiate device return

To begin the return process, take the following steps.

- [Azure Edge Hardware Center \(Preview\)](#)
- [Portal \(Classic\)](#)

If you used the Azure Edge Hardware Center to order your device, follow these steps to return the device:

1. In the Azure portal, go to your Azure Edge Hardware Center order item resource. In the **Overview**, go to the top command bar in the right pane and select **Return**. The return option is only enabled after you have received a device.

The screenshot shows the Azure Edge Hardware Center Overview blade for an order item named 'DemoOrderAS3contoso-re-03'. The top navigation bar includes 'Home >', the order name, and a 'PREVIEW' link. Below the navigation is a search bar and a set of top-level navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Automation, Tasks (preview), Support + troubleshooting, and New Support Request. On the right side, there's a summary section with details like Resource group, Location, Subscription, and Tags. Below this is a status section showing a flow from 'Confirmed' to 'Shipped' to 'Delivered'. A message states 'Order item delivered' and 'Your order item was delivered to your address.' At the bottom, there's a call-to-action to 'Configure and activate your hardware by creating an Azure Stack Edge management resource.'

2. In the **Return hardware** blade, provide the following information:

Return hardware

PREVIEW

Reset your hardware unit and initiate return by providing the information below.

Reason for returning *

Business need is met

Hardware details

Serial number *

DemoOrderAS3contoso-re-03

Service tag

 Shipping box required to return the hardware unit

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

 I have reviewed the provided information. I agree to the privacy terms.

Pickup details

Contact person

Address

Gus Poland
4255555555
gusp@contoso.com
Contoso LE

One Microsoft Way
Building 52
Redmond
WA 98152 United States

[Add a new address](#) [Select a different address](#)

a. From the dropdown list, select a **Reason for returning**.

b. Provide the serial number of the device. To get the device serial number, go to the local web UI of the device and then go to **Overview**.

System		Device	
Health status : Healthy	Device serial no. : HW9C1T2	Software version : 2.1.1272.1632	Node serial no. : HW9C1T2
Software version : 2.1.1272.1632	Total capacity : 4.19 TB	Total capacity : 4.19 TB	State : Not activated
Total capacity : 4.19 TB	Available capacity : 4.15 TB	Available capacity : 4.15 TB	

c. (Optional) Enter the **Service tag** number. The service tag number is an identifier with five or more characters, which is unique to your device. The service tag is located on the bottom-right corner of the device (as you face the device). Pull out the information tag (it is a slide-out label panel). This panel contains system information such as service tag, NIC, MAC address, and so on.



- d. To request a return shipping box, check the **Shipping box required to return the hardware unit**. You can request it. Answer **Yes** to the question **Need an empty box to return**.
- e. Review the **Privacy terms**, and select the checkbox by the note that you have reviewed and agree to the privacy terms.
- f. Verify the **Pickup details**. By default, these are set to your shipping address. You can add a new address or select a different one from the saved addresses for the return pickup.

Return hardware

Reason for returning: Business need is met

Hardware details:

- Serial number: DemoOrderAS3contoso-re-03
- Service tag: ASE-service-tag-number-1234

Shipping box required to return the hardware unit

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Pickup details

Contact person	Address
Gus Poland 4255555555 gusp@contoso.com Contoso LE	One Microsoft Way Building 52 Redmond WA 98152 United States

[Add a new address](#) [Select a different address](#)

Select address(es)

Showing addresses from address book with selected ship to country/region | PREVIEW

Maximum of 20 addresses can be added to an order

Contact person	Address
Noopur 9112312312 test@test.com Microsoft	RedmondOffice One Microsoft Way Redmond WA 233435 United States
Bldg42Office One microsoft way, building 42 Redmond WA 233434 United States	TestReturnAddress 9112312312 test@test.com
AddressAlias Line1 City	

Initiate Return **Select** **Cancel**

g. Select **Initiate return**.

- Once the return request is submitted, the order item resource starts reflecting the status of your return shipment. The status progresses from **Return initiated** to **Picked up** to **Return completed**. Use the portal to check the return status of your resource at any time.

DemoOrderAS3contoso-re-03

Resource group (change) : testRG

Location (change) : East US

Subscription (change) : Azure Data Box testing

Subscription ID : <Subscription ID>

Tags (change) : test : test

Return initiated → **Picked-up** → **Return completed**

Return initiated

Return request for your hardware is in progress. We will reach out to you with more details via email.

Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage

Device serial number: DemoOrderAS3contoso-re-03

Order name : DemoOrderAS3

Requested on : 9/16/2021

Pickup address : 1020 Enterprise Way, Sunnyvale CA 94089 US

Contact information : Gus Poland 4085555555, gus.poland@contoso.com

[View Updates](#)

- Once the request is initiated, the Azure Stack Edge operations team reaches out to you to help schedule the device pickup.

The next step is to package the device.

Pack the device

To pack the device, take the following steps.

- Shut down the device. In the local web UI, go to **Maintenance > Power settings**.
- Select **Shut down**. When prompted for confirmation, click **Yes** to continue. For more information, see [Manage power](#).

3. Unplug the power cables and remove all the network cables from the device.
4. Carefully prepare the shipment package as per the following instructions and as shown in the following diagram:



- a. Use the shipping box you requested from Azure or the original shipping box with its foam packaging.
- b. Place the bottom foam piece in the box.
- c. Lay the device on top of the foam taking care that it sits snugly in the foam.
- d. Place the top foam piece in the package.
- e. Place the power cords in the accessory tray and the rails on the top foam piece.
- f. Seal the box and affix the shipping label that you received from Azure on the package.

IMPORTANT

If proper guidelines to prepare the return shipment aren't observed, the device could be damaged and damaged device fee may apply. Review the [Product Terms of service](#) and the [FAQ on lost or damaged device](#).

Schedule a pickup

To schedule a pickup, take the following steps.

1. Schedule a pickup with your regional carrier. If returning the device in US, your carrier could be UPS or FedEx. To schedule a pickup with UPS:

- a. Call the local UPS (country/region-specific toll free number).
 - b. In your call, quote the reverse shipment tracking number as shown on your printed label.
 - c. If the tracking number isn't quoted, UPS will require you to pay an extra charge during pickup.
- Instead of scheduling the pickup, you can also drop off the Azure Stack Edge at the nearest drop-off location.

Complete return

In this section, you can verify when the return is complete and then choose to delete the order.

-
- [Azure Edge Hardware Center \(Preview\)](#)
 - [Portal \(Classic\)](#)

When you initiate the return, the billing is paused. After the device is received at the Azure datacenter, the device is inspected for damage or any signs of tampering.

- If the device arrives intact and is in good shape, Azure Stack Edge operations team will contact you to confirm that the device was returned. You can choose to delete the resource associated with the device in the Azure portal.
- If the device arrives significantly damaged, charges may apply. For details, see the [FAQ on lost or damaged device](#) and [Product Terms of Service](#).

Next steps

- Learn how to [Get a replacement Azure Stack Edge device](#).

Replace your Azure Stack Edge device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to replace your Azure Stack Edge device. A replacement device is needed when the existing device has a hardware failure or needs an upgrade.

In this article, you learn how to:

- Open a Support ticket for hardware issue
- Create a new order for a replacement device in the Azure portal
- Install, activate the replacement device
- Return the original device

Open a Support ticket

If your existing device has a hardware failure, open a Support ticket by following these steps:

1. Open a Support ticket with Microsoft Support indicating that you wish to return the device. Select the **Azure Stack Edge Hardware** problem type, and choose the **Hardware issues** subtype.

The screenshot shows the 'contoso-edgeprod01 - New support request' page in the Azure portal. The 'Basics' tab is selected. On the left sidebar, 'New support request' is highlighted with a red box. The main form fields include:

- * Issue type: Technical
- * Subscription: MyAzureStack-test-subscription
- * Service: My services (selected)
- Azure Stack Edge and Data Box Gateway
- * Resource: contoso-edgeprod01
- * Problem type: Azure Stack Edge Hardware
- * Problem subtype: Hardware issues
- * Subject: I need to return the Azure Stack Edge device.

2. A Microsoft Support engineer will get in touch with you to determine if a Field Replacement Unit (FRU) can fix the problem and is available for this instance. If a FRU is not available or the device needs a hardware upgrade, Support will guide you to place a new order and return your old device.

Create a new order

Create a new resource for the activation of your replacement device by following the steps in [Create a new resource](#).

NOTE

Activation of a replacement device against an existing resource is not supported. The new resource is considered a new order. You will start getting billed 14 days after the device is shipped to you.

Install and activate the replacement device

Follow these steps to install and activate the replacement device:

1. [Install your device](#).
2. [Activate your device](#) against the new resource that you created earlier.

Return your existing device

Follow all the steps to return the original device:

1. [Erase the data on the device](#).
2. [Initiate device return](#) for the original device.
3. [Schedule a pickup](#).
4. Once the device is received at Microsoft, you can [Delete the resource](#) associated with the returned device.

Next steps

- Learn how to [Return an Azure Stack Edge device](#).

Prepare for an Azure Stack Edge Pro GPU device failure

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

This article helps you prepare for a device failure by detailing how to save and back up the device configuration and data on your Azure Stack Edge Pro GPU device.

The article does not include steps to back up Kubernetes and IoT containers deployed on your Azure Stack Edge Pro GPU device.

Understand device failures

Your Azure Stack Edge Pro GPU device can experience two types of hardware failures.

- Tolerable failures that require you to replace a hardware component. These failures will allow you to operate the device in a degraded state. Examples of these failures include a single failed power supply unit (PSU) or a single failed disk on the device. In each of these cases, the device can continue to operate. Contact Microsoft Support as soon as possible to replace the failed components.
- Non-tolerable failures that require you to replace the entire device - for example, when two disks have failed on your device. In these cases, contact Microsoft Support immediately. After they determine that a device replacement's needed, Support will help with the replacement of your Azure Stack Edge device.

To prepare for non-tolerable failures, you need to back up the following things on your device:

- Information on the device configuration
- Data in Edge local shares and Edge cloud shares
- Files and folders associated with the VMs running on your device

Back up device configuration

During initial configuration of the device, it's important to keep a copy of the device configuration information as outlined in the [Deployment checklist](#). During recovery, this configuration information will be used to apply to the new replacement device.

Protect device data

The device data can be of one of the following types:

- Data in Edge cloud shares
- Data in local shares
- Files and folders on VMs

The following sections discuss the steps and recommendations to protect each of these types of data on your device.

Protect data in Edge cloud shares

You can create Edge cloud shares that tier data from your device to Azure. Depending on the network bandwidth

available, configure bandwidth templates on your device to minimize any data loss if a non-tolerable failure occurs.

IMPORTANT

If the device has a non-tolerable failure, local data that is not tiered off from the device to Azure may be lost.

Protect data in Edge local shares

If you're deploying Kubernetes or IoT Edge, configure to save the application data on the device locally and do not sync with Azure Storage. The data is stored on a share on the device. You might find it important to backup the data in these shares.

The following third-party data protection solutions can provide a backup solution for the data in the local SMB or NFS shares.

THIRD-PARTY SOFTWARE	REFERENCE TO THE SOLUTION
Cohesity	https://www.cohesity.com/solution/cloud/azure/ For details, contact Cohesity.
Commvault	https://www.commvault.com/azure For details, contact Commvault.
Veritas	http://veritas.com/azure For details, contact Veritas.
Veeam	https://www.veeam.com/kb4041 For details, contact Veeam.

Protect files and folders on VMs

Azure Stack Edge works with Azure Backup and other third-party data protection solutions to provide a backup solution to protect data contained in the VMs that are deployed on the device. The following table lists references to available solutions that you can choose from.

BACKUP SOLUTIONS	SUPPORTED OS	REFERENCE
Microsoft Azure Recovery Services (MARS) agent for Azure Backup	Windows	About MARS agent
Cohesity	Windows, Linux	Microsoft Azure Integration, Backup & Recovery solution brief For details, contact Cohesity.
Commvault	Windows, Linux	https://www.commvault.com/azure For details, contact Commvault.
Veritas	Windows, Linux	https://vox.veritas.com/t5/Protection/Protecting-Azure-Stack-Edge-with-NetBackup/ba-p/883370 For details, contact Veritas.

BACKUP SOLUTIONS	SUPPORTED OS	REFERENCE
Veeam	Windows, Linux	https://www.veeam.com/kb4041 For details, contact Veeam.

Next steps

- Learn how to [Recover from a failed Azure Stack Edge Pro GPU device](#).

Recover from a failed Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R

This article describes how to recover from a non-tolerable failure on your Azure Stack Edge Pro GPU device. A non-tolerable failure on Azure Stack Edge Pro GPU device requires a device replacement.

Before you begin

Make sure that you have:

- Contacted Microsoft Support regarding the device failure and they have recommended a device replacement.
- Backed up your device configuration as described in [Prepare for a device failure](#).

Configure replacement device

When your device encounters a non-tolerable failure, you need to order a replacement device. The configuration steps for the replacement device remain the same.

Retrieve the device configuration information that you backed up from the device that failed. You will use this information to configure the replacement device.

Follow these steps to configure the replacement device:

1. Gather the information required in the [Deployment checklist](#). You can use the information that you saved from the previous device configuration.
2. Order a new device of the same configuration as the one that failed. To place an order, [Create a new Azure Stack Edge resource](#) in the Azure portal.
3. [Unpack, rack mount and cable your device](#).
4. [Connect to the local UI of the device](#).
5. Configure the network using the same IP addresses that you used for your old device. Using the same IP addresses will minimize the impact on any client machines used in your environment. See how to [configure network settings](#).
6. Assign the same device name and DNS domain as your old device. That way, your clients can use the same device name to talk to the new device. See how to [configure device setting](#).
7. Configure certificates on the new device in the same way as you did for the old device. Keep in mind that the new device has a new node serial number. If you used your own certificates on the old device, you will need to get a new node certificate. See how to [configure certificates](#).
8. Get the activation key from the Azure portal and activate the new device. See how to [activate the device](#).

You are now ready to deploy the workloads that you were running on the old device.

Restore Edge cloud shares

Follow these steps to restore the data on the Edge cloud shares on your device:

1. [Add shares](#) with the same share names created previously on the failed device. Make sure that while creating

- shares, **Select blob container** is set to **Use existing** option and then select the container that was used with the previous device.
2. **Add users** that had access to the previous device.
 3. **Add storage accounts** associated with the shares previously on the device. While creating Edge storage accounts, select from an existing container and point to the container that was mapped to the Azure Storage account mapped on the previous device. Any data from the device that was written to the Edge storage account on the previous device was uploaded to the selected storage container in the mapped Azure Storage account.
 4. **Refresh the share** data from Azure. This pulls down all the cloud data from the existing container to the shares.

Restore Edge local shares

To prepare for a potential device failure, you may have deployed one of the following backup solutions to protect the local shares data from your Kubernetes or IoT workloads:

THIRD-PARTY SOFTWARE	REFERENCE TO THE SOLUTION
Cohesity	https://www.cohesity.com/solution/cloud/azure/ For details, contact Cohesity.
Commvault	https://www.commvault.com/azure For details, contact Commvault.
Veritas	http://veritas.com/azure For details, contact Veritas.
Veeam	https://www.veeam.com/kb4041 For details, contact Veeam.

After the replacement device is fully configured, enable the device for local storage.

Follow these steps to recover the data from local shares:

1. **Configure compute on the device.**
2. **Add a local share** back.
3. Run the recovery procedure provided by the data protection solution of choice. See references from the preceding table.

Restore VM files and folders

To prepare for a potential device failure, you may have deployed one of the following backup solutions to protect the data on VMs:

BACKUP SOLUTIONS	SUPPORTED OS	REFERENCE
Microsoft Azure Recovery Services (MARS) agent for Azure Backup	Windows	About MARS agent
Cohesity	Windows, Linux	Microsoft Azure Integration, Backup & Recovery solution brief For details, contact Cohesity.

BACKUP SOLUTIONS	SUPPORTED OS	REFERENCE
Commvault	Windows, Linux	https://www.commvault.com/azure For details, contact Commvault.
Veritas	Windows, Linux	https://vox.veritas.com/t5/Protection/Protecting-Azure-Stack-edge-with-NetBackup/ba-p/883370 For details, contact Veritas.
Veeam	Windows, Linux	https://www.veeam.com/kb4041 For details, contact Veeam.

After the replacement device is fully configured, you can redeploy the VMs with the VM image previously used.

Follow these steps to recover the data in the VMs:

1. [Deploy a VM from a VM image](#) on the device.
2. Install the data protection solution of choice on the VM.
3. Run the recovery procedure provided by the data protection solution of choice. See references from the preceding table.

Restore a Kubernetes deployment

If you performed your Kubernetes deployment via Azure Arc, you can restore the deployment after a non-tolerable device failure. You'll need to redeploy the customer application/containers from the `git` repository where the application definition is stored. [Information on deploying Kubernetes with Azure Arc](#)

Next steps

- Learn how to [Return an Azure Stack Edge Pro device](#).

Review alerts on Azure Stack Edge

9/21/2022 • 23 minutes to read • [Edit Online](#)

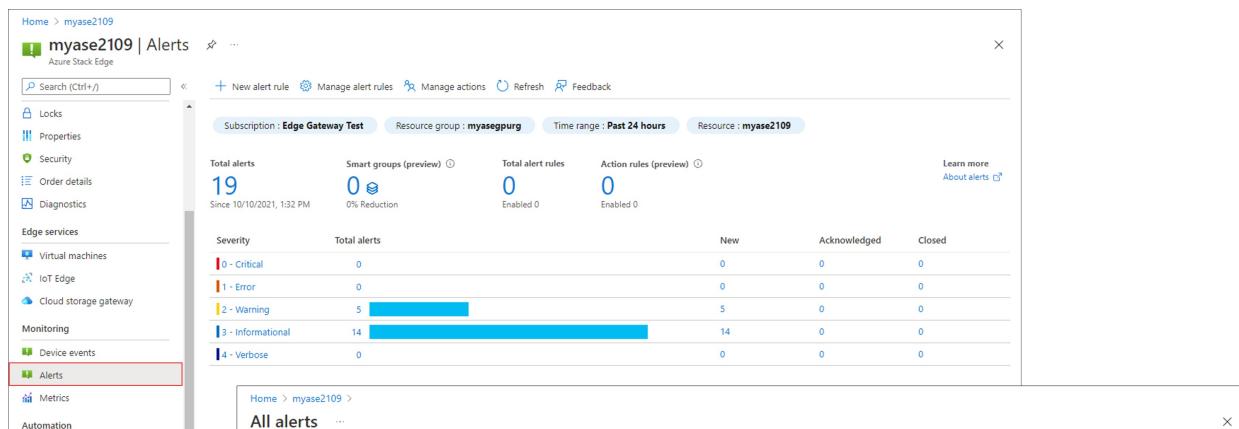
APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to view alerts and interpret alert severity for events on your Azure Stack Edge devices. The alerts generate notifications in the Azure portal. The article includes a quick-reference for Azure Stack Edge alerts.

Overview

The Alerts blade for an Azure Stack Edge device lets you review Azure Stack Edge device-related alerts in real-time. From this blade, you can centrally monitor the health issues of your Azure Stack Edge devices and the overall Microsoft Azure Azure Stack Edge solution.

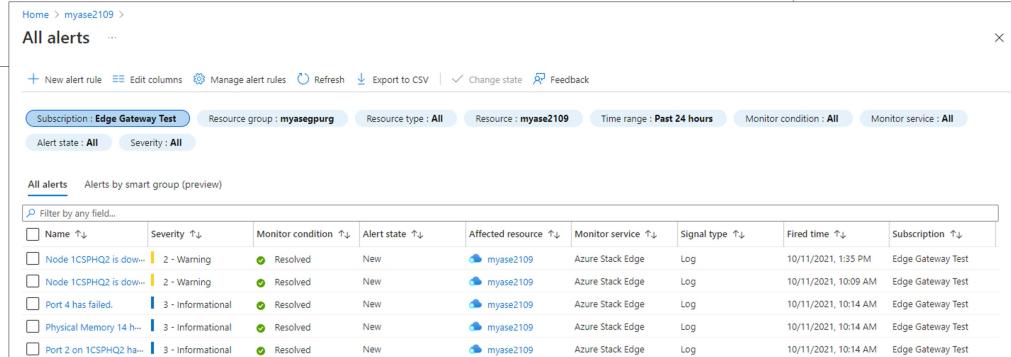
The initial display is a high-level summary of alerts at each severity level. You can drill down to see individual alerts at each severity level.



The screenshot shows the Azure Stack Edge Alerts blade. At the top, it displays a summary: Total alerts (19), Smart groups (0), Total alert rules (0), and Action rules (0). Below this is a table showing the distribution of alerts by severity:

Severity	Total alerts	New	Acknowledged	Closed
0 - Critical	0	0	0	0
1 - Error	0	0	0	0
2 - Warning	5	5	0	0
3 - Informational	14	14	0	0
4 - Verbose	0	0	0	0

At the bottom of the main pane, there is a link to 'Learn more About alerts'.



The screenshot shows the 'All alerts' blade. It lists six alerts, all of which are resolved (green status indicators). The columns include Name, Severity, Monitor condition, Alert state, Affected resource, Monitor service, Signal type, Fired time, and Subscription.

Name	Severity	Monitor condition	Alert state	Affected resource	Monitor service	Signal type	Fired time	Subscription
Node 1CSPHQ2 is down	2 - Warning	Resolved	New	myase2109	Azure Stack Edge	Log	10/11/2021, 1:35 PM	Edge Gateway Test
Node 1CSPHQ2 is down	2 - Warning	Resolved	New	myase2109	Azure Stack Edge	Log	10/11/2021, 10:09 AM	Edge Gateway Test
Port 4 has failed	3 - Informational	Resolved	New	myase2109	Azure Stack Edge	Log	10/11/2021, 10:14 AM	Edge Gateway Test
Physical Memory 14 h...	3 - Informational	Resolved	New	myase2109	Azure Stack Edge	Log	10/11/2021, 10:14 AM	Edge Gateway Test
Port 2 on 1CSPHQ2 ha...	3 - Informational	Resolved	New	myase2109	Azure Stack Edge	Log	10/11/2021, 10:14 AM	Edge Gateway Test

Alert severity levels

Alerts have different severity levels, depending on the impact of the alert situation and the need for a response to the alert. The severity levels are:

- **Critical** – This alert is in response to a condition that is affecting the successful performance of your system. Action is required to ensure that Azure Stack Edge service is not interrupted.
- **Warning** – This condition could become critical if not resolved. You should investigate the situation and take any action required to resolve the issue.
- **Informational** – This alert contains information that can be useful in tracking and managing your system.

Configure alert notifications

You can also send alert notifications by email for events on your Azure Stack Edge devices. To manage these

alert notifications, you create action rules. The action rules can trigger or suppress alert notifications for device events within a resource group, an Azure subscription, or on a device. For more information, see [Using action rules to manage alert notifications](#).

Alerts quick-reference

The following tables list some of the Azure Stack Edge alerts that you might run across, with descriptions and recommended actions. The alerts are grouped in the following categories:

- [Cloud connectivity alerts](#)
- [Edge compute alerts](#)
- [Local Azure Resource Manager alerts](#)
- [Performance alerts](#)
- [Storage alerts](#)
- [Security alerts](#)
- [Key vault alerts](#)
- [Hardware alerts](#)
- [Update alerts](#)
- [Virtual machine alerts](#)

NOTE

In the alerts tables below, some alerts are triggered by more than one event type. If the events have different recommended actions, the table has an alert entry for each of the events.

Cloud connectivity alerts

The following alerts are raised by a failed connection to an Azure Stack Edge device or when no heartbeat is detected.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not connect to the Azure.	Critical	Check your internet connection. In the local web UI of the device, go to Troubleshooting > Diagnostic tests . Run the Internet connectivity diagnostic test.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Lost heartbeat from your device.	Critical	<p>If your device is offline, then the device is not able to communicate with the Azure service. This could be due to one of the following reasons:</p> <ul style="list-style-type: none"> • The Internet connectivity is broken. Check your internet connection. In the local web UI of the device, go to Troubleshooting > Diagnostic tests. Run the diagnostic tests. Resolve the reported issues. • The device is turned off or paused on the hypervisor. Turn on your device! For more information, go to Manage power. • Your device could have rebooted due to an update. Wait a few minutes and try to reconnect.

Edge compute alerts

The following alerts are raised for Edge compute or the compute acceleration card, which can be a Graphical Processing Unit (GPU) or Vision Processing Unit (VPU) depending on the device model.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Edge compute is unhealthy.	Critical	<p>Restart your device to resolve the issue. In the local web UI of your device, go to Maintenance > Power settings and click Restart. If the problem persists, contact Microsoft Support.</p>
Edge compute ran into an issue with name resolution.	Critical	<p>Ensure that your DNS server {15} is online and reachable. If the problem persists, contact your network administrator.</p>
Compute acceleration card configuration has an issue.*	Critical	<p>We've detected an unsupported compute acceleration card configuration. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Compute acceleration card configuration has an issue.*	Critical	<p>We've detected an unsupported compute acceleration card. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.
Compute acceleration card configuration has an issue.*	Critical	<p>This may be due to one of the following reasons:</p> <ol style="list-style-type: none"> 1. If the card is an FPGA, the image is not valid. 2. Compute acceleration card isn't seated properly. 3. Underlying issues with the compute acceleration driver. <p>To resolve the issue, redeploy the Azure IoT Edge module. Once the issue is resolved, the alert goes away. If the issue persists, do the following:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 3. Attach the package to the support request.
Compute acceleration card configuration has an issue.*	Critical	<p>This is due to an internal error. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 3. Attach the package to the support request.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Compute acceleration card configuration has an issue.*	Critical	<p>As your Azure IoT Machine Learning module starts up, you may see this transient issue. Wait a few minutes to see if the issue resolves.</p> <p>If the issue persists, do the following:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. Create a Support request. 3. Attach the package to the support request.
Compute acceleration card driver software is not running.	Critical	<p>This is due to an internal error. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.
Compute acceleration card on your device is unhealthy.	Critical	<p>This is due to an internal error. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.
Shutting down the compute acceleration card as the card temperature has exceeded the operating limit!	Critical	<p>This is due to an internal error. Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Compute acceleration card performance is degraded.	Warning	<p>This might be because the compute acceleration card has a high usage. Consider stopping or reducing the workload on the Azure IoT Machine Learning module.</p> <p>Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.
Compute acceleration card temperature is rising.	Warning	<p>This might be because the compute acceleration card has a high usage. Consider stopping or reducing the workload on the Azure IoT Machine Learning module.</p> <p>Before you contact Microsoft Support, follow these steps:</p> <ol style="list-style-type: none"> 1. In the local web UI, go to Troubleshooting > Support. 2. Create and download a support package. 3. Create a Support request. 4. Attach the package to the support request.
Edge compute couldn't access data on share {16}.	Warning	<p>Verify that you can access share {16}. If you can access the share, it indicates an issue with Edge compute.</p> <p>To resolve the issue, restart your device. In the local web UI of your device, go to Maintenance > Power settings and click Restart.</p> <p>If the issue persists, contact Microsoft Support.</p>
Edge compute couldn't access data on share {16}. This may be because the share doesn't exist anymore.	Warning	<p>If the share does not {16} exist, restart your device to resolve the issue. In the local web UI of your device, go to Maintenance > Power settings and click Restart.</p> <p>If the problem persists, contact Microsoft Support.</p>
IoT Edge agent is not running.	Warning	<p>Restart your device to resolve the issue. In the local web UI of your device, go to Maintenance > Power settings and click Restart.</p> <p>If the problem persists, contact Microsoft Support.</p>

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
IoT Edge service is not running.	Warning	<p>Restart your device to resolve the issue. In the local web UI of your device, go to Maintenance > Power settings and click Restart. If the problem persists, contact Microsoft Support.</p>
Storage used by Edge compute is getting full.	Warning	<p>Contact Microsoft Support for next steps.</p>
Your Edge compute module {20} is disconnected from IoT Edge	Warning	<p>Restart your device to resolve the issue. In the local web UI of your device, go to Maintenance > Power settings and click Restart. If the problem persists, contact Microsoft Support.</p>
Your Edge compute module(s) may be using a local mount point {15} that is different than the local mountpoint used by a share.	Warning	<p>Ensure that the local mountpoint {15} used is the one that is mapped to the share.</p> <ul style="list-style-type: none"> • In the Azure portal, go to Shares in your Data Box Edge resource. • Select a share to view the local mount point for Edge compute module. • Ensure that this path is used in the module and deploy the module again. <p>Restart the device. In the local web UI of your device, go to Maintenance > Power settings and click Restart. If the alert persists, contact Microsoft Support.</p>

* This alert is triggered by more than one event type, with different recommended actions.

Local Azure Resource Manager (ARM) alerts

The following alerts are raised by the local Azure Resource Manager (ARM), which is used to connect to the local APIs on Azure Stack Edge devices.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Specified service authentication certificate with thumbprint '{0}' does not have a private key	Critical	<p>If the issue persists, contact Microsoft Support.</p>
Certificate with thumbprint '{0}' at location '{1}' is not found or not accessible.	Critical	<p>If the issue persists, contact Microsoft Support.</p>

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Unable to connect endpoint: '{0}'	Critical	If the issue persists, contact Microsoft Support .
Error occurred during web request: '{0}'	Critical	If the issue persists, contact Microsoft Support .
Request timed out for url: '{0}'	Critical	If the issue persists, contact Microsoft Support .
Unable to get Token using login endpoint '{0}' for resource '{1}'	Critical	If the issue persists, contact Microsoft Support .
Unknown error occurred. ErrorCode:'{0}'. Details: '{1}'	Critical	If the issue persists, contact Microsoft Support .
Could not start the VM service on the device.	Critical	If you see this alert, contact Microsoft Support .
VM service is not running on the device.	Critical	If you see this alert, contact Microsoft Support .

Performance alerts

The following alerts indicate performance issues related to storage or to CPU, memory, or disk usage on an Azure Stack Edge device.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
The CPU utilization on your device has exceeded the threshold for an extended duration.	Critical	Reduce workloads or modules running on your device. If the problem persists, contact Microsoft Support .
The CPUs reserved for the virtual machines on your device exceeds the configured threshold.	Critical	Take one of the following steps: 1. Reduce CPU reservation for the virtual machines running on your device. 2. Remove some virtual machines off your device.
The memory used by the virtual machines on your device exceeds the configured threshold.	Critical	Take one of the following steps: 1. Reduce memory allocated for the virtual machines running on your device. 2. Remove some virtual machines off your device.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
The data volume on the device is {0}% full. Writes into the device are being throttled.	Critical	<p>1. Distribute your data ingestion to target off-peak hours.</p> <p>2. This may be due to a slow network. In the local web UI of the device, go to Troubleshooting > Diagnostic tests and click Run diagnostic tests. Resolve the reported issues.</p> <p>If the issue persists, contact Microsoft Support.</p>
The memory used by the virtual machines on node {0} of your device exceeds the configured threshold.	Critical	The device will try to balance load across other nodes. Consider reducing some virtual machine workloads from your device. If the problem persists, contact Microsoft Support .
Your device is almost out of storage space. If a disk fails, then you may not be able to restore data on this device.	Critical	Delete data to free up capacity on your device.
The CPU utilization on node {0} of your device has exceeded the threshold for an extended duration.*	Warning	The device will try to balance load across other nodes. Consider reducing some virtual machine workloads from your device. If the problem persists, contact Microsoft Support .
The CPU utilization on node {0} of your device has exceeded the threshold for an extended duration.*	Warning	Reduce workloads or modules running on your device. If the problem persists, contact Microsoft Support .
The node {0} on your device is using more memory than expected.	Warning	If the problem persists, contact Microsoft Support .
The CPUs reserved for the virtual machines on node {0} of your device exceeds the configured threshold.	Warning	<p>Take one of the following steps:</p> <ol style="list-style-type: none"> 1. Reduce CPU reservation for the virtual machines running on your device. 2. Remove some virtual machines off your device.
The memory used by the virtual machines on your device exceeds the configured threshold.	Warning	<p>Take one of the following steps:</p> <ol style="list-style-type: none"> 1. Reduce memory allocated for the virtual machines running on your device. 2. Remove some virtual machines off your device.
Too many virtual machines are active on node {0} of your device.	Warning	The device will try to balance load across other nodes. Consider reducing some virtual machine workloads from your device. If the problem persists, contact Microsoft Support .

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
The virtual hard disk {0} is nearing its capacity.	Warning	Delete some data to free capacity.

* This alert is triggered by more than one event type, with different recommended actions.

Storage alerts

The following alerts are for issues that occur when accessing or uploading data to Azure Storage.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not access volume {0}.*	Critical	<p>This could happen when the volume is offline, or too many drives or servers have failed or are disconnected. Take the following steps:</p> <ol style="list-style-type: none"> 1. Reconnect missing drives and bring up servers that are down. 2. Allow the sync to complete. 3. Replace any failed drives and restore lost data from backup.
Could not access volume {0}.*	Critical	<p>In the local web UI of the device, go to Troubleshooting > Diagnostic tests, and click Run diagnostic tests. Resolve the reported issues. If the issue persists, contact Microsoft Support.</p>
Could not find volume {0}.*	Critical	If the issue persists, contact Microsoft Support .
Could not find volume {0}.*	Critical Warning	Expand the volume or migrate workloads to other volumes.
Some data on this volume {0} is not fully resilient. It remains accessible.	Informational	Restoring resiliency of the data.
Could not upload {0} file(s) from share {1}.	Critical	<p>This could be due to one of the following reasons:</p> <ol style="list-style-type: none"> 1. Due to violations of Azure Storage naming and sizing conventions. For more information, go to Naming conventions. 2. Because the uploaded files were modified in the cloud by other applications outside of the device. <ul style="list-style-type: none"> • {2} inside the {1} share, or • {3} inside the {4} account.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not connect to the storage account '{0}'.*	Critical	This may be because the storage account access keys have been regenerated. If the keys have been regenerated, you will need to synchronize the new keys. To fix the issue, in the Azure portal go to Shares , select the share, and refresh the storage keys.
Could not connect to the storage account '{0}'.*	Critical	This may be due to Internet connectivity issues. The device is not able to communicate with the storage account service. In the local web UI of the device, go to Troubleshooting > Diagnostic tests and click Run diagnostic tests . Resolve the reported issues.
The device has {0} files. A maximum of {1} files are supported.	Critical	Consider deleting some files from the device.
Low throughput to and from Azure Storage detected.	Warning	In the local web UI of the device, go to Troubleshooting > Diagnostic tests and click Run diagnostic tests . Resolve the reported issues. If the issue persists, contact Microsoft Support .

* This alert is triggered by more than one event type, with different recommended actions.

Security alerts

The following alerts signal access issues related to passwords, certificates, or keys, or report attempts to access an Azure Stack Edge device.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
{0} from {1} expires in {2} days.	Critical Warning	Check your certificate and upload a new certificate before the expiration date.
{0} of type {1} is not valid.	Critical	Check your certificate. If the certificate is not valid, upload a new certificate.
Internal certificate rotation failure	Critical	Couldn't rotate the internal certificates. If services are impaired, contact Microsoft Support .

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not login '{0}'. Number of failed attempts : '{1}'.	Critical Warning Informational	Make sure that you have entered the correct password. An authorized user may be attempting to connect to your device with an incorrect password. Verify that these attempts were from a legitimate source. If you continue to see failed login attempts, contact your network administrator.
Rotate SED key protector on node {0}, did not complete in time.	Warning	The attempt to rotate SED key protector to the new default has not completed in time. Please check if node and physical disks are in healthy state. System will retry again.
Device password has changed	Informational	The device administrator password has changed. This is a required action as part of the first-time device setup or regular password reset. No further action is required.
A support session is enabled.	Informational	This is an information alert to ensure that administrators can ensure that the enabling the support session is legitimate. No action is needed.
A support session has started.	Informational	This is an information alert to ensure that administrators can ensure that the support session is legitimate. No action is needed.

Key Vault alerts

The following alerts relate to your Azure Key Vault configuration.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Key Vault is not configured*	Critical Warning	<ol style="list-style-type: none"> Verify that the Key Vault is not deleted. Assign the appropriate permissions for your device to get and set the secrets. For detailed steps, see Prerequisites for an Azure Stack Edge resource. If secrets are soft deleted, follow the steps here to recover the secrets. Refresh the Key Vault details to clear the alert.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Key Vault is not configured*	Warning	Configure the Key Vault for your Azure Stack Edge resource. For detailed steps, see Create a key vault .
Key Vault is deleted	Critical	If the key vault is deleted and the purge protection duration of 90 days hasn't elapsed, follow the steps to Recover your key vault .
Couldn't retrieve secret(s) from the Key Vault	Critical	<ol style="list-style-type: none"> 1. Verify that the Key Vault is not deleted. 2. Assign the appropriate permissions for your device to get and set the secrets. The required permissions are present here. 3. Refresh the Key Vault details to clear the alert.
Couldn't access the Key Vault	Critical	<ol style="list-style-type: none"> 1. Verify that the Key Vault is not deleted. 2. Assign the appropriate permissions for your device to get and set the secrets. For more information, see the detailed steps. 3. Refresh the Key Vault details to clear the alert.

* This alert is triggered by more than one event type, with different recommended actions.

Hardware alerts

The following alerts indicate an issue with a hardware component, such as physical disk, NIC, or power supply unit, on an Azure Stack Edge device.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
{0} on {1} has failed.	Critical	<p>This is because the power supply is not connected properly or has failed. Take the following steps to resolve this issue:</p> <ol style="list-style-type: none"> 1. Make sure that the power supply connection is proper. 2. Contact Microsoft Support to order a replacement power supply unit.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not reach {1}.	Critical	<p>If the controller is turned off, restart the controller.</p> <p>Make sure that the power supply is functional. For information on monitoring the power supply LEDs, go to https://www.microsoft.com/.</p> <p>If the issue persists, contact Microsoft Support.</p>
{0} is powered off.	Warning	Connect the Power Supply Unit to a Power Distribution Unit.
One or more device components are not working properly.	Critical	Contact Microsoft Support for next steps.
Could not replace {0}.	Warning	Contact Microsoft Support for next steps.
Started the replacement of {0}.	Informational	No action is required from you.
Successfully replaced {0}	Informational	No action is required from you.
{0} is disconnected.	Warning	Verify that '{0}' is cabled properly and the network interface is up.
{0} has failed.*	Critical	The device needs to be replaced. Contact Microsoft Support to replace the device.
{0} has failed.*	Critical	<p>Verify that '{0}' is cabled properly and the network interface is up.</p> <p>In the local web UI of the device, go to Troubleshooting > Diagnostic tests and click Run diagnostic tests. Resolve the reported issues.</p> <p>If the issue persists, contact Microsoft Support at https://aka.ms/getazuresupport.</p>
Some data on the cache physical disk {0} on node {1} can't be read, preventing us from moving it onto capacity drives.	Warning	Replace the physical disk.
The cache physical disk {0} on node {1} failed some reads or writes, so to protect your data we've moved it onto capacity drives.	Warning	Replace the physical disk.
The physical disk {0} on node {1} failed to read or write multiple times in the last couple of days. If this keeps happening, it could mean that the drive is malfunctioning, damaged, or beginning to fail.	Warning	If the issue persists, consider replacing the physical disk.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
The physical disk {0} on node {1} has issues with reads or writes.	Warning	If the issue persists, consider replacing the physical disk.
The physical disk {0} on node {1} has reached 100% of its rated write endurance and is now read-only, meaning it cannot perform any more writes.	Warning	Consider replacing the physical disk.
The physical disk {0} on node {1} has failed.	Warning	Replace the physical disk.
The physical disk {0} on node {1} has issues.*	Warning	<p>The physical disk has encountered multiple bad blocks during writes in the last couple of days. This could mean that the drive is malfunctioning, damaged, or beginning to fail.</p> <p>If the issue persists, consider replacing the physical disk.</p>
The physical disk {0} on node {1} has issues.*	Warning	<p>The physical disk {0} on node {1} encountered multiple bad blocks during writes in the last couple of days. This could mean that the drive is malfunctioning, damaged, or beginning to fail.</p> <p>If the issue persists, consider replacing the physical disk.</p>
The physical disk {0} on node {1} has problems.	Warning	If the issue persists, consider replacing the physical disk.
The physical disk {0} on node {1} is wearing out. It may become read-only, meaning it cannot perform any more writes, when it reaches 100% of its rated endurance.	Warning	Consider replacing the physical disk.
The physical disk {0} on node {1} is performing slowly.	Warning	If the issue persists, consider replacing the physical disk.
There is no connectivity to the physical disk {0} on node {1}.	Warning	Make sure that the physical disk is working and is properly connected.
{0} has failed or is missing.	Critical	Your device is degraded. The device will become unhealthy if one more disk fails. Contact Microsoft Support to order a replacement disk. Replace the disk.
The physical disk {0} on node {1} could fail soon.	Warning	Replace the physical disk.
A disk replacement operation is being performed. PercentComplete = {0}, Disk = {2}.	Critical	This is an informational event. No action is required at this time.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
------------	----------	----------------------------------

The physical disk {0} on node {1} has failed.	Warning	Replace the physical disk.
The physical disk {0} on node {1} is not responding intermittently.	Warning	Replace the physical disk.
The physical disk {0} on node {1} does not have current default SED key protector set on it.	Warning	System will attempt to update the SED key protector to latest. If issue persists, check if drive is in healthy state.
The physical disk {0} on node {1} has failed rotation of SED key protector.	Warning	The attempt to rotate SED key protector to the new default has failed. Please check if physical disk is in healthy state. System will retry again, if issue persists, please replace the drive.
The physical disk {0} on node {1} has unrecognized metadata.	Critical	The disk may contain data from an unknown storage pool. Replace this disk with a Microsoft supported disk for your device that does not contain any data.
The physical disk {0} on node {1} is running an unsupported firmware version.	Warning	Contact Microsoft Support .
The physical disk {0} on node {1} is not a supported disk.	Warning	Replace the physical disk with supported hardware.
The temperature sensor on the motherboard of server {0} has raised a warning.	Warning	Check the node temperature.

* This alert is triggered by more than one event type, with different recommended actions.

Update alerts

The following alerts relate to Microsoft updates and firmware updates for physical device components.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Could not download the updates. Error message : '{0}'.	Critical	{0}
Could not install the updates. Error message : '{0}'.	Critical	Resolve the error : {0}
Could not scan for updates. Error message : '{0}'.	Critical	Resolve the error : {0}

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
{0} update(s) available.	Informational	We strongly recommend that you install these updates. For more information, refer How to install updates .
Could not update the disk firmware.	Critical	Contact Microsoft Support for next steps.
Could not update the firmware on physical disk {0} on node {1}.	Warning	Contact Microsoft Support.
Could not make progress as a firmware rollout is in progress.	Warning	Verify all storage spaces are healthy, and that no fault domain is currently in maintenance mode.
Canceled the firmware rollout due to unreadable or unexpected version information after applying the firmware update.	Warning	Restart the firmware rollout after the firmware issue is resolved.
Canceled the firmware rollout as firmware update on too many physical disks failed.	Warning	Restart the firmware rollout after the firmware issue is resolved.
Started a disk firmware update.	Informational	No action is required from you.
Successfully updated the disk firmware.	Informational	No action is required from you.
A physical disk firmware rollout is in progress. PercentComplete = {0}.	Informational	This is an informational event. No action is required at this time.

Virtual machine alerts

The following alerts are raised for virtual machines on an Azure Stack Edge device.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
The virtual machine {0} is not healthy.	Warning	To troubleshoot the virtual machine, see https://aka.ms/vmtroubleshoot .
The virtual machine {0} is not operating properly.	Warning	To troubleshoot the virtual machine, see https://aka.ms/vmtroubleshoot .
Your virtual machine {0} is not running.	Warning	If the issue persists, delete and redeploy the virtual machine.
The guest operating system in the virtual machine {0} is unhealthy.	Warning	To troubleshoot the virtual machine, see https://aka.ms/vmtroubleshoot .
Your virtual machine {0} is almost out of memory.	Warning	Reduce the memory usage on your virtual machine.

ALERT TEXT	SEVERITY	DESCRIPTION / RECOMMENDED ACTION
Your virtual machine {0} is not responding to host requests.	Warning	To troubleshoot the virtual machine, see https://aka.ms/vmtroubleshoot .

Next steps

- [Create action rules to manage alert notifications.](#)
- [Use metrics charts.](#)
- [Set up Azure Monitor.](#)

Use action rules to manage alert notifications on Azure Stack Edge devices

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to create action rules in the Azure portal to trigger or suppress alert notifications for device events that occur within a resource group, an Azure subscription, or an individual Azure Stack Edge resource.

About action rules

An action rule can trigger or suppress alert notifications. The action rule is added to an *action group* - a set of notification preferences that's used to notify users who need to act on alerts triggered in different contexts for a resource or set of resources.

For more information about action rules, see [Configuring an action rule](#). For more information about action groups, see [Create and manage action groups in the Azure portal](#).

NOTE

The action rules feature is in preview. Some screens and steps might change as the process is refined.

Create an action rule

Take the following steps in the Azure portal to create an action rule for your Azure Stack Edge device.

NOTE

These steps create an action rule that sends notifications to an action group. For details about creating an action rule to suppress notifications, see [Configuring an action rule](#).

1. Go to the Azure Stack Edge device in the [Azure portal](#), and select the **Alerts** menu item (under **Monitoring**). Then select **Action rules (preview)**.

The screenshot shows the Azure Stack Edge Alerts interface. The top navigation bar includes 'Home > myasegpu' and 'myasegpu | Alerts'. Below the navigation is a search bar and a toolbar with 'Create', 'Alert rules', 'Action groups', 'Action rules (preview)' (which is highlighted with a red box), 'Refresh', and 'Feedback'. The main content area displays subscription information: 'Subscription : mySubscription', 'Resource group : myasegpurg', 'Time range : Past 24 hours', and 'Resource : myase2109'. It shows 'Total alerts' (7), 'Smart groups (preview)' (0), and 'Total alert rules' (0). A table below lists alert severity counts: 0 Critical, 0 Error, 7 Warning, 0 Informational, and 0 Verbose. The left sidebar contains sections for Edge services (Virtual machines, IoT Edge, Cloud storage gateway), Monitoring (Device events, Alerts - highlighted with a red box), Automation (Tasks (preview)), and Support + troubleshooting (New Support Request).

2. In the Action rules (preview), select + Create.

The screenshot shows the 'Action rules (preview)' page. The top navigation bar includes 'Home > myasegpu' and 'Action rules (preview)'. Below the navigation is a toolbar with '+ Create' (highlighted with a red box), 'Columns', 'Refresh', 'Delete', 'Enable', 'Disable', and 'Feedback'. The main content area displays subscription information: 'Subscription : mySubscription', 'Resource group : myasegpurg', 'Resource type : All', and 'Resource : All'.

3. On the **Create action rule** screen, create a **Scope** to select an Azure subscription, resource group, or target resource. The action rule will act on all alerts generated within that scope.

a. Select **Edit** beside Scope to open the **Select scope** panel.

The screenshot shows the 'Create action rule' screen. On the left, there's a note: 'An action rule allows you to set granular control of notifications and suppression.' Below it are 'Scope' (selected), 'Filter', and 'Define on this scope'. The 'Scope' section shows 'myasegpurg' and 'mySubscription' with an 'Edit' button (highlighted with a red box). To the right is the 'Select Scope' panel, which has a 'Filter by subscription *' dropdown set to 'mySubscription' and a 'Search to filter items...' input field. The 'Resource' section lists resources under 'Edge Gateway Test': '-contoso-uswest-rg', '-contoso-uswest-01', and '-contoso-uswest-02'. There's also a note at the bottom: 'No filter is applied. This rule will run for all alerts on selected scope.'

b. On the **Select Scope** panel, select the **Subscription** for the action rule, and optionally filter by a **Resource type**. To filter to Azure Stack Edge resources, select **Data Box Edge devices (dataBoxEdge)**.

Select Scope

Filter by subscription * ⓘ mySubscription Filter by resource type ⓘ Data Box Edge devices (dataBoxEdg...)

Search to filter items...

Resource	Resource Type
Edge Gateway Test	Subscription
contoso-uswest-rg	Resource group
contoso-uswest-01	Azure Stack Edge
contoso-uswest-02	Azure Stack Edge
contoso-uswest-03	Azure Stack Edge
contoso-uswest-04	Azure Stack Edge

Selection preview

Done

The **Resource** area lists the available resources based on your selections.

- c. Select the check box by each resource you want to apply the rule to. You can select the subscription, resource groups, or individual resources.
- d. When you finish, select **Done**.

Filter by subscription * ⓘ mySubscription Filter by resource type ⓘ Data Box Edge devices (dataBoxEdg...)

Search to filter items...

Resource	Resource Type
<input checked="" type="checkbox"/> contoso-uswest-rg	Resource group
<input type="checkbox"/> contoso-uswest-01	Azure Stack Edge
<input type="checkbox"/> contoso-uswest-02	Azure Stack Edge
<input type="checkbox"/> contoso-uswest-03	Azure Stack Edge
<input type="checkbox"/> contoso-uswest-04	Azure Stack Edge

Selection preview

3 Selected
mySubscription -contoso-uswest-rg

Done

The **Create action rule** screen shows the selected scope.

Home > myasegpu > Action rules (preview) >

Create action rule

An action rule allows you to set granular control of notifications and suppression. [Learn more](#)

Scope contoso-uswest-rg mySubscription -contoso-uswest-rg [Edit](#)

Filter No filter is applied. This rule will run for all alerts on selected scope. [Add](#)

Define on this scope Suppression Action group

Action rule name

Description

Save action rule in resource group contoso-uswest-rg [Edit](#)

Enable rule upon creation Yes No

[Create](#)

4. Use **Filter** options to narrow the application of the rule to a subset of alerts within the selected scope.

- Select **Add** to open the **Add filters** pane.

Home > myasegpu > Action rules (preview) >

Create action rule

An action rule allows you to set granular control of notifications and suppression. [Learn more](#)

Scope contoso-uswest-rg mySubscription -contoso-uswest-rg [Edit](#)

Filter No filter is applied. This rule will run for all alerts on selected scope. [Add](#)

Define on this scope Suppression Action group

- On the **Add filters** pane, under **Filters**, add each filter you want to apply. For each filter, select the filter type, **Operator**, and **Value**.

For a list of filter options, see [Filter criteria](#).

The sample filters below apply to all alerts at Severity levels 2, 3, and 4 that the Monitor service raises for Azure Stack Edge resources.

Add filters

Filter alerts on selected scope using these criteria. [Learn more](#)

Filters	Operator	Value
Resource type	Equals	Data Box Edge devices (dataBoxEdgeDevices) Delete
Severity (1)	Equals	Sev2, Sev3, Sev4 Delete
Monitor service	Equals	Azure Stack Edge Delete
Add filter		

Filter preview

Severity equals any of 'Sev2, Sev3, Sev4' and Monitor service equals 'Azure Stack Edge' and Resource type equals 'Data Box Edge devices (dataBoxEdgeDevices)'

Done Cancel Clear

- c. When you finish adding filters, select **Done**.
5. On the **Create action rule** screen, select **Action group** to create a rule that sends notifications. Then, by **Actions**, choose **Select**.

Home > myasequpu > Action rules (preview) >

Create action rule ... X

An action rule allows you to set granular control of notifications and suppression. [Learn more](#)

Scope (1)	contoso-uswest-rg Edit
Filter (1)	Severity equals any of 'Sev2, Sev3, Sev4' and Monitor service equals 'Azure Stack Edge' a... Edit
Define on this scope * (1)	<input type="radio"/> Suppression <input checked="" type="radio"/> Action group
Actions (1)	No action group selected Select
Action rule name *	<input type="text"/>
Description	<input type="text"/>
Save action rule in resource group *	abbharGATestPass Select
Create	

NOTE

To create a rule that suppresses notifications, you would choose **Suppression**. For more information, see [Configuring an action rule](#).

6. On the **Add action groups** screen, select the action group to use with this action rule. Then choose **Select**. Your new action rule will be added to the notification preferences of the action group.

If you need to create a new action group, select + **Create action group**, and follow the steps in [Create an action group by using the Azure portal](#).

Add action groups

Select up to five action groups to attach to this alert rule.

+ Create action group

Subscription ⓘ

mySubscription

ⓘ You can select one action group per alert processing rule.

Search

Action group name	Resource group	Contain actions
<input checked="" type="checkbox"/> sendmail	contoso-uswest-rg	1 Email ⓘ
<input type="checkbox"/> Application Insights Smart Detection	DataBoxBotResourceGroup	2 Email Azure Resource Manager Roles ⓘ
<input type="checkbox"/> ExceptionActionGroup	databoxbotresourcegroup	1 Email, 1 Azure app ⓘ
<input type="checkbox"/> Application Insights Smart Detection	DataBoxPPEResourceGroup	2 Email Azure Resource Manager Roles ⓘ
<input type="checkbox"/> Migration_AG1	DataBoxPPEResourceGroup	
<input type="checkbox"/> Migration_AG2	DataBoxPPEResourceGroup	2 Email Azure Resource Manager Roles ⓘ

Select

- Give the new action rule a **Name** and **Description** (optional), and assign the rule to a resource group.
- The new rule will be enabled by default. If you don't want to start using the rule immediately, select **No** for **Enable rule update creation**.
- When you finish your settings, select **Create**.

Home > myaseqpu > Action rules (preview) >

Create action rule

Scope ⓘ contoso-uswest-rg mySubscription > [] -contoso-uswest-rg Edit

Filter ⓘ Severity equals any of 'Sev2, Sev3, Sev4' and Monitor service equals 'Azure Stack Edge' a... Edit

Define on this scope * ⓘ Suppression Action group

Actions sendSMS 2 Emails, 2 SMS messages Select

Action rule name * contoso-actionrule1

Description Alert notifications, Sev2 - Sev4, Azure Stack Edge resources, contoso-uswest-rg

Save action rule in resource group * contoso-uswest-rg

Enable rule upon creation Yes No

Create

The **Action rules (Preview)** screen opens, but you might not see your new action rule immediately. The focus is **All** resource groups.

- To see your new action rule, select the resource group for the rule.

Subscription : mySubscription Resource group : **contoso-uswest-rg** Resource : All Status : Enabled Contains : All Action groups : All

Action rule name ↑	Scope	Filter	Contains	Action rule status
<input checked="" type="checkbox"/> contoso-actionrule1	mySubscription	For alerts with Severity equals 'Sev4'	Action groups: myaseactgrp1	Enabled
<input type="checkbox"/> Supress Action	mySubscription		Action groups: suppress action group	Enabled

View notifications

Notifications go out when a new event triggers an alert for a resource that's within the scope of an action rule.

The action group for a rule sets who receives a notification and the type of notification that's sent - email, a Short Message Service (SMS) message, or both.

It might take a few minutes to receive notifications after an alert is triggered.

The email notification will look similar to this one.

Fired:Sev4 Azure Monitor Alert Device password has changed on contoso-databoxedge (microsoft.databoxedge/databoxedgedevices) at 1/28/2021 5:49:03 PM

[View the alert in Azure Monitor >](#)

Summary

Alert name	Device password has changed
Severity	Sev4
Monitor condition	Fired
Affected resource	contoso-databoxedge
Resource type	microsoft.databoxedge/databoxedgedevices
Resource group	contoso-uswest-rg
Subscription	Edge Gateway Test
Description	The device administrator password has changed. This is a required action as part of the first time device setup or regular password reset. No further action is required.
Monitoring service	Azure Stack Edge
Signal type	Log
Fired time	January 28, 2021 17:49 UTC
Alert ID	1234567-890a-1bcd-234e-fg56hij78

You're receiving this notification as a member of the contoso-ag01 action group. To unsubscribe from emails directed to this action group, [click here](#).

f t v in

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Next steps

- [View device alerts.](#)
- [Work with alert metrics.](#)
- [Set up Azure Monitor.](#)

Monitor your Azure Stack Edge device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R ✓ Azure Stack Edge Pro - FPGA

This article describes how to monitor your Azure Stack Edge device. To monitor your device, you can use the Azure portal or the local web UI. Use the Azure portal to view metrics, view device events, and configure and manage alerts. Use the local web UI on your physical device to view the hardware status of the various device components.

In this article, you learn how to:

- View capacity and transaction metrics for your device
- View hardware status of device components

View metrics

You can also view the metrics to monitor the performance of the device and in some instances for troubleshooting device issues.

Take the following steps in the Azure portal to create a chart for selected device metrics.

1. For your resource in the Azure portal, go to **Monitoring > Metrics** and select **Add metric**.

The screenshot shows the Azure portal Metrics blade for the resource 'contoso-edgeprod02'. The left sidebar contains navigation links for Order details, Device setup, Gateway (Get started, Users, Shares, Bandwidth), Edge compute (Get started, Modules, Triggers), Monitoring (Device events, Alerts), and Support + troubleshooting (New support request). The main area displays a chart titled 'contoso-edgeprod02 - Metrics' with a Y-axis from 0 to 100 and an X-axis showing time from 06 PM to 12 PM. A legend indicates the chart type is a Line chart. Above the chart, there are buttons for 'Add chart', 'Refresh', 'Share', and a time range selector set to 'Last 24 hours (Automatic)'. Below the chart, there are three cards: 'Filter + Split' (Apply filters and splits to identify outlying segments), 'Plot multiple metrics' (Create charts with multiple metrics and resources), and 'Build custom dashboards' (Pin charts to your dashboards). The 'Metrics' link in the sidebar is also highlighted with a red box.

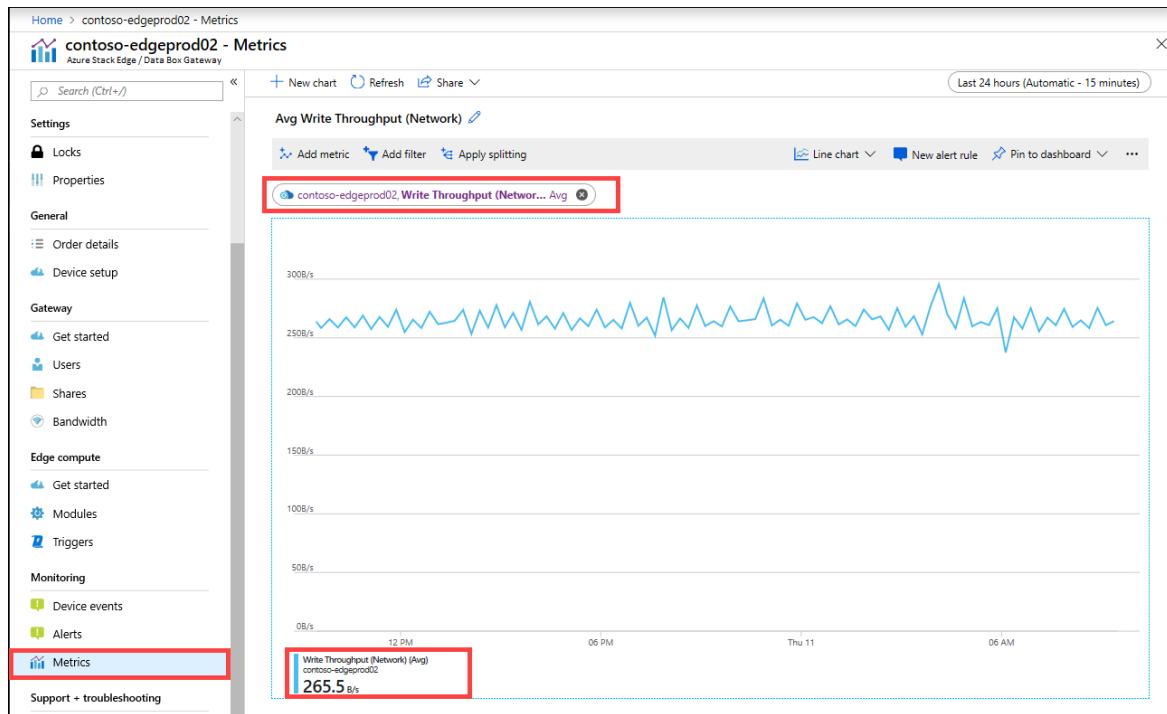
2. The resource is automatically populated.

The screenshot shows the 'contoso-edgeprod02 - Metrics' blade. On the left, a navigation menu includes 'Metrics' (which is highlighted with a red box). In the main area, there's a search bar and a chart title section. Below that is a row of filters: 'Add metric', 'Add filter', 'Apply splitting', 'Line chart' (selected), 'New alert rule', 'Pin to dashboard', and '...'. A red box highlights the 'RESOURCE' dropdown, which is set to 'contoso-edgeprod02'. To the right of it are 'METRIC NAMESPACE' (set to 'Standard metrics'), 'METRIC' (set to 'Select metric'), and 'AGGREGATION' (set to 'Select aggregation'). Below these controls is a line chart showing data from 10 to 100. At the bottom of the chart area, there are three cards: 'Filter + Split', 'Plot multiple metrics', and 'Build custom dashboards'. The 'Metrics' link in the left sidebar is also highlighted with a red box.

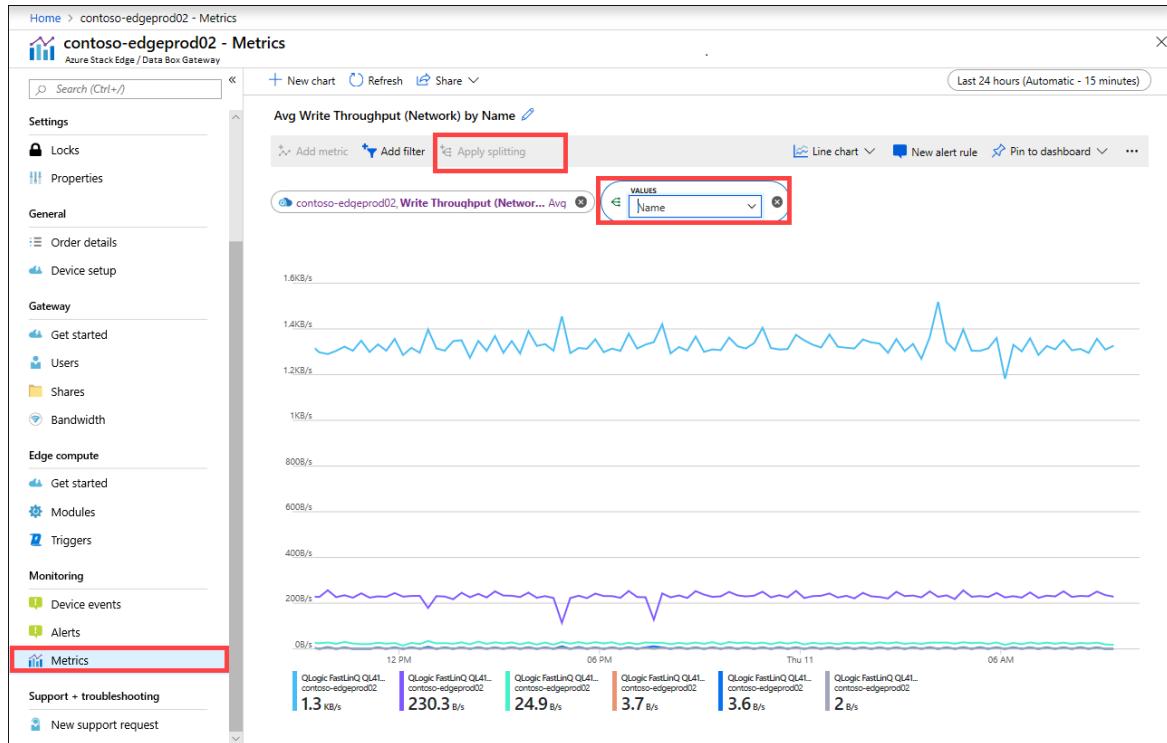
To specify another resource, select the resource. On **Select a resource** blade, select the subscription, resource group, resource type, and the specific resource for which you want to show the metrics and select **Apply**.

The screenshot shows the 'Select a resource' blade. It has tabs for 'Browse' and 'Recent'. Under 'Subscriptions', it says 'All 16 selected – Don't see a subscription? Open Directory + Subscription settings'. It shows dropdowns for 'Subscription' (set to 'All subscriptions'), 'Resource group' (set to '2 resource groups'), and 'Resource type' (set to 'Azure Stack Edge / Data Box Gateway'). A red box highlights the 'RESOURCE' dropdown in the main metrics blade. In the 'Select a resource' blade, a red box highlights the 'contoso-edgeprod01' entry in the list, which is associated with 'ContosoRG'. At the bottom are 'Apply' and 'Cancel' buttons.

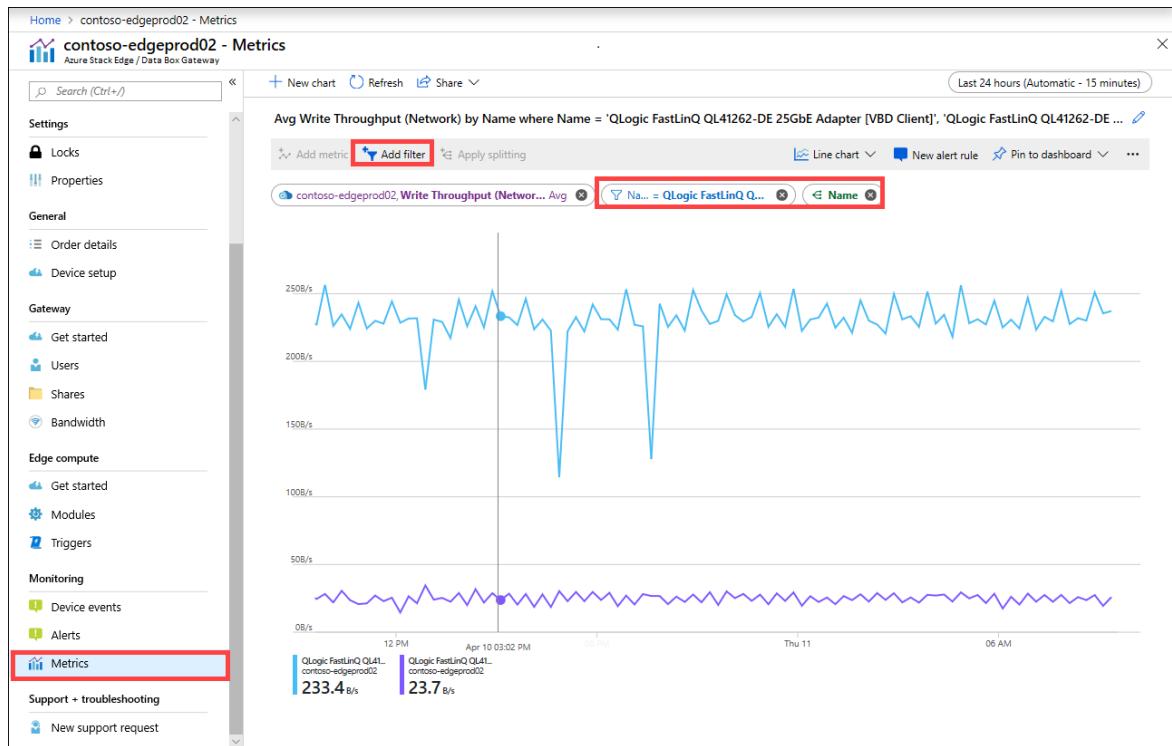
3. From the dropdown list, select a metric to monitor your device. For a full list of these metrics, see [Metrics on your device](#).
4. When a metric is selected from the dropdown list, aggregation can also be defined. Aggregation refers to the actual value aggregated over a specified span of time. The aggregated values can be average, minimum, or the maximum value. Select the Aggregation from Avg, Max, or Min.



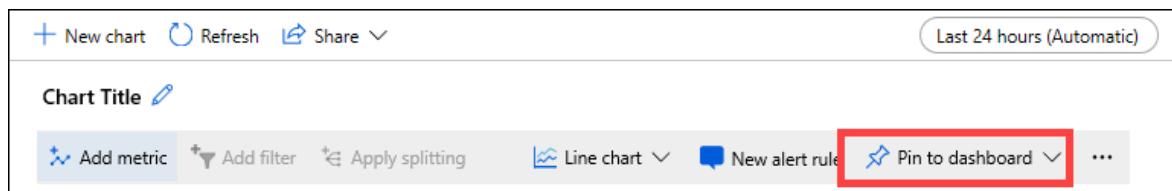
- If the metric you selected has multiple instances, then the splitting option is available. Select **Apply splitting** and then select the value by which you want to see the breakdown.



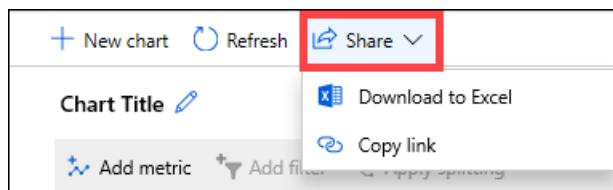
- If you now want to see the breakdown only for a few instances, you can filter the data. For example, in this case, if you want to see the network throughput only for the two connected network interfaces on your device, you could filter those interfaces. Select **Add filter** and specify the network interface name for filtering.



7. You could also pin the chart to dashboard for easy access.



8. To export chart data to an Excel spreadsheet or get a link to the chart that you can share, select the share option from the command bar.



Metrics on your device

This section describes the monitoring metrics on your device. The metrics can be:

- Capacity metrics. The capacity metrics are related to the capacity of the device.
- Transaction metrics. The transaction metrics are related to the read and write operations to Azure Storage.
- Edge compute metrics. The Edge compute metrics are related to the usage of the Edge compute on your device.

A full list of the metrics is shown in the following table:

CAPACITY METRICS	DESCRIPTION
------------------	-------------

CAPACITY METRICS	DESCRIPTION
Available capacity	<p>Refers to the size of the data that can be written to the device. In other words, this metric is the capacity that can be made available on the device.</p> <p>You can free up the device capacity by deleting the local copy of files that have a copy on both the device and the cloud.</p>
Total capacity	<p>Refers to the total bytes on the device to write data to, which is also referred to as the total size of the local cache.</p> <p>You can now increase the capacity of an existing virtual device by adding a data disk. Add a data disk through the hypervisor management for the VM and then restart your VM. The local storage pool of the Gateway device will expand to accommodate the newly added data disk.</p> <p>For more information, go to Add a hard drive for Hyper-V virtual machine.</p>
TRANSACTION METRICS	DESCRIPTION
Cloud bytes uploaded (device)	Sum of all the bytes uploaded across all the shares on your device
Cloud bytes uploaded (share)	<p>Bytes uploaded per share. This metric can be:</p> <p>Avg, which is the (Sum of all the bytes uploaded per share / Number of shares),</p> <p>Max, which is the maximum number of bytes uploaded from a share</p> <p>Min, which is the minimum number of bytes uploaded from a share</p>
Cloud download throughput (share)	<p>Bytes downloaded per share. This metric can be:</p> <p>Avg, which is the (Sum of all bytes read or downloaded to a share / Number of shares)</p> <p>Max, which is the maximum number of bytes downloaded from a share</p> <p>and Min, which is the minimum number of bytes downloaded from a share</p>
Cloud read throughput	Sum of all the bytes read from the cloud across all the shares on your device
Cloud upload throughput	Sum of all the bytes written to the cloud across all the shares on your device
Cloud upload throughput (share)	Sum of all bytes written to the cloud from a share / # of shares is average, max, and min per share

TRANSACTION METRICS	DESCRIPTION
Read throughput (network)	<p>Includes the system network throughput for all the bytes read from the cloud. This view can include data that is not restricted to shares.</p> <p>Splitting will show the traffic over all the network adapters on the device, including adapters that are not connected or enabled.</p>
Write throughput (network)	<p>Includes the system network throughput for all the bytes written to the cloud. This view can include data that is not restricted to shares.</p> <p>Splitting will show the traffic over all the network adapters on the device, including adapters that are not connected or enabled.</p>
EDGE COMPUTE METRICS	DESCRIPTION
Edge compute - memory usage	
Edge compute - percentage CPU	

View device events

Take the following steps in the Azure portal to view a device event.

1. In the Azure portal, go to your Azure Stack Edge / Data Box Gateway resource and then go to **Monitoring > Device events**.
2. Select an event and view the alert details. Take appropriate action to resolve the alert condition.

The screenshot shows the Azure portal interface for a device named 'MyDataBoxGW1'. On the left, the 'Device events' section is highlighted with a red box. A specific event, 'Lost heartbeat from your device.', is selected and also highlighted with a red box. To the right, an 'Alert details' modal is open, also with a red box around its content area. The modal displays the message 'Lost heartbeat from your device.' and a recommendation: 'If your device is offline, then the device is not able to communicate with the Azure service. This could be due to one of the following reasons: 1. The internet connectivity is broken. Check your internet connection. In the local web UI of the device, go to Troubleshooting > Diagnostic tests. Run the diagnostic tests. Resolve the reported issues. 2. The device is turned off or paused on the hypervisor. Turn on your device. For more information, go to Turn on your device. 3. Your device could have rebooted due to an update. Wait a few minutes and try to reconnect.' Below the modal, the 'Additional information' section shows 'Occurrences: 1'.

View hardware status

Take the following steps in the local web UI to view the hardware status of your device components.

1. Connect to the local web UI of your device.
2. Go to **Maintenance > Hardware status**. You can view the health of the various device components.

The screenshot shows the Azure Stack Edge management interface. On the left, there's a navigation sidebar with sections for Configuration (Device name, Network settings, Web proxy settings, Time settings, Cloud settings, Compute settings) and Maintenance (Power settings, Hardware status, Software update, Password change). The 'Hardware status' option is selected and highlighted with a red box. The main content area is titled 'Hardware status' and displays a table of device components and their statuses. All components listed are marked as 'Healthy'.

COMPONENT	STATUS
Power Supply 1	Healthy
Power Supply 2	Healthy
Processor 0	Healthy
Processor 1	Healthy
Physical Memory 1	Healthy
Physical Memory 2	Healthy
Physical Memory 13	Healthy
Physical Memory 14	Healthy
Disk 2	Healthy
Disk 3	Healthy

Next steps

- Learn how to [Manage bandwidth](#).
- Learn how to [Manage alert notifications](#).

Use Kubernetes dashboard to monitor your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to access and use the Kubernetes dashboard to monitor your Azure Stack Edge Pro GPU device. To monitor your device, you can use charts in Azure portal, view the Kubernetes dashboard, or run `kubectl` commands via the PowerShell interface of the device.

This article focuses only on the monitoring tasks that can be performed on the Kubernetes dashboard.

In this article, you learn how to:

- Access the Kubernetes dashboard on your device
- View modules deployed on your device
- Get IP address for applications deployed on your device
- View container logs for modules deployed on your device

About Kubernetes Dashboard

Kubernetes Dashboard is a web-based user interface that you can use to troubleshoot your containerized applications. Kubernetes Dashboard is a UI-based alternative to the Kubernetes `kubectl` command line. For more information, see [Kubernetes Dashboard](#).

On your Azure Stack Edge Pro device, you can use the Kubernetes Dashboard in *read-only* mode to get an overview of the applications running on your Azure Stack Edge Pro device, view status of Kubernetes cluster resources, and see any errors that have occurred on the device.

Access dashboard

The Kubernetes Dashboard is *read-only* and runs on the Kubernetes master node at port 31000. Follow these steps to access the dashboard:

1. In the local UI of your device, go to **Device** and then go to **Device endpoints**.
2. Copy the **Kubernetes dashboard** endpoint. Create a DNS entry into the `C:\Windows\System32\Drivers\etc\hosts` file of your client to connect to the Kubernetes dashboard.
`<IP address of the Kubernetes dashboard> <Kubernetes dashboard endpoint suffix>`

```

hosts - Notepad
File Edit Format View Help
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com          # source server
#      38.25.63.10        x.acme.com            # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1        localhost
#      ::1              localhost

192.168.167.192 kubernetes-dashboard.dbe-1d8phq2.microsoftdatabox.com

```

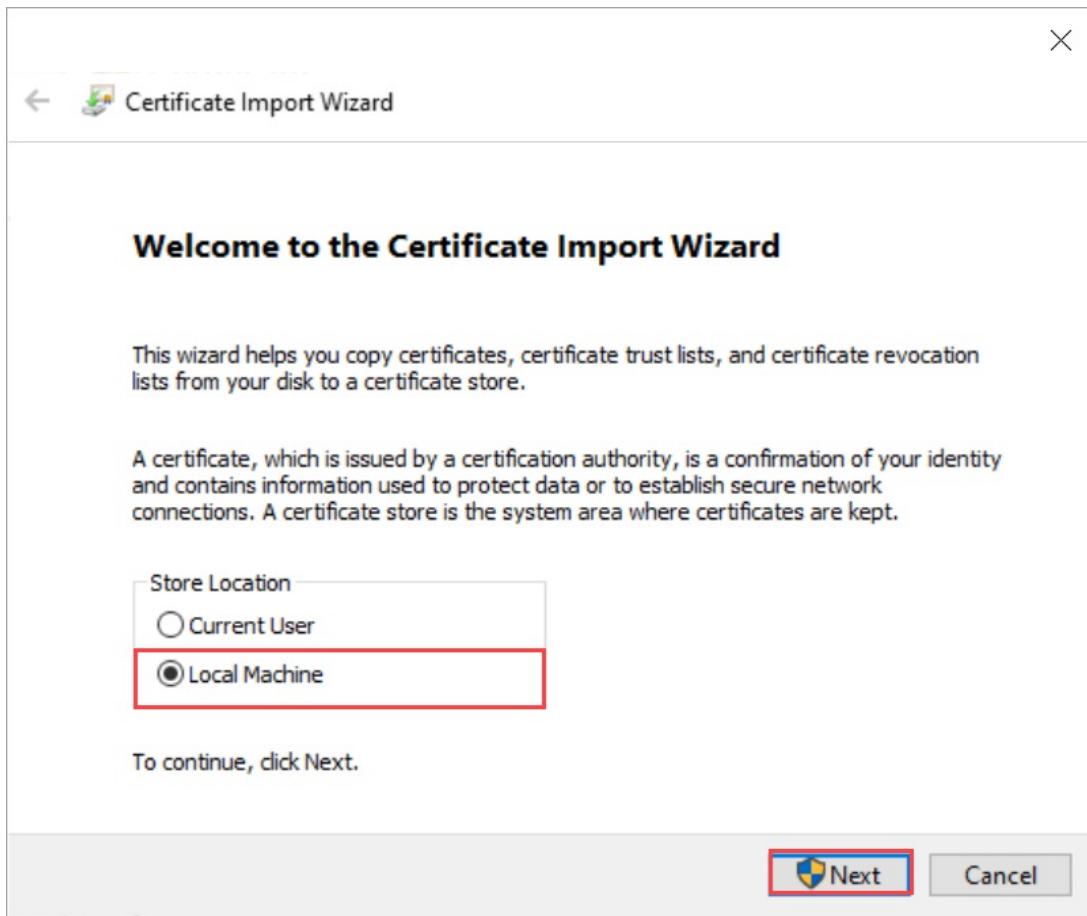
Ln 24, Col 77 100% Windows (CRLF) UTF-8 with BOM

3. In the row for the **Kubernetes dashboard** endpoint, select **Download config**. This action downloads a `kubeconfig` that allows you to access the dashboard. Save the `config.json` file on your local system.
4. Download the Kubernetes dashboard certificate from Local UI.
 - a. In the local UI of the device, go to **Certificates**.
 - b. Locate the entry for **Kubernetes dashboard endpoint certificate**. To the right of this entry, select the **Download** to download the certificate on your client system that you'll use to access the dashboard.

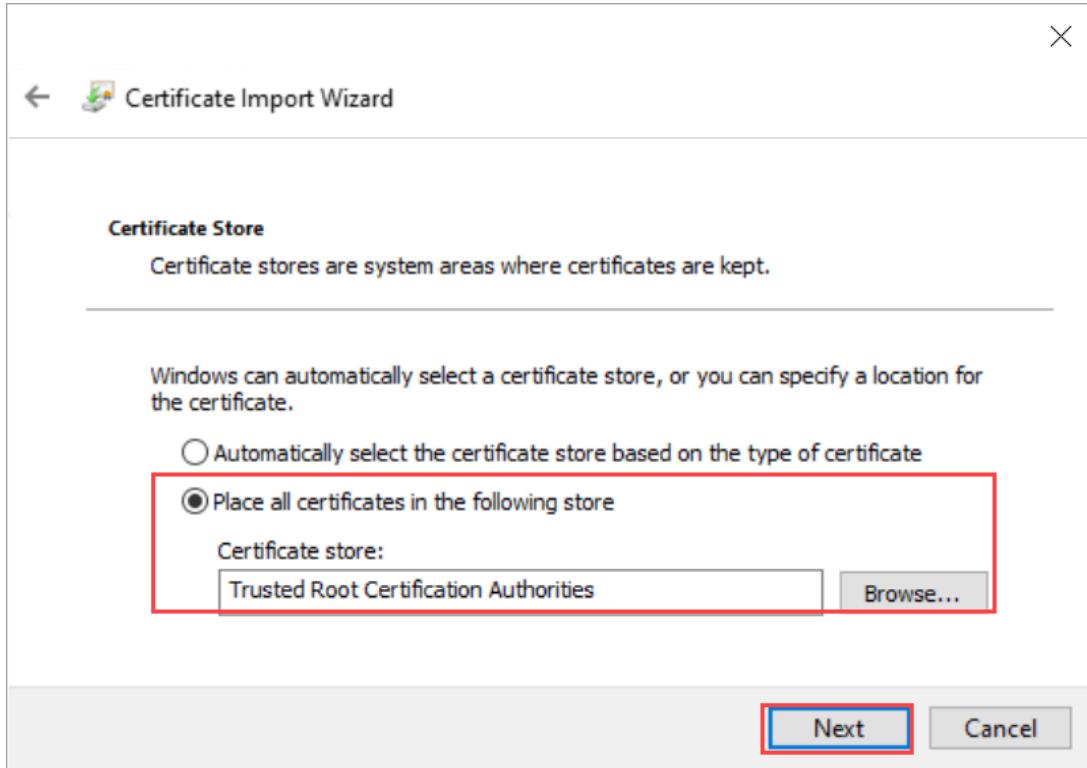
The screenshot shows the Azure Stack Edge Pro (1 GPU) Local UI with the 'Certificates' page selected. The left sidebar has a red box around the 'Certificates' link under the 'CONFIGURATION' section. The main area displays a table of certificates:

Name	Status	Expiration date	Thumbprint	Download
Node (1D8PHQ2)	Valid	8/26/2023	4E72AF4F7E791DC2B306D45AEB9B900E86A117F0	Download
Azure Resource Manager	Valid	8/26/2023	676FE35F442736828EF3B8BC8B74F0510C52EDA3	Download
Blob storage	Valid	8/26/2023	28D656692D3109D42BAD1A7709F3F77B58CD97B2	Download
Local web UI	Valid	8/26/2023	28D656692D3109D42BAD1A7709F3F77B58CD97B2	Download
IoT device root CA	Valid	8/26/2023	5190B3E0A9DB006477621F133EAE299D835634E	Download
IoT device CA	Valid	8/26/2023	A22AE53B7D5AE00D5854E6BA3B4B8CD9821A6241	-
IoT device Key	Valid	-	2658BBB447A1F1E335BF9CA1423AB08E3C826AE33D3996ACAD412...	-
Kubernetes dashboard certificate	Valid	8/26/2023	E1135A1C06E115F10D819A6C8CD9887661A8ED4A	Download
Kubernetes dashboard key	Valid	-	976E9BCBC781453BC84775B6A74099B5CA8F7D3DBEE3CE1A15361E...	-
Edge container registry certificate	Not present	-	-	-
Edge container registry key	Not present	-	-	-

5. Install the downloaded certificate on the client. If using a Windows client, follow these steps:
 - a. Select the certificate and in the **Certificate Import Wizard**, select store location as **Local machine**.



- b. Install the certificate on your Local machine in the trusted root store.



6. Copy and use the Kubernetes dashboard URL to open the dashboard in a browser. On the **Kubernetes Dashboard sign in** page:
- Select `kubeconfig`.
 - Select the ellipsis Browse and point to the `kubeconfig` that you downloaded earlier on your local system. Select **Sign in**.

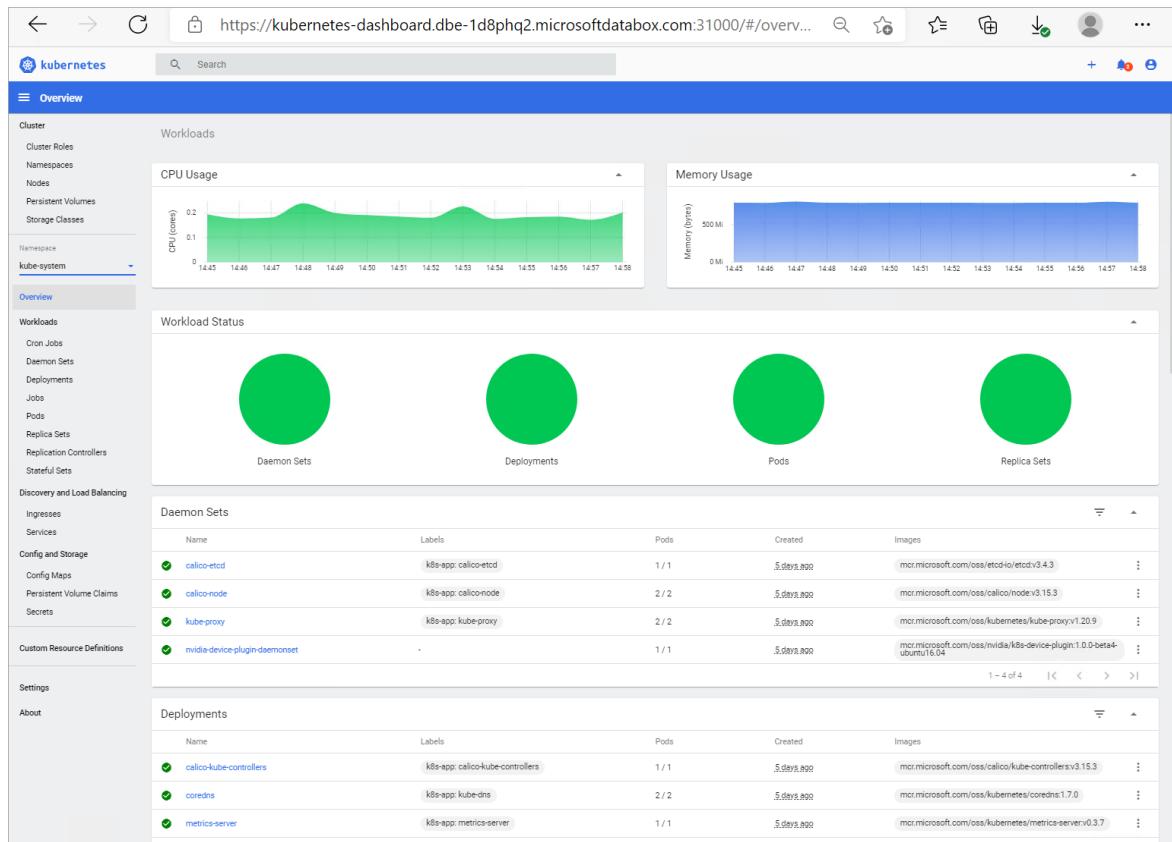
7. You can now view the Kubernetes Dashboard for your Azure Stack Edge Pro device in read-only mode.

View module status

Compute modules are containers that have a business logic implemented. You can use the dashboard to verify if a compute module has deployed successfully on your Azure Stack Edge Pro device.

To view the module status, follow these steps on the dashboard:

1. In the left-pane of the dashboard, go to **Namespace**. Filter by the namespace where IoT Edge modules are displayed, in this case, **iotedge**.
2. In the left-pane, go to **Workloads > Deployments**.
3. In the right-pane, you will see all the modules deployed on your device. In this case, a **GettingStartedWithGPU** module was deployed on the Azure Stack Edge Pro. You can see that the module was deployed.



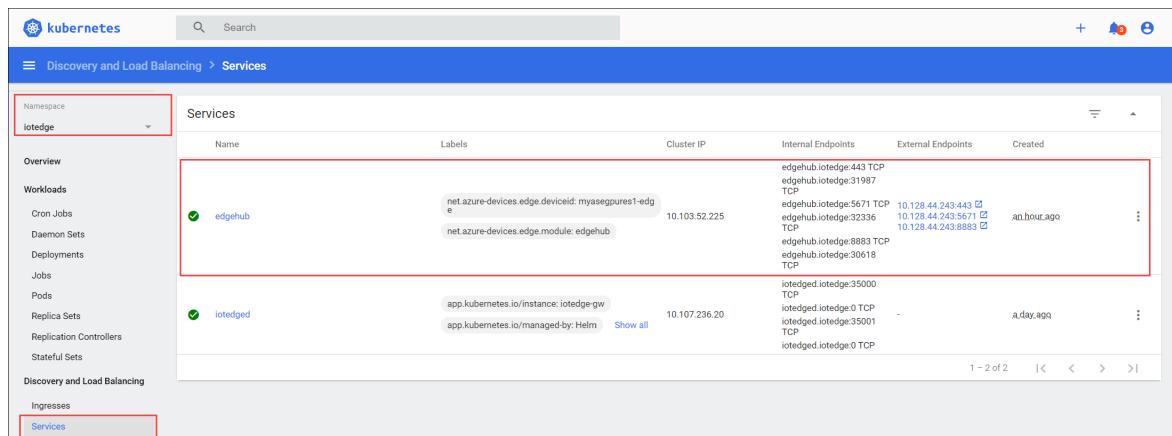
Get IP address for services or modules

You can use the dashboard to get the IP addresses of the services or modules that you want to expose outside of the Kubernetes cluster.

You assign the IP range for these external services via the local web UI of the device in the **Compute network settings** page. After you have deployed IoT Edge modules, you may want to get the IP address assigned to a specific module or service.

To get the IP address, follow these steps on the dashboard:

1. In the left-pane of the dashboard, go to **Namespace**. Filter by the namespace where an external service is deployed, in this case, **iotedge**.
2. In the left-pane, go to **Discovery and Load balancing > Services**.
3. In the right-pane, you will see all the services that are running in the **iotedge** namespace on your Azure Stack Edge Pro device.

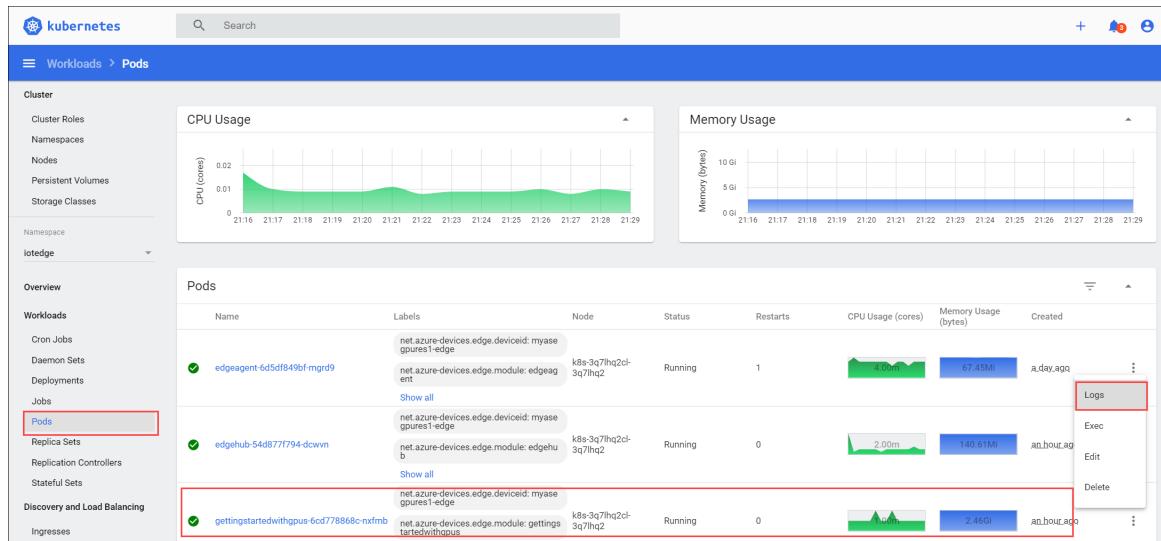


View container logs

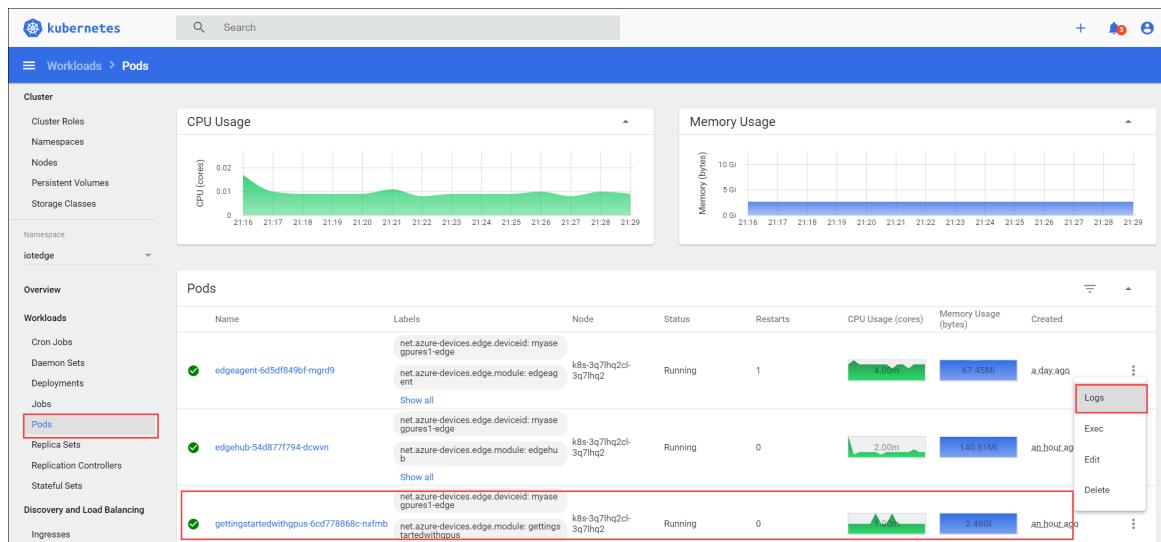
There are instances where you need to view the container logs. You can use the dashboard to get logs for a specific container that you have deployed on your Kubernetes cluster.

To view the container logs, follow these steps on the dashboard:

1. In the left-pane of the dashboard, go to **Namespace**. Filter by the namespace where the IoT Edge modules are deployed, in this case, **iotedge**.
2. In the left-pane, go to **Workloads > Pods**.
3. In the right-pane, you will see all the pods running on your device. Identify the pod that is running the module for which you want to view the logs. Select the vertical ellipsis for the pod that you identified and from the context menu, select **Logs**.



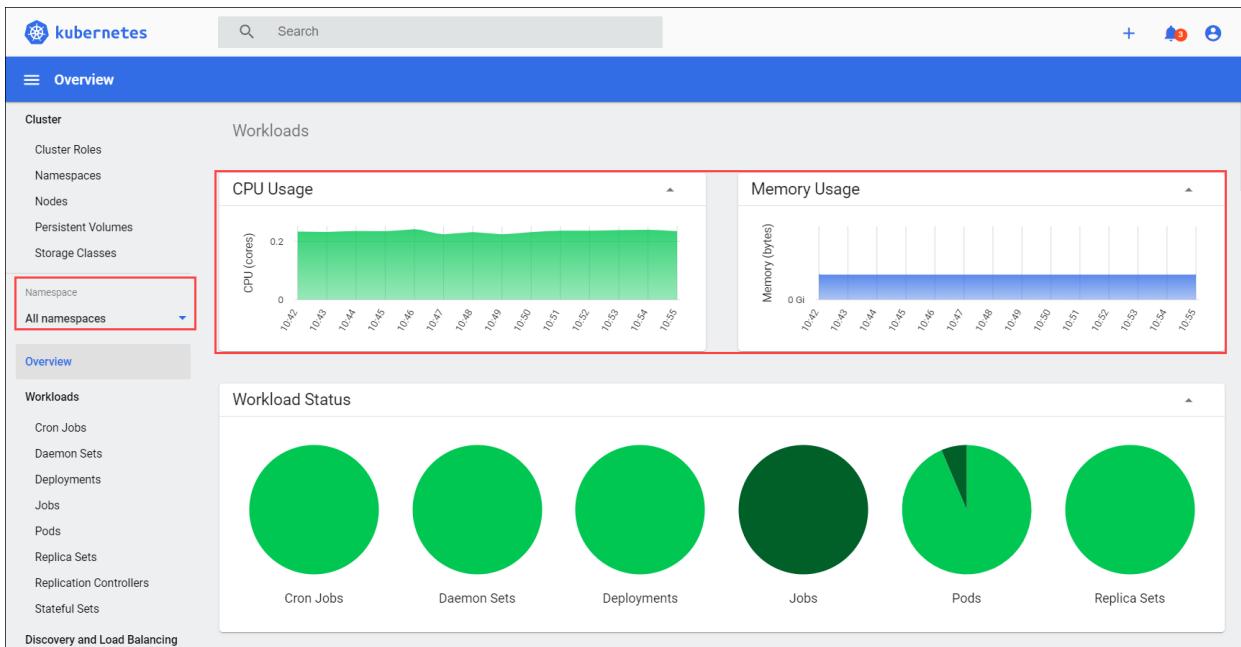
4. The logs are displayed in a logs viewer that is built into the dashboard. You can also download the logs.



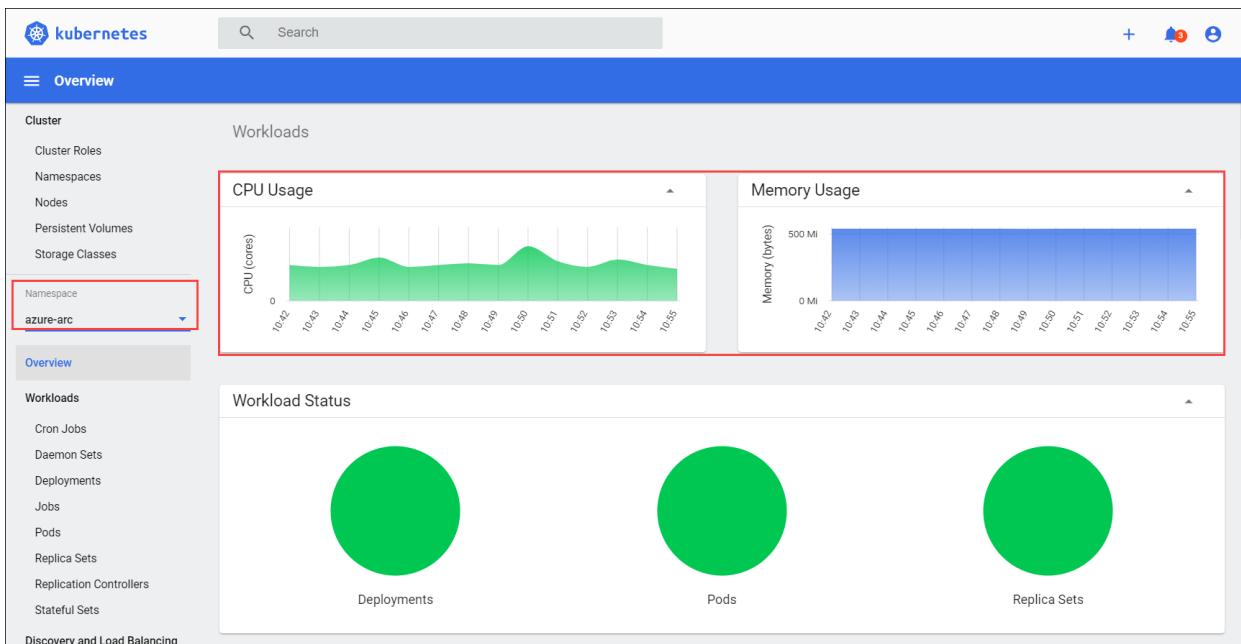
View CPU, memory usage

The Kubernetes dashboard for Azure Stack Edge Pro device also has a [Metrics server add-on](#) that aggregates the CPU and memory usage across Kubernetes resources.

For example, you can view the CPU and memory consumed across deployments in all namespaces.



You could also filter by a specific namespace. In the following example, you could view the CPU and memory consumption only for Azure Arc deployments.



The Kubernetes metrics server provides autoscaling pipelines such as [Horizontal Pod Autoscaler](#).

Next steps

Learn how to [Monitor using Azure Monitor](#). Learn how to [Run diagnostics and collect logs](#)

Enable Azure Monitor on your Azure Stack Edge Pro GPU device

9/21/2022 • 4 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Monitoring containers on your Azure Stack Edge Pro GPU device is critical, specially when you are running multiple compute applications. Azure Monitor lets you collect container logs and memory and processor metrics from the Kubernetes cluster running on your device.

This article describes the steps required to enable Azure Monitor on your device and gather container logs in Log Analytics workspace. The Azure Monitor metrics store is currently not supported with your Azure Stack Edge Pro GPU device.

NOTE

If Azure Arc is enabled on the Kubernetes cluster on your device, follow the steps in [Azure Monitor Container Insights for Azure Arc-enabled Kubernetes clusters](#) to set up container monitoring.

Prerequisites

Before you begin, you'll need:

- An Azure Stack Edge Pro device. Make sure that the device is activated as per the steps in [Tutorial: Activate your device](#).
- You've completed **Configure compute** step as per the [Tutorial: Configure compute on your Azure Stack Edge Pro device](#) on your device. Your device should have an associated IoT Hub resource, an IoT device, and an IoT Edge device.

Create Log Analytics workspace

Take the following steps to create a log analytics workspace. A log analytics workspace is a logical storage unit where the log data is collected and stored.

1. In the Azure portal, select **+ Create a resource** and search for **Log Analytics Workspace** and then select **Create**.
2. In the **Create Log Analytics workspace**, configure the following settings. Accept the remainder as default.
 - a. On the **Basics** tab, provide the subscription, resource group, name, and region for the workspace.

Create Log Analytics workspace

X

[Basics](#) [Pricing tier](#) [Tags](#) [Review + Create](#)

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) X

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

ExpressPod BVT (Creates order in BVT env)

Resource group * ⓘ

(New) myaserg

[Create new](#)

Instance details

Name * ⓘ

myaseloganalyticsws



Region * ⓘ

West US

[Review + Create](#)[« Previous](#)[Next : Pricing tier >](#)

- b. On the **Pricing tier** tab, accept the default Pay-as-you-go plan.

Create Log Analytics workspace

X

[Basics](#)[Pricing tier](#)[Tags](#)[Review + Create](#)

The cost of your workspace depends on the pricing tier and what solutions you use.
To learn more about Log Analytics pricing [click here](#)

Pricing tier

You can change to a Capacity Reservation tier after your workspace is created. [Learn more](#)
To learn more about access to legacy pricing tiers [click here](#)

Pricing tier *

Pay-as-you-go (Per GB 2018)

[Review + Create](#)[« Previous](#)[Next : Tags >](#)

- c. On the **Review + Create** tab, review the information for your workspace and select **Create**.

Create Log Analytics workspace



Validation passed

Basics Pricing tier Tags Review + Create

 Log Analytics workspace
by Microsoft

Basics

Subscription	ExpressPod BVT (Creates order in BVT env)
Resource group	myaserg
Name	myaseloganalyticsws
Region	West US

Pricing

Pricing tier	Pay-as-you-go (Per GB 2018)
--------------	-----------------------------

Tags

(none)

Create

[« Previous](#)

[Download a template for automation](#)

For more information, see the detailed steps in [Create a Log Analytics workspace via Azure portal](#).

Enable container insights

Take the following steps to enable Container Insights on your workspace.

1. Follow the detailed steps in the [How to add the Azure Monitor Containers solution](#). Use the following template file `containerSolution.json`:

```

{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "workspaceResourceId": {
            "type": "string",
            "metadata": {
                "description": "Azure Monitor Log Analytics Workspace Resource ID"
            }
        },
        "workspaceRegion": {
            "type": "string",
            "metadata": {
                "description": "Azure Monitor Log Analytics Workspace region"
            }
        }
    },
    "resources": [
        {
            "type": "Microsoft.Resources/deployments",
            "name": "[Concat('ContainerInsights', '-', uniqueString(parameters('workspaceResourceId')))]",
            "apiVersion": "2017-05-10",
            "subscriptionId": "[split(parameters('workspaceResourceId'), '/')[2]]",
            "resourceGroup": "[split(parameters('workspaceResourceId'), '/')[4]]",
            "properties": {
                "mode": "Incremental",
                "template": {
                    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
                    "contentVersion": "1.0.0.0",
                    "parameters": {},
                    "variables": {},
                    "resources": [
                        {
                            "apiVersion": "2015-11-01-preview",
                            "type": "Microsoft.OperationsManagement/solutions",
                            "location": "[parameters('workspaceRegion')]",
                            "name": "[Concat('ContainerInsights', '(', split(parameters('workspaceResourceId'), '/')[8], ')')]",
                            "properties": {
                                "workspaceResourceId": "[parameters('workspaceResourceId')]"
                            },
                            "plan": {
                                "name": "[Concat('ContainerInsights', '(', split(parameters('workspaceResourceId'), '/')[8], ')')]",
                                "product": "[Concat('OMSGallery/', 'ContainerInsights')]",
                                "promotionCode": "",
                                "publisher": "Microsoft"
                            }
                        }
                    ]
                },
                "parameters": {}
            }
        }
    ]
}

```

2. Get the resource ID and location. Go to [Your Log Analytics workspace > General > Properties](#). Copy the following information:

- **resource ID**, which is the fully qualified Azure resource ID of the Azure Log Analytics workspace.
- **location**, which is the Azure region.

3. Use the following parameters file `containerSolutionParams.json`. Replace `workspaceResourceId` with the resource ID and `workspaceRegion` with the location copied in the earlier step.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "workspaceResourceId": {
            "value": "/subscriptions/fa68082f-8ff7-4a25-95c7-ce9da541242f/resourcegroups/myaserg/providers/microsoft.operationalinsights/workspaces/myaseloganalyticsws"
        },
        "workspaceRegion": {
            "value": "westus"
        }
    }
}
```

Here is a sample output of a Log Analytics workspace with Container Insights enabled:

```

Requesting a Cloud Shell.Succeeded.
Connecting terminal...
MOTD: Switch to Bash from PowerShell: bash
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...

PS /home/myaccount> az account set -s fa68082f-8ff7-4a25-95c7-ce9da541242f
PS /home/myaccount> ls
clouddrive containerSolution.json
PS /home/myaccount> ls
clouddrive containerSolution.json containerSolutionParams.json
PS /home/myaccount> az deployment group create --resource-group myaserg --name Testdeployment1 --template-file containerSolution.json --parameters containerSolutionParams.json
{- Finished ..
  "id": "/subscriptions/fa68082f-8ff7-4a25-95c7-ce9da541242f/resourceGroups/myaserg/providers/Microsoft.Resources/deployments/Testdeployment1",
  "location": null,
  "name": "Testdeployment1",
  "properties": {
    "status": "Succeeded"
  }
}

```

```

    "properties": {
      "correlationId": "3a9045fe-2de0-428c-b17b-057508a8c575",
      "debugSetting": null,
      "dependencies": [],
      "duration": "PT11.1588316S",
      "error": null,
      "mode": "Incremental",
      "onErrorDeployment": null,
      "outputResources": [
        {
          "id": "/subscriptions/fa68082f-8ff7-4a25-95c7-ce9da541242f/resourceGroups/myaserg/providers/Microsoft.OperationsManagement/solutions/ContainerInsights(myaseloganalyticsws)",
          "resourceGroup": "myaserg"
        }
      ],
      "outputs": null,
      "parameters": {
        "workspaceRegion": {
          "type": "String",
          "value": "westus"
        },
        "workspaceResourceId": {
          "type": "String",
          "value": "/subscriptions/fa68082f-8ff7-4a25-95c7-ce9da541242f/resourcegroups/myaserg/providers/microsoft.operationalinsights/workspaces/myaseloganalyticsws"
        }
      },
      "parametersLink": null,
      "providers": [
        {
          "id": null,
          "namespace": "Microsoft.Resources",
          "registrationPolicy": null,
          "registrationState": null,
          "resourceTypes": [
            {
              "aliases": null,
              "apiProfiles": null,
              "apiVersions": null,
              "capabilities": null,
              "defaultApiVersion": null,
              "locations": [
                null
              ],
              "properties": null,
              "resourceType": "deployments"
            }
          ]
        }
      ],
      "provisioningState": "Succeeded",
      "templateHash": "10500027184662969395",
      "templateLink": null,
      "timestamp": "2020-11-06T22:09:56.908983+00:00",
      "validatedResources": null
    },
    "resourceGroup": "myaserg",
    "tags": null,
    "type": "Microsoft.Resources/deployments"
  }
}
PS /home/myaccount>

```

Configure Azure Monitor on your device

1. Go to the newly created Log Analytics Resource and copy the **Workspace ID** and **Primary key**

(workspace key).

The screenshot shows the 'Agents management' section of the Azure Log Analytics workspace. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, and Agents management (which is highlighted with a red box). The main area displays '0 Windows computers connected' and a 'Download agent' section. It shows 'Workspace ID' (703e2834-8ca8-44f7-ad28-ee1dbaa2bcff) and 'Primary key' (bvpQT3tpBXGs7aq+DT6yY+1hnxDKhr...), both of which are also highlighted with a red box. There are 'Regenerate' buttons for each. Below that is a 'Secondary key' field with its own 'Regenerate' button. Further down, there's a 'Log Analytics Gateway' section with a note about machines without internet connectivity, a link to learn more, and a download link.

Save this information as you will use it in a later step.

2. Connect to the PowerShell interface of the device.
3. Use the log analytics Workspace ID and Workspace key with the following cmdlet:

```
Set-HcsKubernetesAzureMonitorConfiguration -WorkspaceId <> -WorkspaceKey <>
```

NOTE

By default, this cmdlet configures the Azure public cloud. To configure a government cloud or non-public cloud, use the parameter `AzureCloudDomainName`.

4. After the Azure Monitor is enabled, you should see logs in the Log Analytics workspace. To view the status of the Kubernetes cluster deployed on your device, go to **Azure Monitor > Insights > Containers**. For the environment option, select **All**.

The screenshot shows the 'Containers' page in Azure Monitor. The left sidebar has options like Overview, Activity log, Alerts, Metrics, Logs, Service Health, Workbooks, and Containers (which is highlighted with a red box). The main area shows a 'Monitored clusters (6)' tab and an 'Unmonitored clusters (108)' tab. A dropdown for 'Environment' is set to 'All' (highlighted with a red box). Below is a 'Cluster Status Summary' with counts: Total 114, Critical 1 (red), Warning 1 (orange), Unknown 3 (grey), Healthy 1 (green), and Unmonitored 108. A search bar 'Search by name...' is below. A table lists monitored clusters with columns: CLUSTER NAME, CLUSTER TYPE, VERSION, STATUS, NODES, USER PODS, and SYSTEM PODS. Two clusters are shown: 'DBE-HW6H1T2.m...' (Kubernetes, non-Azure, 1.17.3, Healthy, 2/2 nodes, 16/16 user pods, 16/16 system pods) and 'KubEdgeCluster' (AKS, 1.16.9, Warning, 3/3 nodes, 34/36 user pods, 14/14 system pods).

Next steps

- Learn how to [Monitor Kubernetes workloads via the Kubernetes Dashboard](#).
- Learn how to [Manage device event alert notifications](#).

Troubleshoot your Azure Stack Edge ordering issues

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to troubleshoot Azure Stack Edge ordering issues.

Unsupported subscription or region

Error Description: In Azure portal, if you get the error:

Selected subscription or region is not supported. Choose a different subscription or region.

The screenshot shows a form with two dropdown menus. The first dropdown is labeled "1. Select a subscription * ⓘ" and contains "Azure subscription 1". The second dropdown is labeled "2. Select ship to country * ⓘ" and contains "In your hypervisor". Below the dropdowns, a red box highlights the error message: "Selected subscription or region is not supported. Choose a different subscription or region."

Suggested solution: Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#). Pay-as-you-go subscriptions aren't supported. For more information, see [Azure Stack Edge resource prerequisites](#).

There's the possibility that Microsoft may allow a subscription type upgrade on a case-by-case basis. Contact [Microsoft support](#) so that they can understand your needs and adjust these limits appropriately.

Selected subscription type not supported

Error: You have an EA, CSP, or sponsored subscription and you get the following error:

*The selected subscription type is not supported. Make sure that you use a supported subscription. [Learn more](#). If using a supported subscription type, make sure:

- That the `Microsoft.DataBoxEdge` provider is registered, when placing orders via the classic portal.
- That the `Microsoft.EdgeOrder` provider is registered, when placing orders via the Azure Edge Hardware Center (Preview).

For information on how to register, see [Register resource provider*](#).

Suggested solution: Follow these steps to register your Azure Stack Edge resource provider:

1. In Azure portal, go to **Home > Subscriptions**.
2. Select the subscription that you'll use to order your device.
3. Select **Resource providers** and then search for **Microsoft.DataBoxEdge**.

Provider	Status
microsoft.batch	Registered
Microsoft.Cdn	Registered
Microsoft.ClassicCompute	Registered
Microsoft.ClassicNetwork	Registered
Microsoft.ClassicStorage	Registered
Microsoft.ClassicInfrastructureMigrate	Registered
Microsoft.CognitiveServices	Registered
Microsoft.Commerce	Registered
Microsoft.HybridData	Registered
Microsoft.DataBox	Registered
Microsoft.DataBoxEdge	Registered
Microsoft.Databricks	Registered
Microsoft.Devices	Registered
Microsoft.DocumentDB	Registered

If you don't have owner or contributor access to register the resource provider, you see the following error: *The subscription <subscription name> doesn't have permissions to register the resource provider(s): Microsoft.DataBoxEdge.*

For more information, see [Register resource providers](#).

Resource provider not registered for subscription

Error: In Azure portal, you select a subscription to use for Azure Stack Edge or Data Box Gateway and get one of the following error:

Resource provider(s): Microsoft.DataBoxEdge are not registered for subscription <subscription name> and you don't have permissions to register a resource provider for subscription <subscription name>.

Resource provider(s): Microsoft.EdgeOrder are not registered for subscription <subscription name> and you don't have permissions to register a resource provider for subscription <subscription name>.

Suggested solution: Elevate your subscription access or find someone with owner or contributor access to register the resource provider.

Resource disallowed by policy

Error: In Azure portal, you attempt to register a resource provider and get the following error:

Resource <resource name> was disallowed by policy. (Code: RequestDisallowedByPolicy). Initiative: Deny generally unwanted Resource Types. Policy: Not allowed resource types.

Suggested solution: This error occurs due to an existing Azure Policy assignment that blocks the resource creation. Azure Policy definitions and assignments are set by an organization's system administrator to ensure compliance while using or creating Azure resources. If any such policy assignment is blocking Azure Stack Edge resource creation, contact your system administrator to edit your Azure Policy definition.

Next steps

- Learn more about how to [Troubleshoot your Azure Stack Edge issues](#).

Troubleshoot activation or secret deletion issues on Azure Key Vault for your Azure Stack Edge Pro GPU device

9/21/2022 • 5 minutes to read • [Edit Online](#)

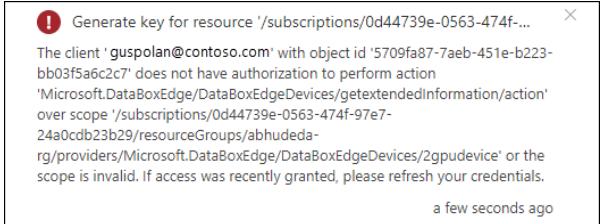
APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot activation issues on your Azure Stack Edge Pro GPU device.

Activation errors

The following table summarizes the errors related to device activation and the corresponding recommended resolution.

ERROR MESSAGE	RECOMMENDED RESOLUTION
<p>If the Azure Key Vault that's used for activation is deleted before the device is activated using the activation key, then you receive this error.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> Generate key for resource 'errorRes' ×</p><p>Message: (Http status code: 404) Can not perform requested operation on nested resource. Parent resource 'placTest2' not found.</p><p style="text-align: right;">a few seconds ago</p></div>	<p>If the key vault was deleted, you can restore the key vault if the vault is in purge-protection duration. Follow the steps in Recover a key vault.</p> <p>If the purge-protection duration has elapsed, then you'll need to create a new key vault via the Recover a key vault blade.</p>
<p>If the Azure Key Vault is deleted after the device is activated, and you then try to perform any operation that involves encryption - for example, Add User, Add Share, or Configure Compute - then you receive this error.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> Adding user 'user2' ×</p><p>Message: (Http status code: 404) Could not perform the operation on nested resource. Could not find the Azure Key Vault placetest1</p><p style="text-align: right;">a few seconds ago</p></div>	<p>If the key vault was deleted, you can restore the key vault if the vault is in purge-protection duration. Follow the steps in Recover a key vault.</p> <p>If the purge-protection duration has elapsed, then you'll need to create a new key vault as described in Recover a key vault.</p>
<p>If the activation key generation fails due to any error, then you receive this error. The notification includes more details.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> 4 Configure and activate</p><p> Could not generate the activation key. Click Retry to restart this process.</p><p style="text-align: right;">Show details</p></div>	<p>Ensure that the ports and URLs specified in Access Azure Key Vault behind a firewall are open on your firewall to enable you to access the key vault. Wait a few minutes, and retry the operation. If the problem persists, contact Microsoft Support.</p>

ERROR MESSAGE	RECOMMENDED RESOLUTION
<p>If the user has read-only permissions, then the user is not allowed to generate an activation key, and this error is presented.</p> 	<p>This could be because you don't have the right access or <code>Microsoft.KeyVault</code> is not registered.</p> <ul style="list-style-type: none"> • Make sure that you have owner or contributor access at the resource group level used for your Azure Stack Edge resource. • Make sure that the <code>Microsoft.KeyVault</code> resource provider is registered. To register a resource provider, go to the subscription used for Azure Stack Edge resource. Go to Resource providers, search for <i>Microsoft.KeyVault</i> and select and Register. For more information, see Register resource providers.

Unregistered resource provider errors

ERROR MESSAGE	RECOMMENDED RESOLUTION
<p>If the Key Vault resource provider is not registered, then you'll see an error when creating a key vault during the activation key generation.</p>	<p>The activation key won't be generated. Make sure that the <code>Microsoft.KeyVault</code> resource provider is registered. To register a resource provider, go to the subscription used for Azure Stack Edge resource. Go to Resource providers, search for <i>Microsoft.KeyVault</i> and select and Register. For more information, see Register resource providers.</p>
<p>If the Storage resource provider is not registered, then you'll see an error when creating a storage account for audit logs.</p>	<p>This error is not a blocking error and the activation key will be generated. The Storage resource provider is usually automatically registered but if it isn't, follow the steps in Register a resource provider to register <code>Microsoft.Storage</code> against your subscription.</p>

Key vault or secret deletion errors

ERROR MESSAGE	RECOMMENDED RESOLUTION
<p>If the Channel Integrity Key in the Azure Key Vault was deleted, and you try to perform any operations that involve encryption - for example, Add User, Add Share, or Configure Compute - then you will receive this error.</p>	<p>If the Channel Integrity Key in the key vault was deleted, but the key is still within the purge duration, follow the steps in Undo Key vault key removal. If the purge protection duration has elapsed, and if you've backed up the key, you can restore the key from the backup. Otherwise, you can't recover the key. Contact Microsoft Support for next steps.</p>

Audit logging errors

ERROR MESSAGE	RECOMMENDED RESOLUTION
<p>If the diagnostic setting creation fails for your key vault, you'll see this error.</p>	<p>This is not a blocking error and the activation key will be generated. You can manually Create a diagnostic setting to store your audit logs.</p>

ERROR MESSAGE	RECOMMENDED RESOLUTION
If the storage account creation fails, for example, because an account already exists for the name you specified, you'll see this error.	You can manually create a storage account and link it to the diagnostic setting on your key vault. This account is then used to store audit logs. For more information, see Create a storage account for your logs .
If the system assigned managed identity for your Azure Stack Edge resource is deleted, you'll see this error.	You'll see an alert in the Security blade for your Azure Stack Edge resource. Select this alert to Create a new managed identity through the Recover key vault blade
If the managed identity doesn't have access to the key vault, you'll see this error.	You'll see an alert in the Security blade for your Azure Stack Edge resource. Select this alert to Grant managed identity access to the key vault through the Recover key vault blade .

Resource move errors

ERROR MESSAGE	RECOMMENDED RESOLUTION
If the key vault resource is moved across resource groups or subscriptions, you'll see this error.	The key vault resource move is treated the same way as key vault deletion. You can restore the key vault if the vault is in purge-protection duration. If the purge-protection duration has elapsed, then you'll need to create a new key vault. For more information on either of the above cases, see Recover a key vault .
If the subscription you are using, is moved across tenants, you'll see this error.	Reconfigure managed identity and create a new key vault. You can also move the key vault resource in which case only the managed identity will need to be reconfigured. In each of the above cases, see Recover a key vault .
If the storage account resource that is used for audit logs, is moved across resource groups or subscriptions, you won't see an error.	You can Create a new storage account and configure it to store the audit logs .

Other errors

ERROR MESSAGE	RECOMMENDED RESOLUTION
If the network restrictions are configured for the key vault, you'll see this error.	The service can't differentiate between key vault deletion or key vault not accessible scenario due to network restrictions. In each case, you'll be directed to the Recover a key vault blade .

Next steps

- [Install Azure Stack Edge Pro with GPU](#).

Run diagnostics, collect logs to troubleshoot Azure Stack Edge device issues

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to run diagnostics, collect a Support package, gather advanced security logs, and review logs to troubleshoot device upload and refresh issues on your Azure Stack Edge device.

Run diagnostics

To diagnose and troubleshoot any device errors, you can run the diagnostics tests. Do the following steps in the local web UI of your device to run diagnostic tests.

1. In the local web UI, go to **Troubleshooting > Diagnostic tests**. Select the test you want to run and select **Run test**. You are notified that the device is running tests.

The screenshot shows the Azure Stack Edge local web interface. On the left, there's a navigation sidebar with sections like Overview, Configuration, Maintenance, and Troubleshooting. The Troubleshooting section is highlighted with a red box, and the Diagnostic tests option is selected, also highlighted with a red box. The main content area is titled "Diagnostic tests" and shows a table of available tests. The table has columns for Test, Category, Status, and Recommended actions. Most tests have a green checkmark icon next to them. A "Run test" button is at the bottom of the table. The status column for the "Azure container read/write" test is highlighted with a light blue background.

Test	Category	Status	Recommended actions
Azure portal connectivity	Azure connectivity	✓ -	-
Azure storage account credentials	Azure connectivity	✓ -	-
Azure container read/write	Azure connectivity	✓ -	-
Azure consistent services health check	Azure consistent services	✓ -	-
Certificates	Certificates	✓ -	-
Azure Edge compute runtime	Edge compute	✓ -	-
Disks	Hardware	✓ -	-
Power Supply Units	Hardware	✓ -	-
Network interfaces	Hardware	✓ -	-
CPUs	Hardware	✓ -	-
Compute acceleration	Hardware	✓ -	-
Network settings	Networking	✓ -	-
Internet connectivity	Networking	✓ -	-
System software	Software	✓ -	-
Time sync	Time	✓ -	-
Software update readiness	Update	✓ -	-

Here is a table that describes each of the diagnostics test that is run on your Azure Stack Edge device.

TEST NAME	DESCRIPTION
Azure portal connectivity	The test validates the connectivity of your Azure Stack Edge device to Azure portal.

TEST NAME	DESCRIPTION
Azure consistent health services	Several services such as Azure Resource Manager, Compute resource provider, Network resource provider, and Blob storage service run on your device. These services together provide an Azure consistent stack. The health check ensures that these Azure consistent services are up and running.
Certificates	The test validates the expiration date and the device and DNS domain change impact on certificates. The health check verified that all the certificates are imported and applied on all the device nodes.
Azure Edge Compute runtime	The test validates that the Azure Stack Edge Kubernetes service is functioning as expected. This includes checking the Kubernetes VM health as well as the status of the Kubernetes services deployed by your device.
Disks	The test validates that all the device disks are connected and functional. This includes checking that the disks have the right firmware installed and Bitlocker is configured correctly.
Power supply units (PSUs)	The test validates all the power supplies are connected and working.
Network interfaces	The test validates that all the network interfaces are connected on your device and that the network topology for that system is as expected.
Central Processing Units (CPUs)	The test validates that CPUs on the system have the right configuration and that they are up and functional.
Compute acceleration	The test validates that the compute acceleration is functioning as expected in terms of both hardware and software. Depending on the device model, the compute acceleration could be a Graphical Processing Unit (GPU) or Vision Processing Unit (VPU) or a Field Programmable Gate Array (FPGA).
Network settings	This test validates the network configuration of the device.
Internet connectivity	This test validates the internet connectivity of the device.
System software	This test validates that the system storage and software stack is functioning as expected.
Time sync	This test validates the device time settings and checks that the time server configured on the device is valid and accessible.
Software Update readiness	This test validates that the update server configured is valid and accessible.

2. After the tests have completed, the results are displayed.

The screenshot shows the Azure Stack Edge local web interface. On the left, a dark sidebar lists navigation options under four main categories: Configuration, Maintenance, and Troubleshooting. Under Troubleshooting, 'Diagnostic tests' is selected and highlighted in blue. The main content area is titled 'Diagnostic tests' and shows a table of test results for the device 'myasegpu1'. The table has columns for Test, Category, Status, and Recommended actions. All tests listed are marked as 'Healthy'. A large blue button at the bottom of the table says 'Run test'.

Test	Category	Status	Recommended actions
Azure portal connectivity	Azure connectivity	Healthy	-
Azure storage account credentials	Azure connectivity	Healthy	-
Azure container read/write	Azure connectivity	Healthy	-
Azure consistent services health check	Azure consistent services	Healthy	-
Certificates	Certificates	Healthy	-
Azure Edge compute runtime	Edge compute	Healthy	-
Disks	Hardware	Healthy	-
Power Supply Units	Hardware	Healthy	-
Network interfaces	Hardware	Healthy	-
CPUs	Hardware	Healthy	-
Compute acceleration	Hardware	Healthy	-
Network settings	Networking	Healthy	-
Internet connectivity	Networking	Healthy	-
System software	Software	Healthy	-
Time sync	Time	Healthy	-
Software update readiness	Update	Healthy	-

If a test fails, then a URL for recommended action is presented. Select the URL to view the recommended action.

Recommended actions

To resolve the issue(s), complete the following:

- RDMA performance is slower than expected. Examine your network adapters.

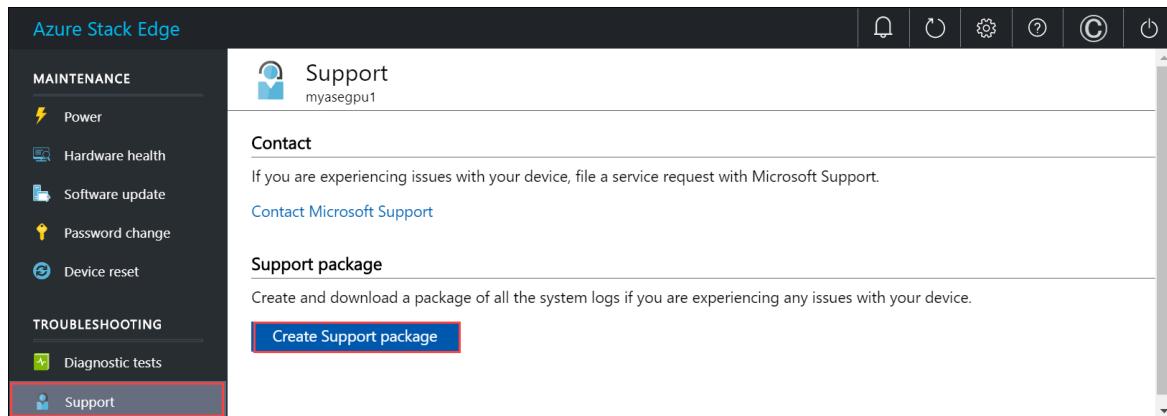
OK

Collect Support package

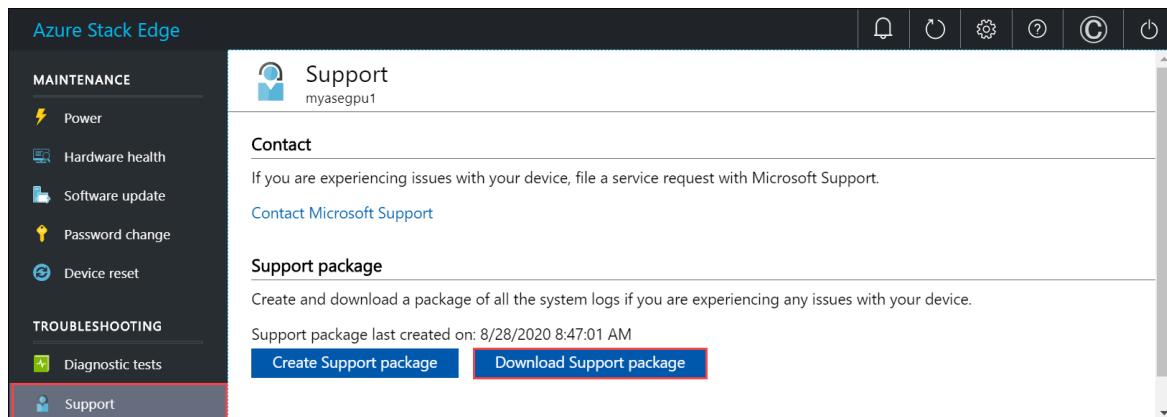
A log package is composed of all the relevant logs that can help Microsoft Support troubleshoot any device issues. You can generate a log package via the local web UI.

Do the following steps to collect a Support package.

1. In the local web UI, go to **Troubleshooting > Support**. Select **Create support package**. The system starts collecting support package. The package collection may take several minutes.



2. After the Support package is created, select **Download Support package**. A zipped package is downloaded on the path you chose. You can unzip the package and view the system log files.



Gather advanced security logs

The advanced security logs can be software or hardware intrusion logs for your Azure Stack Edge Pro device.

Software intrusion logs

The software intrusion or the default firewall logs are collected for inbound and outbound traffic.

- When the device is imaged at the factory, the default firewall logging is enabled. These logs are bundled in the support package by default when you create a support package via the local UI or via the Windows PowerShell interface of the device.
- If only the firewall logs are needed in the support package to review any software (NW) intrusion in the device, use `-Include FirewallLog` option when creating the support package.
- If no specific include option is provided, firewall log is included as a default in the support package.
- In the support package, firewall log is the `pfirewall.log` and sits in the root folder. Here is an example of the software intrusion log for the Azure Stack Edge Pro device.

```

#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin
#icmptype icmpcode info path

2019-11-06 12:35:19 DROP UDP 5.5.3.197 224.0.0.251 5353 5353 59 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e88 ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e88 ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e88 ff02::fb 5353 5353 89 - - - - -
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9d87 ff02::fb 5353 5353 79 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP 5.5.3.193 224.0.0.251 5353 5353 59 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe08:20d5 ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe08:20d5 ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e8b ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e8b ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP 5.5.3.33 224.0.0.251 5353 5353 59 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e8a ff02::fb 5353 5353 89 - - - - - RECEIVE
2019-11-06 12:35:19 DROP UDP fe80::3680:dff:fe01:9e8b ff02::fb 5353 5353 89 - - - - - RECEIVE

```

Hardware intrusion logs

To detect any hardware intrusion into the device, currently all the chassis events such as opening or close of chassis, are logged.

- The system event log from the device is read using the `racadm` cmdlet. These events are then filtered for chassis-related event in to a `HWIntrusion.txt` file.
- To get only the hardware intrusion log in the support package, use the `-Include HWselLog` option when you create the support package.
- If no specific include option is provided, the hardware intrusion log is included as a default in the support package.
- In the support package, the hardware intrusion log is the `HWIntrusion.txt` and sits in the root folder. Here is an example of the hardware intrusion log for the Azure Stack Edge Pro device.

```

09/04/2019 15:51:23 system Critical The chassis is open while the power is off.
09/04/2019 15:51:30 system Ok The chassis is closed while the power is off.

```

Troubleshoot device upload and refresh errors

Any errors experienced during the upload and refresh processes are included in the respective error files.

- To view the error files, go to your share and select the share to view the contents.
- Select the *Microsoft Data Box Edge folder*. This folder has two subfolders:

- Upload folder that has log files for upload errors.
- Refresh folder for errors during refresh.

Here is a sample log file for refresh.

```

<root container="test1" machine="VM15BS020663" timestamp="03/18/2019 00:11:10" />
<file item="test.txt" local="False" remote="True" error="16001" />
<summary runtime="00:00:00.0945320" errors="1" creates="2" deletes="0" insync="3" replaces="0"
pending="9" />

```

- When you see an error in this file (highlighted in the sample), note down the error code, in this case it is

16001. Look up the description of this error code against the following error reference.

ERROR CODE	ERROR DESCRIPTION
100	The container or share name must be between 3 and 63 characters.
101	The container or share name must consist of only letters, numbers, or hyphens.
102	The container or share name must consist of only letters, numbers, or hyphens.
103	The blob or file name contains unsupported control characters.
104	The blob or file name contains illegal characters.
105	Blob or file name contains too many segments (each segment is separated by a slash -/).
106	The blob or file name is too long.
107	One of the segments in the blob or file name is too long.
108	The file size exceeds the maximum file size for upload.
109	The blob or file is incorrectly aligned.
110	The Unicode encoded file name or blob is not valid.
111	The name or the prefix of the file or blob is a reserved name that isn't supported (for example, COM1).
2000	An etag mismatch indicates that there is a conflict between a block blob in the cloud and on the device. To resolve this conflict, delete one of those files – either the version in the cloud or the version on the device.
2001	An unexpected problem occurred while processing a file after the file was uploaded. If you see this error, and the error persists for more than 24 hours, contact support.
2002	The file is already open in another process and can't be uploaded until the handle is closed.
2003	Couldn't open the file for upload. If you see this error, contact Microsoft Support.
2004	Couldn't connect to the container to upload data to it.
2005	Couldn't connect to the container because the account permissions are either wrong or out of date. Check your access.

ERROR CODE	ERROR DESCRIPTION
2006	Couldn't upload data to the account as the account or share is disabled.
2007	Couldn't connect to the container because the account permissions are either wrong or out of date. Check your access.
2008	Couldn't add new data as the container is full. Check the Azure specifications for supported container sizes based on type. For example, Azure File only supports a maximum file size of 5 TB.
2009	Couldn't upload data because the container associated with the share doesn't exist.
2997	An unexpected error occurred. This is a transient error that will resolve itself.
2998	An unexpected error occurred. The error may resolve itself but if it persists for more than 24 hours, contact Microsoft Support.
16000	Couldn't bring down this file.
16001	Couldn't bring down this file since it already exists on your local system.
16002	Couldn't refresh this file since it isn't fully uploaded.

Next steps

- [Troubleshoot device activation issues.](#)
- [Troubleshoot Azure Resource Manager issues.](#)
- [Troubleshoot Blob storage issues.](#)
- [Troubleshoot compute issues in IoT Edge.](#)

Proactive log collection on your Azure Stack Edge device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

Proactive log collection gathers system health indicators on your Azure Stack Edge device to help you efficiently troubleshoot any device issues. Proactive log collection is enabled by default. This article describes what is logged, how Microsoft handles the data, and how to disable or enable proactive log collection.

About proactive log collection

Microsoft Customer Support and Engineering teams use system logs from your Azure Stack Edge device to efficiently identify and fix issues that might come up during operation. Proactive log collection is a method that alerts Microsoft that an issue/event has been detected by the customer's Azure Stack Edge appliance. See [Proactive log collection indicators](#) for events that are tracked. The support logs pertaining to the issue are automatically uploaded to an Azure Storage account that Microsoft manages and controls. Microsoft Support and Microsoft engineers review these support logs to determine the best course of action to resolve the issue with the customer.

NOTE

These logs are only used for debugging purposes and to provide support to the customers in case of issues.

Enabling proactive log collection

Proactive log collection is enabled by default. You can disable proactive log collection when trying to activate the device via the local UI.

1. In the local web UI of the device, go to the [Get started](#) page.
2. On the **Activation** tile, select **Activate**.

The screenshot shows the Azure Stack Edge Pro R (1 GPU) configuration interface. On the left, there's a sidebar with sections like Overview, Configuration (highlighted), Maintenance, and Power. Under Configuration, 'Get started' is selected and highlighted with a red border. The main area is titled 'Get started with standalone device setup' and shows four steps: 1. Network, 2. Device setup, 3. Security, and 4. Activation. Step 1 shows Network, Compute network, and Web proxy status. Step 2 shows Device, Update, and Time status. Step 3 shows Certificates and Encryption at rest status. Step 4 is an activation section with a 'Activate' button.

3. In the **Activate** pane:

- Enter the **Activation key** that you got in [Get the activation key for Azure Stack Edge Pro R](#).

Once activated, proactive log collection is enabled by default, allowing Microsoft to collect logs based on the health status of the device. These logs are uploaded to an Azure Storage account.

You can disable proactive log collection to stop Microsoft from collecting logs.

- If you want to disable proactive log collection on the device, select **Disable**.
- Select **Activate**.

Activate

Activate the device with Azure service. [Learn how to get the activation key](#). After the device is activated, the system checks for and applies any critical updates.

* Activation key
1abC2def3gH4jk56lmnO7pq8rs9tu01vwX==#1abcd2e3456f78 ✓

Proactive log collection

Based on proactive log collection indicators, logs are proactively uploaded to an Azure Storage account to help Microsoft Support troubleshoot issues when they arise. [Learn more](#).

[Enable](#) [Disable](#)

If you click the "Disable" button, you agree to deactivate the proactive log collection. After the proactive log collection is disabled, logs are not uploaded automatically if a proactive log collection indicator is detected.
[Learn more about Microsoft's privacy practices](#).

[Activate](#)

Proactive log collection indicators

After the proactive log collection is enabled, logs are uploaded automatically when one of the following events is detected on the device:

ALERT/ERROR/CONDITION	DESCRIPTION
AcsUnhealthyCondition	Azure Consistent Services are unhealthy.
IOTEdgeAgentNotRunningCondition	IoT Edge Agent is not running.
UpdateInstallFailedEvent	Could not install the update.

Microsoft will continue to add new events to the preceding list. No additional consent is needed for new events. Refer to this page to learn about the most up-to-date proactive log collection indicators.

Other log collection methods

Besides proactive log collection, which collects specific logs pertaining to a specific issue detected, other log collections can give a much deeper understanding of system health and behavior. Usually, these other logs can

be collected during a support request or triggered by Microsoft based on telemetry data from the device.

Handling data

When proactive log collection is enabled, the customer agrees to Microsoft collecting logs from the Azure Stack Edge device as described herein. The customer also acknowledges and consents to the upload and retention of those logs in an Azure Storage account managed and controlled by Microsoft.

Microsoft uses the data for troubleshooting system health and issues only. The data is not used for marketing, advertising, or any other commercial purposes without the customer consent.

The data Microsoft collects is handled as per our standard privacy practices. Should a customer decide to revoke its consent for proactive log collection, any data collected with consent prior to the revocation will not be affected.

Next steps

Learn how to [Gather a support package](#).

Remote support and diagnostics for Azure Stack Edge

9/21/2022 • 15 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

IMPORTANT

Remote support is in public preview and applies to Azure Stack Edge version 2110 or later.

On your Azure Stack Edge device, you can enable remote support to allow Microsoft Engineers to diagnose and remediate issues by accessing your device remotely. When you enable this feature, you provide consent for the level of access and the duration of access.

This article describes the remote support feature including when to use this feature, how the feature can be enabled, and provides a list of allowed operations that Microsoft Engineers can run on your device remotely.

About remote support

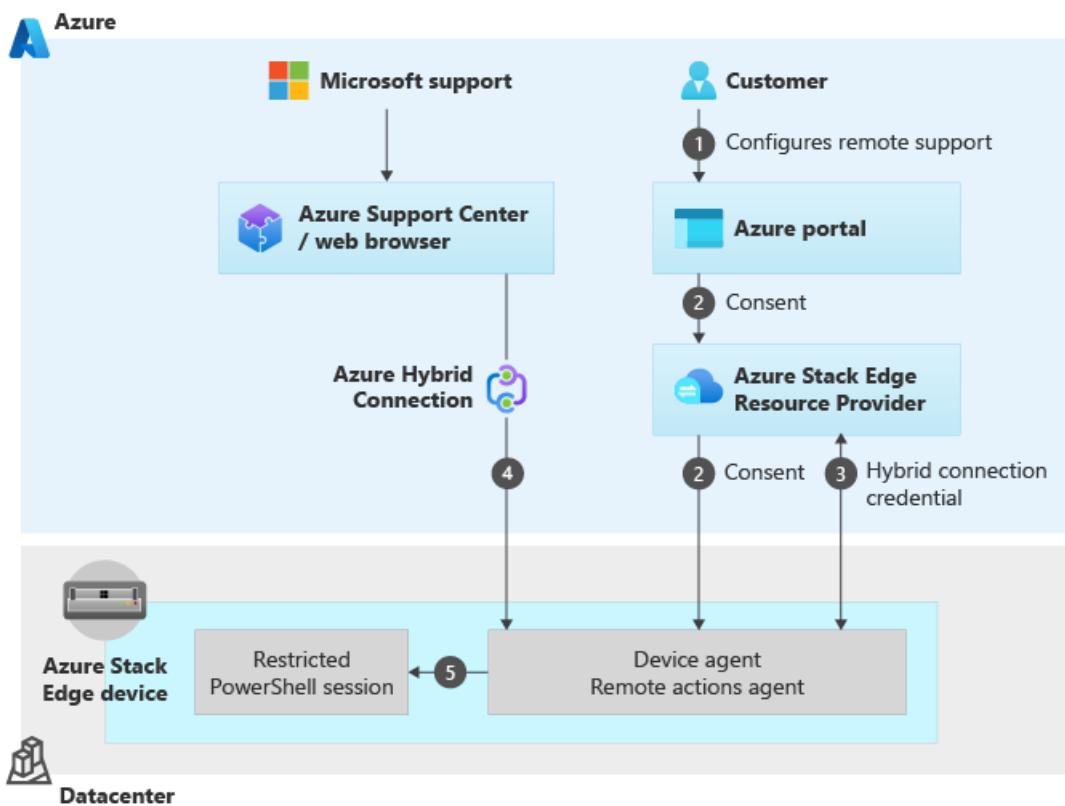
If you experience an issue with Azure Stack Edge, typically, you should collect a support package and provide to Microsoft Support. In some cases, the logs do not have enough information to diagnose and remediate the issue. Microsoft Support then reaches out to you to get your consent for remote support.

Here are some benefits of remote support:

- You can resolve the issue faster as Microsoft Support doesn't need to arrange an in-person meeting.
- You can view the transcript of the remote support session including all the operations that were executed on the device.
- You are in full control of your data and can revoke consent at any time. If you forget to exit the session, the access to the session is automatically disabled once the access duration expires.

How remote support works

The following illustration shows how the remote support works.



1. You provide consent for remote support for your device via the Azure portal. You also configure the level and the duration of access for your device.
2. The consent and request for remote support is sent from the Azure portal to the Azure Stack Edge Resource Provider (RP) which in turn sends it down to the device. The device agent asks the RP for the hybrid connection credential that it can connect to.
3. A hybrid connection credential is created that is used to establish an Azure hybrid connection. This connection is:
 - Device specific. Each device has its own connection and the connection is not shared.
 - Allows Microsoft Support to have a just-in-time (JIT) access to device over a secure, audited, and compliant channel.
 - This connection uses an *https* protocol over port 443 and the traffic is encrypted with TLS 1.2.
4. The device agent starts listening onto that hybrid connection for any requests that are coming via the browser interface for the Azure Support Center.
5. The browser requests to connect to the hybrid connection and the request is sent to the device to open a restricted PowerShell session. If the consent exists, the request is accepted. If the device doesn't have the consent, it just rejects that connection.

Once the connection is established, all the communication occurs over this secure connection.

The operations that Microsoft Support can perform over this connection are *restricted* based on the access level granted using [just enough administration](#) (JEA). For more information about cmdlets that Microsoft Support can execute during a remote support session, see the [list of allowed Microsoft Support operations](#) in this article.

Enable remote support

To configure remote support for your Azure Stack Edge device, follow these steps:

1. In the Azure portal, go to the Azure Stack Edge resource for your device and then go to **Diagnostics**.
2. By default, Microsoft does not have remote access to your device and remote support status is displayed

as **Not enabled**. To enable this feature, select **Configure remote support**.

The screenshot shows the 'Diagnostics' section of the Azure Stack Edge portal. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Security, Order details), and Edge services (Virtual machines, IoT Edge). The 'Diagnostics' option is highlighted with a red box. In the main content area, there are two sections: 'Device Log Collection' and 'Remote Support'. Under 'Device Log Collection', it says 'Consent enabled for log collection' with a 'Revoke Consent' button. Under 'Remote Support', it says 'Allow authorized Microsoft customer service engineers to remotely connect to your device.' with a 'Remote support' status labeled 'Not enabled' and a 'Configure Remote Support' button highlighted with a red box.

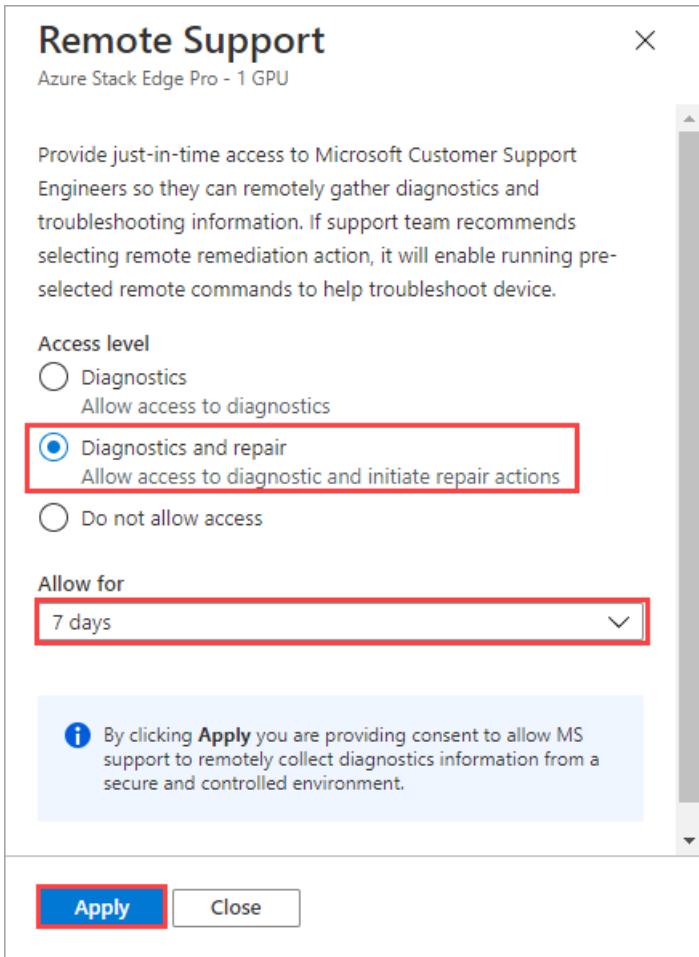
3. Select the **Access level** as **Diagnostics** to provide JIT access to Microsoft Support to remotely gather diagnostics information. If needed, Support team will recommend that you select **Diagnostics and repair** to allow remote remediation action.

Each access level enables a different set of remote commands on the device and hence, a different set of operations.

- Diagnostics allows mostly read operations and hence, mostly `Get` cmdlets are available.
- Diagnostics and repair allows read-write access and hence, in addition to `Get` cmdlets, `Set`, `Add`, `Start`, `Restart`, `Stop`, `Invoke`, `Remove` cmdlets are also available.

For more information, see a [List of all the Support operations allowed in each access level](#).

4. Select the duration over which to provide remote access. The duration can be 7, 15, 21, or 30 days. At the end of this duration, the remote access to the device is automatically disabled.
5. To revoke access at any time, set to **Do not allow access**. This action terminates any existing sessions does not allow new sessions to be established.
6. Once you have configured remote support, select **Apply** for the settings to take effect. When you select **Apply**, you provide consent to Microsoft to remotely collect diagnostics information from a secure and controlled environment.



Remote support examples

The following example scenarios show you how to perform various operations when remote support is enabled on your device.

To perform the remote support operations, you'll first need to [Connect to the PowerShell interface](#) of the device and then run the cmdlets.

List existing remote sessions

Use the `Get-HcsRemoteSupportSession` cmdlet to list all the remote sessions that were made to the device within the specified number of days.

```
Get-HcsRemoteSupportSession -IncludeTranscriptContents $false -NumberOfDays <Number of days>
```

Here is an example output for all the remote support sessions configured in the past 10 days.

```
[10.126.76.20]: PS>Get-HcsRemoteSupportSession -IncludeTranscriptContents $false -NumberOfDays 10

SessionId          : 3c135cba-f479-4fef-8dbb-a2b52b744504
RemoteApplication : Powershell
AccessLevel        : ReadWrite
ControlSession     : False
SessionStartTime   : 8/19/2021 10:41:03 PM +00:00
SessionEndTime     : 8/19/2021 10:44:31 PM +00:00
SessionTranscriptPath :
C:\ProgramData\JEAConfiguration\Transcripts\RemoteRepair\PowerShell_transcript.HW4J1T2.Lp+Myhb.20210
                                         819154101.txt
SessionTranscriptContent :

SessionId          : c0f2d002-66a0-4d54-87e4-4b1b949ad686
RemoteApplication : Powershell
AccessLevel        : ReadWrite
ControlSession     : False
SessionStartTime   : 8/19/2021 7:41:19 PM +00:00
SessionEndTime     : 8/19/2021 7:58:20 PM +00:00
SessionTranscriptPath :
C:\ProgramData\JEAConfiguration\Transcripts\RemoteRepair\PowerShell_transcript.HW4J1T2.j01Cd5Tm.20210
                                         819124117.txt
SessionTranscriptContent :

SessionId          : ca038e58-5344-4377-ab9c-c857a27c8b73
RemoteApplication : Powershell
AccessLevel        : ReadOnly
ControlSession     : False
SessionStartTime   : 8/19/2021 10:49:39 PM +00:00
SessionEndTime     : 8/20/2021 12:49:40 AM +00:00
SessionTranscriptPath :
C:\ProgramData\JEAConfiguration\Transcripts\RemoteDiagnostics\PowerShell_transcript.HW4J1T2.YHmes94q.
                                         20210819154937.txt
SessionTranscriptContent :

[10.126.76.20]: PS>
```

Get details on a specific remote session

Use the `Get-HcsRemoteSupportSession` cmdlet to get the details for remote session with the ID *SessionID*.

```
Get-HcsRemoteSupportSession -SessionId <SessionId> -IncludeSessionTranscript $true
```

Here is an example output for a specific session in which the remote support was configured with the **Diagnostics** option. The `AccessLevel` in this case is `ReadOnly`.

```
[10.126.76.20]: PS>Get-HcsRemoteSupportSession -SessionId 360706a2-c530-419f-932b-55403e19502e -
IncludeTranscriptContents $true

SessionId          : 360706a2-c530-419f-932b-55403e19502e
RemoteApplication : Powershell
AccessLevel        : ReadOnly
ControlSession     : False
SessionStartTime   : 8/26/2021 2:35:37 PM +00:00
SessionEndTime     :
SessionTranscriptPath :
C:\ProgramData\JEAConfiguration\Transcripts\RemoteDiagnostics\PowerShell_transcript.HW4J1T2.u7qF2J2d.
                                         20210826073536.txt
SessionTranscriptContent : ****
Windows PowerShell transcript start
Start time: 20210826073536
Username: WORKGROUP\HW4J1T2$
RunAs User: WORKGROUP\SYSTEM
Configuration Name: RemoteDiagnostics
```

```
Machine: HW4J1T2 (Microsoft Windows NT 10.0.17763.0)
Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding
Process ID: 10976
PSVersion: 5.1.17763.10520
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.10520
BuildVersion: 10.0.17763.10520
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
PS>CommandInvocation(Get-Command): "Get-Command"
>> ParameterBinding(Get-Command): name="Name"; value="Out-Default, Exit-
PSSession"
>> ParameterBinding(Get-Command): name=" CommandType"; value="Alias, Function,
Filter, Cmdlet,
Configuration"
>> ParameterBinding(Get-Command): name="Module"; value=""
>> ParameterBinding(Get-Command): name="ListImported"; value="True"
>> ParameterBinding(Get-Command): name="ErrorAction"; value="SilentlyContinue"
>> CommandInvocation(Measure-Object): "Measure-Object"
>> CommandInvocation(Select-Object): "Select-Object"
>> ParameterBinding(Select-Object): name="Property"; value="Count"
>> ParameterBinding(Measure-Object): name="InputObject"; value="Out-Default"
>> ParameterBinding(Measure-Object): name="InputObject"; value="Exit-PSSession"
PS>ParameterBinding(Select-Object): name="InputObject";
value="Microsoft.PowerShell.Commands.GenericMeasureInfo"

Count
-----
2

PS>CommandInvocation(Get-Command): "Get-Command"
>> ParameterBinding(Get-Command): name="Name"; value="Out-Default, Exit-
PSSession"
>> ParameterBinding(Get-Command): name=" CommandType"; value="Alias, Function,
Filter, Cmdlet,
Configuration"
>> ParameterBinding(Get-Command): name="Module"; value=""
>> ParameterBinding(Get-Command): name="ListImported"; value="True"
>> CommandInvocation(Select-Object): "Select-Object"
>> ParameterBinding(Select-Object): name="Property"; value="Name, Namespace,
HelpUri, CommandType,
ResolvedCommandName, OutputType, Parameters"
>> ParameterBinding(Select-Object): name="InputObject"; value="Out-Default"

Name : Out-Default
Namespace : Microsoft.PowerShell.Core
HelpUri : https://go.microsoft.com/fwlink/?LinkID=113362
CommandType : Cmdlet
ResolvedCommandName :
OutputType : {}
Parameters : {[Transcript,
System.Management.Automation.ParameterMetadata], [InputObject,
System.Management.Automation.ParameterMetadata], [Verbose,
System.Management.Automation.ParameterMetadata], [Debug,
System.Management.Automation.ParameterMetadata]...}

>> ParameterBinding(Select-Object): name="InputObject"; value="Exit-PSSession"
Name : Exit-PSSession
Namespace :
HelpUri :
CommandType : Function
ResolvedCommandName :
OutputType : {}
Parameters : {}
```

```
PS>CommandInvocation(Get-Command): "Get-Command"
```

```
CommandInvocation(Get-HcsApplianceInfo): "Get-HcsApplianceInfo"
```

```
[10.126.76.20]: PS>
```

Here is an example sample output when the **Diagnostics and repair** option was configured for remote support. The `AccessLevel` for remote support session is `ReadWrite`.

```
[10.126.76.20]: PS>Get-HcsRemoteSupportSession -SessionId add360db-4593-4026-93d5-6d6d05d39046 -  
IncludeTranscriptContents $true  
  
SessionId : add360db-4593-4026-93d5-6d6d05d39046  
RemoteApplication : Powershell  
AccessLevel : ReadWrite  
ControlSession : False  
SessionStartTime : 8/26/2021 2:57:08 PM +00:00  
SessionEndTime :  
SessionTranscriptPath :  
C:\ProgramData\JEAConfiguration\Transcripts\RemoteRepair\PowerShell_transcript.HW4J1T2.ZroHb8Un.20210  
826075705.txt  
SessionTranscriptContent : *****  
Windows PowerShell transcript start  
Start time: 20210826075705  
Username: WORKGROUP\HW4J1T2$  
RunAs User: WORKGROUP\SYSTEM  
Configuration Name: RemoteRepair  
Machine: HW4J1T2 (Microsoft Windows NT 10.0.17763.0)  
Host Application: C:\Windows\system32\wsmpprovhost.exe -Embedding  
Process ID: 21832  
PSVersion: 5.1.17763.10520  
PSEdition: Desktop  
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.10520  
BuildVersion: 10.0.17763.10520  
CLRVersion: 4.0.30319.42000  
WSManStackVersion: 3.0  
PSRemotingProtocolVersion: 2.3  
SerializationVersion: 1.1.0.1  
*****  
PS>CommandInvocation(Get-Command): "Get-Command"  
>> ParameterBinding(Get-Command): name="Name"; value="Out-Default, Exit-  
PSSession"  
>> ParameterBinding(Get-Command): name=" CommandType"; value="Alias, Function,  
Filter, Cmdlet,  
Configuration"  
>> ParameterBinding(Get-Command): name="Module"; value=""  
>> ParameterBinding(Get-Command): name="ListImported"; value="True"  
>> ParameterBinding(Get-Command): name="ErrorAction"; value="SilentlyContinue"  
>> CommandInvocation(Measure-Object): "Measure-Object"  
>> CommandInvocation(Select-Object): "Select-Object"  
>> ParameterBinding(Select-Object): name="Property"; value="Count"  
>> ParameterBinding(Measure-Object): name="InputObject"; value="Out-Default"  
>> ParameterBinding(Measure-Object): name="InputObject"; value="Exit-PSSession"  
PS>ParameterBinding(Select-Object): name="InputObject";  
value="Microsoft.PowerShell.Commands.GenericMeasureInfo"  
  
Count  
----  
2  
  
PS>CommandInvocation(Get-Command): "Get-Command"  
>> ParameterBinding(Get-Command): name="Name"; value="Out-Default, Exit-  
PSSession"  
>> ParameterBinding(Get-Command): name=" CommandType"; value="Alias, Function,  
Filter, Cmdlet,  
Configuration"  
>> ParameterBinding(Get-Command): name="Module"; value=""
```

```

    >> ParameterBinding(Get-Command): name=Module , value
    >> ParameterBinding(Get-Command): name="ListImported"; value="True"
    >> CommandInvocation(Select-Object): "Select-Object"
    >> ParameterBinding(Select-Object): name="Property"; value="Name, Namespace,
HelpUri, CommandType,
ResolvedCommandName, OutputType, Parameters"
    >> ParameterBinding(Select-Object): name="InputObject"; value="Out-Default"

        Name          : Out-Default
        Namespace     : Microsoft.PowerShell.Core
        HelpUri       : https://go.microsoft.com/fwlink/?LinkID=113362
        CommandType   : Cmdlet
        ResolvedCommandName :
        OutputType    : {}
        Parameters    : {[Transcript,
System.Management.Automation.ParameterMetadata], [InputObject,
System.Management.Automation.ParameterMetadata], [Verbose,
System.Management.Automation.ParameterMetadata], [Debug,
System.Management.Automation.ParameterMetadata]...}

    >> ParameterBinding(Select-Object): name="InputObject"; value="Exit-PSSession"
        Name          : Exit-PSSession
        Namespace     :
        HelpUri       :
        CommandType   : Function
        ResolvedCommandName :
        OutputType    : {}
        Parameters    : {}

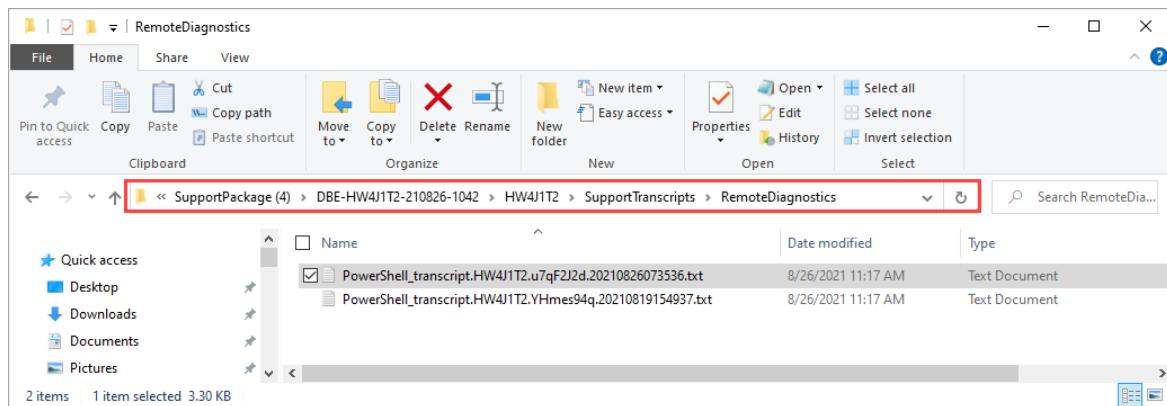
PS>CommandInvocation(Get-Command): "Get-Command"
[10.126.76.20]: PS>

```

Collect remote session transcripts

Depending on your audit requirements, you may need to view the transcripts. Follow these steps to collect remote session transcripts:

1. In the local UI, go to **Troubleshooting > Support**. Gather a Support package.
2. Once the support package is collected, download the support package. Extract the zipped folder. The transcripts are located in **SupportTranscripts** folder in the support package.



Operations allowed in remote support

The following sections list the allowed cmdlets that Microsoft Support can execute during a remote support session. The cmdlet availability is broken down by the access level set to **Diagnostics** or **Diagnostics and repair**.

Azure Stack Edge cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Add-HcsExternalVirtualSwitch		Y	Creates a new external virtual switch to configure Kubernetes on your device.
Add-HcsVirtualNetwork		Y	Creates a new virtual switch on a specified network interface.
Get-AcsHealthStatus	Y	Y	Gets the health status of Azure Consistent Service Providers.
Get-AzureDataBoxEdgeRole	Y	Y	Gets compute logs via the PowerShell interface if compute role is configured on your device .
Get-HcsApplianceInfo	Y	Y	Gets information for your device such as ID, friendly name, software version, or system state.
Get-HcsApplianceSupportPackage	Y	Y	Collects support package for your device.
Get-HcsArpResponse	Y	Y	
Get-HcsControllerSetupInformation	Y	Y	Gets the Microsoft.Hcs.Setup.ControllerInfo object.
Get-HcsDataBoxAccount	Y	Y	
Get-HcsExternalVirtualSwitch	Y	Y	Gets the switch Kubernetes should be configured on.
Get-HcsGpuNvidiaSmi	Y	Y	Gets the GPU driver information for your device.
Get-HcsIPAddress	Y	Y	Fetches network adapters configuration from datastore or system.
Get-HcsIPAddressPool		Y	
Get-HcsKubeClusterInfo	Y	Y	Gets Kubernetes cluster configuration information.
Get-HcsKubeClusterNetworkInfo	Y	Y	Gets the Kubernetes service and pod subnets.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-HcsKubernetesAzureMonitorConfiguration	Y	Y	Gets information on the Azure Monitor running on the Kubernetes cluster on your device.
Get-HcsKubernetesContainerRegistryInfo	Y	Y	Gets the details for the edge container registry on your device.
Get-HcsKubernetesDashboardToken	Y	Y	Gets the Kubernetes dashboard token to view the dashboard (you can do that same via the local UI).
Get-HcsKubernetesNamespaces	Y	Y	Gets Kubernetes namespace that you've configured.
Get-HcsKubernetesUserConfig	Y	Y	Gets the <code>kubeconfig</code> corresponding to a specific namespace that you've configured.
Get-HcsLocalWebUICertificateHash	Y	Y	Gets the thumbprint of the configured local web UI certificate.
Get-HcsMacAddressPool		Y	Gets the Kubernetes VM Mac address pool.
Get-HcsNetBmcInterface	Y	Y	Gets the network configuration properties of the baseboard management controller (BMC) such as IPv4 address, IPv4 gateway, IPv4 subnet mask and whether DHCP is enabled or not on your device.
Get-HcsNetInterface	Y	Y	Fetches the desired network configuration of the device.
Get-HcsNetRoute	Y	Y	Checks for all the custom route configurations that you added on your device. These routes do not include all the system routes or default routes that already exist on the device.
Get-HcsNodeSecureEraseLogs	Y	Y	to be removed, confirm from Ernie - Retrieves logs that confirm that drives in the device were securely erased during the previous reset to factory defaults.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-HcsNodeSupportPackage	Y	Y	Collects logs from your device and copies those logs to a specified network or local share in form of support package.
Get-HcsRemoteSupportConsent	Y	Y	Gets consent from the customer to enable remote support on the device.
Get-HcsRestEndPoint	Y	Y	
Get-HcsSetupDesiredStateResult	Y	Y	Gets Desired State Configuration (DSC) result objects of some DSC executions for your device.
Get-HcsSmbConfiguration	Y	Y	
Get-HcsSupportedVpnRegions	Y	Y	
Get-HcsSupportPackageUploadJob	Y	Y	Gets the status of a Support package upload job that is running.
Get-HcsUpdateConfiguration	Y	Y	Gets the update server settings such as server type, URI path to the server, configured for your Azure Stack Edge device.
Get-HcsUpdateJob	Y	Y	Fetches all the update jobs running on your device or the status of a given update job when the job ID is passed.
Get-HcsVirtualNetwork		Y	Identifies the virtual network and the subnet associated with a switch that you created on your device.
Get-HcsVirtualSwitch	Y	Y	Gets virtual switch associated with a specified network interface.
Get-VMInGuestLogs		Y	Collects in-guest logs for failed VMs on your device.
Invoke-AzureDataBoxEdgeRoleReconcile		Y	Used to bring the Kubernetes cluster configuration up-to-date.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Invoke-AzureDataBoxEdgeRoleReconfigure		Y	Used to change the configuration of the Kubernetes cluster.
Remove-HcsIPAddressPool			Removes the Kubernetes VM Mac address pool.
Remove-HcsKubeClusterNetworkInfo		Y	Change the Kubernetes service subnets or pods.
Remove-HcsKubernetesAzureArcAgent		Y	Removes the Azure Arc agent from the Kubernetes cluster on your device.
Remove-HcsKubernetesAzureMonitorConfiguration		Y	Removes Azure Monitor from the Kubernetes cluster on your device and allows you to collect container logs and processor metrics from the Kubernetes cluster.
Remove-HcsKubernetesContainerRegistry		Y	Deletes the edge container registry from your device.
Remove-HcsKubernetesNamespace		Y	Deletes a specified Kubernetes namespace.
Remove-HcsMacAddressPool		Y	Removes the Kubernetes VM Mac address pool.
Remove-HcsNetRoute		Y	Removes a route configuration that you added on your device.
Remove-HcsVirtualNetwork		Y	Removes a virtual network and the subnet associated with a switch that you created on your device.
Remove-HcsVirtualSwitch		Y	Removes a virtual switch associated with a port on your device.
Restart-HcsNode		Y	Restarts a node on your device. For a single node device, this restarts the device and results in a downtime.
Set-AzureDataBoxEdgeRoleCompute		Y	Used to configure compute through the Azure portal and creates and configures the Kubernetes cluster.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Set-HcsCertificate		Y	Enables to bring your own certificates.
Set-HcsClusterLevelSecurity		Y	Configure the level of security of cluster traffic. This includes intra-node cluster traffic and traffic from Cluster Shared Volumes (CSV).
Set-HcsClusterWitness		Y	Creates or configures a Windows cluster witness. A cluster witness helps establish a quorum when a node goes down in a 2-node device.
Set-HcsEastWestCsvEncryption		Y	
Set-HcsExternalVirtualSwitch		Y	Configures an external virtual switch on the port for which you enabled compute on your device.
Set-HcsIpAddress		Y	Updates network interface properties.
Set-HcsIpAddressPool			Sets the Kubernetes VM Mac address pool.
Set-HcsKubeClusterNetworkInfo		Y	Changes Kubernetes pod and service subnets before you configure compute from the Azure portal on your device.
Set-HcsKubernetesAzureArcAgent		Y	Enables Azure Arc on Kubernetes cluster by installing the Arc agent on your device.
Set-HcsKubernetesAzureArcDataController		Y	Creates a data controller on Kubernetes cluster on your device.
Set-HcsKubernetesAzureMonitorConfiguration		Y	Enables Azure Monitor on the Kubernetes cluster on your device and allows you to collect container logs and processor metrics from the Kubernetes cluster.
Set-HcsKubernetesContainerRegistry		Y	Enables edge container registry as an add-on for your device.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Set-HcsMacAddressPool		Y	Sets the Kubernetes VM Mac address pool.
Set-HcsNetBmcInterface		Y	Enables or disables DHCP configuration for BMC.
Set-HcsNetInterface		Y	Configure IP address, subnet mask, and gateway for a network interface on your Azure Stack Edge device.
Set-HcsSmbServerEncryptionConfiguration		Y	
Set-HcsSmbSigningConfiguration		Y	
Set-HcsUpdateConfiguration		Y	Sets the update server settings for your device including the server type and the URI path to the server. You can choose to install updates from a Microsoft Update server or from Windows Server Update Services (WSUS) server.
Set-HcsVirtualNetwork		Y	Creates a virtual network and the subnet associated with a switch that you created on your device.
Set-HcsVpnS2SInterface		Y	
Start-HcsGpuMPS		Y	Enables Multi-processor service (MPS) on your device.
Start-HcsSupportPackageUploadJob	Y	Y	Collects a support package with all the logs and uploads the package so that Microsoft can use it to debug any issues with your device.
Start-HcsUpdateJob		Y	Starts update job.
Stop-HcsGpuMPS		Y	Disables Multi-processor service (MPS) on your device.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Test-HcsKubernetesStatus	Y	Y	Runs the Kubernetes diagnostics container.

Generic network cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Find-NetRoute	Y	Y	Finds the best local IP address and the best route to reach a remote address.
Get-NetAdapter	Y	Y	Gets the basic network adapter properties.
Get-NetIPAddress	Y	Y	Gets the entire IP address configuration for the computer.
Get-NetNat	Y	Y	Gets Network Address Translation (NAT) objects configured on a computer.
Get-NetNatExternalAddress	Y	Y	Gets a list of external addresses configured on a network address translation (NAT) instance.
Get-NetRoute	Y	Y	Gets IP route information from the IP routing table, including destination network prefixes, next hop IP addresses, and route metrics.
Get-NetCompartment	Y	Y	Gets network compartments in the protocol stack
Get-NetNeighbor	Y	Y	Gets neighbor cache entries.
Get-NetAdapterSriov	Y	Y	Gets the SR-IOV properties of the network adapter.
Resolve-DnsName		Y	Performs a DNS name query resolution for the specified name.

Multi-access Edge Computing (MEC) cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
---------	-------------	----------------------	-------------

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-MecVnf	Y	Y	Gets a list of all multi-access edge compute virtual network function VMs deployed on your Azure Stack Edge.
Get-MecVirtualMachine	Y	Y	Gets a list of virtual machines created by multi-access edge compute virtual networks functions.
Get-MecServiceConfig	Y	Y	Gets multi-access edge compute service configuration that affects the virtual network functions. lifecycle workflow.
Get-MecInformation	Y	Y	Gets multi-access edge compute information. For example, whether your Azure Stack Edge device has registered with the Azure Network Function Manager.

General-purpose OS cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Select-String	Y	Y	Finds text in strings and files.
Write-Progress	Y	Y	Displays a progress bar within a PowerShell command window.
Get-Command	Y	Y	Gets a list of commands that can be run in a session.
Measure-Object	Y	Y	Calculates the numeric properties of objects, and the characters, words, and lines in string objects, such as files of text.
Select-Object	Y	Y	Selects objects or object properties.
Out-Default		Y	Sends the output to the default formatter and to the default output cmdlet.
Get-WinEvent	Y	Y	Gets events from event logs and event tracing log files.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-Counter	Y	Y	Gets performance counter data.
Get-Volume	Y	Y	Gets the specified Volume object, or all Volume objects if no filter is provided.
Get-Service	Y	Y	Gets objects that represent the services.

Cluster cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-ClusterResource	Y	Y	Gets information about one or more resources in a failover cluster.
Get-Cluster	Y	Y	Gets information about failover cluster.
Get-ClusterNode	Y	Y	Gets information about one or more nodes, or servers, in a failover cluster.
Start-Cluster		Y	Starts the Cluster service on all nodes of the cluster on which it is not yet started.
Start-ClusterResource		Y	Brings a resource online in a failover cluster.
Stop-ClusterResource		Y	Takes a resource offline in a failover cluster.

Hyper-V cmdlets

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-Vm	Y	Y	Gets the virtual machines on the computer.
Get-VMNetworkAdapter	Y	Y	Gets the virtual network adapters of a virtual machine, snapshot, management operating system, or of a virtual machine and management operating system.
Get-VMHardDiskDrive	Y	Y	Gets the virtual hard disk drives attached to one or more virtual machines.

CMDLETS	DIAGNOSTICS	DIAGNOSTICS & REPAIR	DESCRIPTION
Get-VMSwitch	Y	Y	Gets the list of virtual switches.

Next steps

[Contact Microsoft Support.](#)

Open a support ticket for Azure Stack Edge and Azure Data Box Gateway

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R Azure Stack Edge Mini R Azure Stack Edge FPGA Azure Data Box Gateway

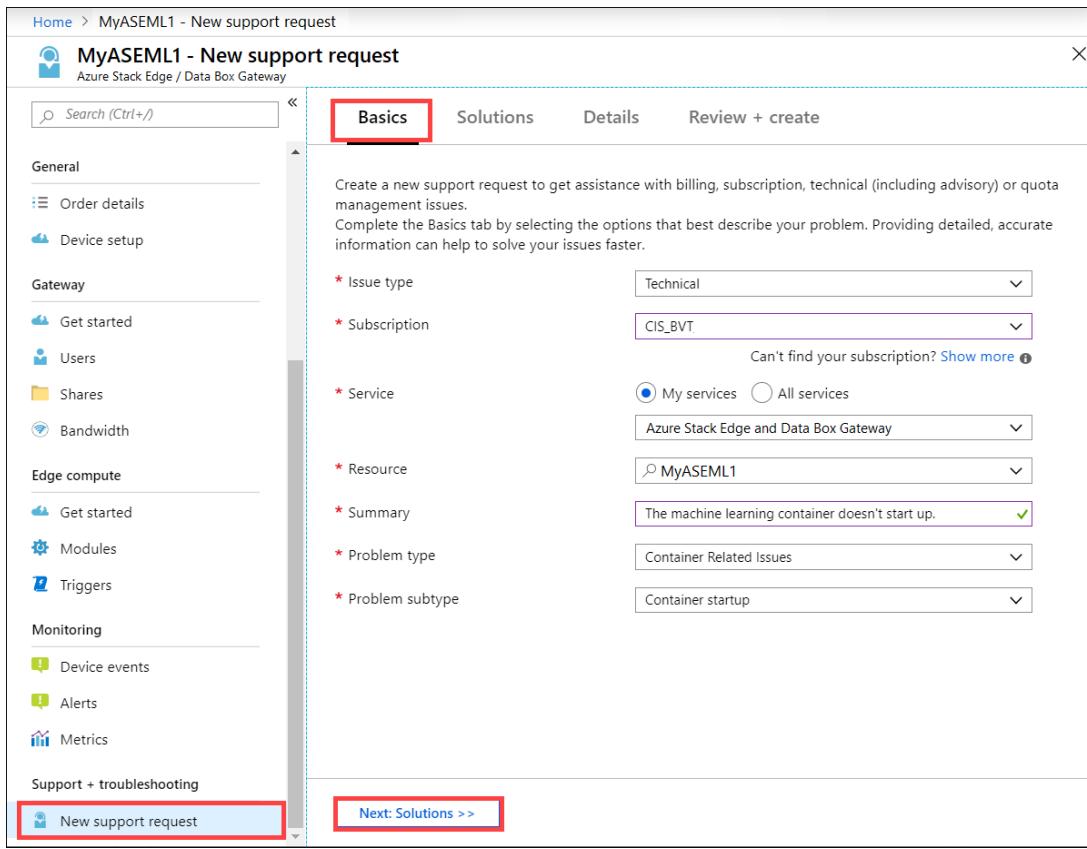
This article applies to Azure Stack Edge and Azure Data Box Gateway both of which are managed by the Azure Stack Edge / Azure Data Box Gateway service. If you encounter any issues with your service, you can create a service request for technical support. This article walks you through:

- How to create a support request.
- How to manage a support request lifecycle from within the portal.

Create a support request

Do the following steps to create a support request:

1. Go to your Azure Stack Edge or Data Box Gateway order. Navigate to **Support + troubleshooting** section and then select **New support request**.
2. In **New support request**, on the **Basics** tab, take the following steps:
 - a. From the **Issue type** dropdown list, select **Technical**.
 - b. Choose your **Subscription**.
 - c. Under **Service**, check **My Services**. From the dropdown list, select **Azure Stack Edge and Data Box Gateway**.
 - d. Select your **Resource**. This corresponds to the name of your order.
 - e. Give a brief **Summary** of the issue you are experiencing.
 - f. Select your **Problem type**.
 - g. Based on the problem type you selected, choose a corresponding **Problem subtype**.
 - h. Select **Next: Solutions >>**.



3. On the **Details** tab, take the following steps:

- a. Provide the start date and time for the problem.
- b. Supply a **Description** for your problem.
- c. In the **File upload**, select the folder icon to browse any other files you want to upload.
- d. Check **Share diagnostic information**.
- e. Based on your subscription, a **Support plan** is automatically populated.
- f. From the dropdown list, select the **Severity**.
- g. Specify a **Preferred contact method**.
- h. The **Response hours** are automatically selected based on your subscription plan.
- i. Provide the language you prefer for Support.
- j. In the **Contact information**, provide your name, email, phone, optional contact, country/region. Microsoft Support uses this information to reach out to you for further information, diagnosis, and resolution.
- k. Select **Next: Review + Create >>**.

Home > MyASEML1 - New support request

MyASEML1 - New support request

Azure Stack Edge / Data Box Gateway

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Properties

General

Order details

Device setup

Gateway

Get started

Users

Shares

Bandwidth

Edge compute

Get started

Modules

Triggers

Monitoring

Device events

Alerts

Metrics

Support + troubleshooting

New support request

Basics Solutions Details Review + create

PROBLEM DETAILS

When did the problem start? 2019-07-10 12:00 AM

* Description
The machine learning container that I deployed on Azure Stack Edge does not start up.

File upload Choose file to upload

Consent Share diagnostic information

SUPPORT METHOD

Support plan Azure Support Plan - Internal

* Severity B - Moderate impact

* Preferred contact method

Contact me later Email Call me later Phone

* Response hours Business Hours 24x7

* Support language English

CONTACT INFO Edit

Contact name John Contoso

Email john@contoso.com

Additional email for notification --

<< Previous: Basics Next: Review + create >>

The screenshot shows the 'New support request' interface in the Azure Stack Edge portal. The 'Details' tab is active. In the 'PROBLEM DETAILS' section, the 'Description' field contains a note about a machine learning container not starting. The 'SUPPORT METHOD' section shows the support plan as 'Azure Support Plan - Internal' and the severity as 'B - Moderate impact'. Under 'Preferred contact method', both 'Contact me later' (Email) and 'Call me later' (Phone) are listed. The 'CONTACT INFO' section shows the contact name as 'John Contoso' and the email as 'john@contoso.com'. Navigation buttons at the bottom allow switching between 'Basics' and 'Review + create'.

4. On the **Review + Create** tab, review the information related to Support ticket. Select **Create**.

Home > MyASEML1 - New support request

MyASEML1 - New support request

Azure Stack Edge / Data Box Gateway

Search (Ctrl+I)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Properties

General

Order details

Device setup

Gateway

Get started

Users

Shares

Bandwidth

Edge compute

Get started

Modules

Triggers

Monitoring

Device events

Alerts

Metrics

Support + troubleshooting

New support request

Basics Solutions Details Review + create

BASICS

Issue type	Technical
Subscription	CIS_BVT
Service	Azure Stack Edge and Data Box Gateway
Resource	MyASEML1
Problem type	Container Related Issues
Problem subtype	Container startup
Summary	The machine learning container doesn't start up.

TERMS, CONDITIONS AND PRIVACY POLICY

By clicking "Create" you accept the [terms and conditions](#).

View our [privacy policy](#).

DETAILS

When did the problem start?	Wed, Jul 10, 2019, 12:00 AM PDT
Description	The machine learning container that I deployed on Azure Stack Edge does not start up.
Consent	Share diagnostic information

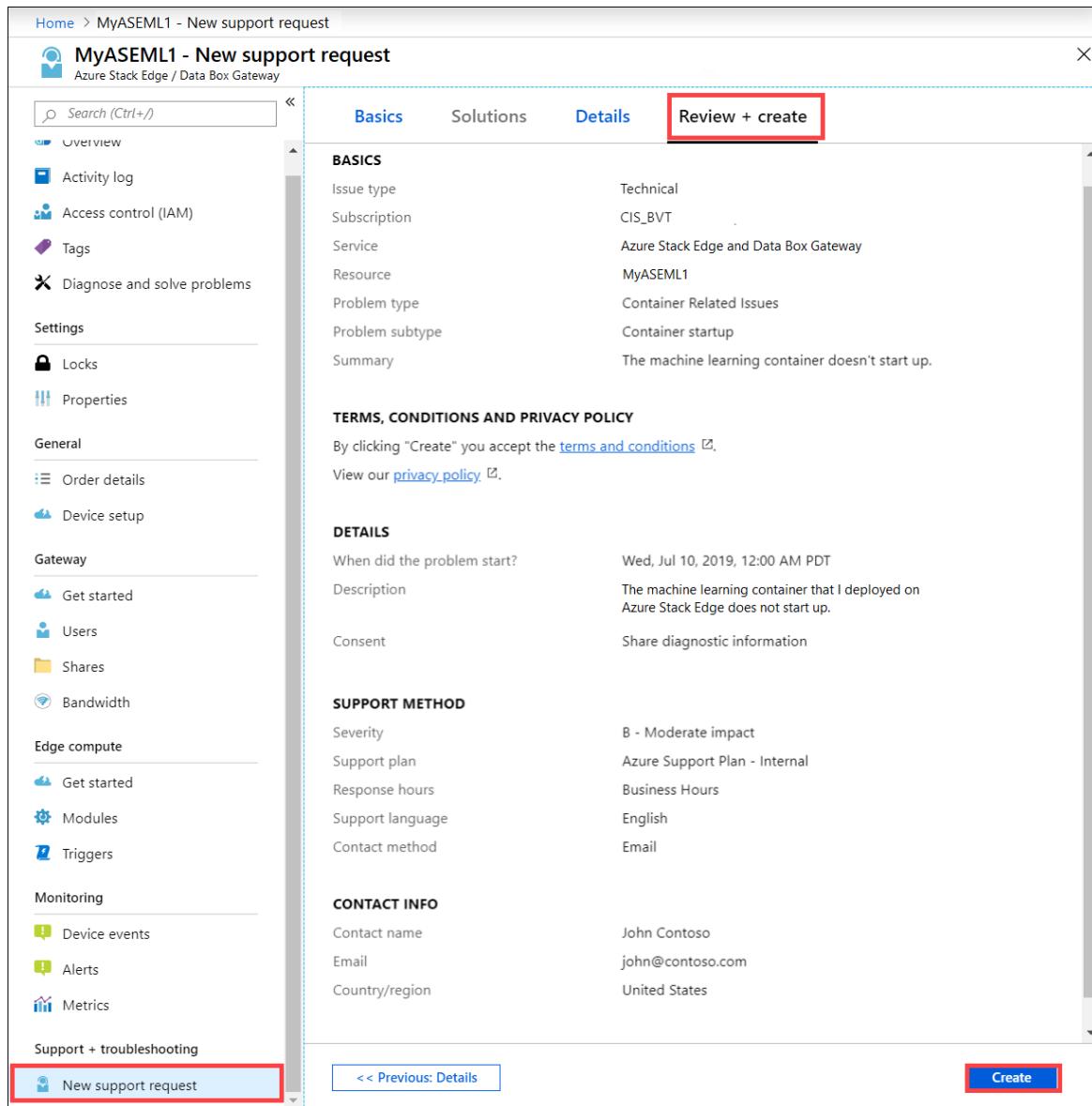
SUPPORT METHOD

Severity	B - Moderate impact
Support plan	Azure Support Plan - Internal
Response hours	Business Hours
Support language	English
Contact method	Email

CONTACT INFO

Contact name	John Contoso
Email	john@contoso.com
Country/region	United States

<< Previous: Details Create



After you create the Support ticket, a Support engineer will contact you as soon as possible to proceed with your request.

Get hardware support

This information only applies to Azure Stack device. The process to report hardware issues is as follows:

1. Open a Support ticket from the Azure portal for a hardware issue. Under **Problem type**, select **Azure Stack Hardware**. Choose the **Problem subtype** as **Hardware failure**.

The screenshot shows the 'MyASEML1 - New support request' page in the Azure Stack Edge / Data Box Gateway portal. The left sidebar includes sections for Gateway (Get started, Users, Shares, Bandwidth), Edge compute (Get started, Modules, Triggers), Monitoring (Device events, Alerts, Metrics), and Support + troubleshooting (New support request). The main area has tabs for Basics, Solutions, Details, and Review + create. The Basics tab is active. It contains fields for Issue type (Technical), Subscription (CIS_BVT.), Service (My services selected, Azure Stack Edge and Data Box Gateway), Resource (MyASEML1), Summary (My power supply unit LED indicates that there is a problem...), Problem type (Azure Stack Edge Hardware selected), and Problem subtype (Hardware failure selected). A red box highlights the Problem type and Problem subtype fields.

After you have created the Support ticket, a Support engineer will contact you as soon as possible to proceed with your request.

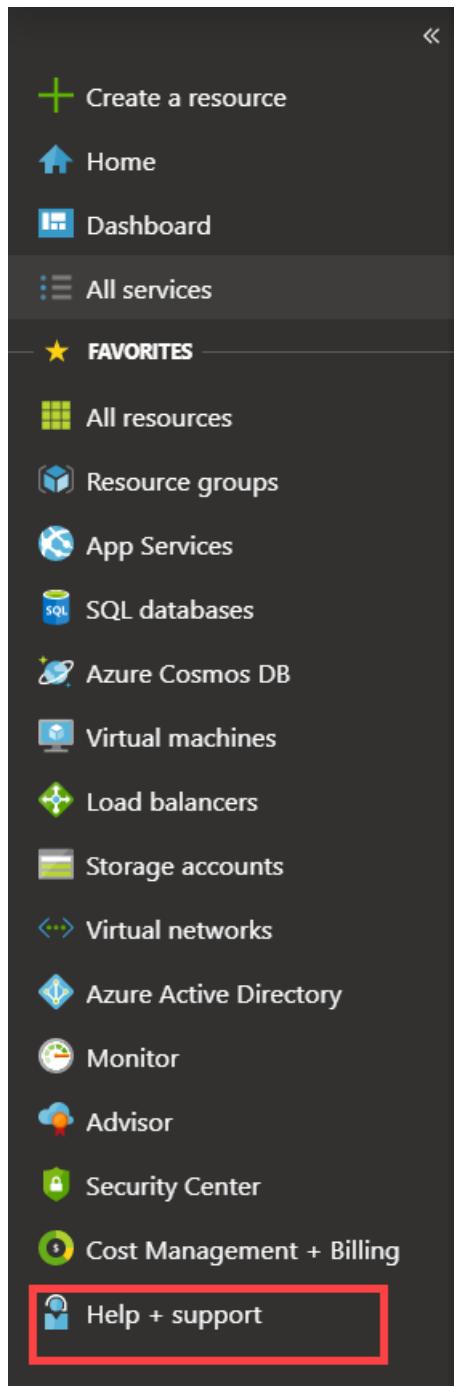
2. If Microsoft Support determines that this is a hardware issue, then one of the following actions occurs:
 - A Field Replacement Unit (FRU) for the failed hardware part is sent. Currently, power supply units and solid-state drives are the only supported FRUs.
 - Only FRUs are replaced within the next business day, everything else requires a full system replacement (FSR) to be shipped.
3. If it is determined that a FRU replacement is needed by 1 PM local time (Monday to Friday), an onsite technician is dispatched the next business day to your location to perform a FRU replacement. A full system replacement typically will take much longer because the parts are shipped from our factory and could be subject to transportation and customs delays.

Manage a support request

After creating a support ticket, you can manage the lifecycle of the ticket from within the portal.

To manage your support requests

1. To get to the help and support page, navigate to **Browse > Help + support**.



2. A tabular listing of **Recent support requests** is displayed in **Help + support**.
3. Select and click a support request. You can view the status and the details for this request. Click **+ New message** if you want to follow up on this request.

Next steps

- [Troubleshoot issues related to Azure Stack Edge FPGA](#).
- [Troubleshoot device issues for Azure Stack Edge Pro GPU](#).
- [Troubleshoot issues related to Data Box Gateway](#).

Azure Stack Edge 2207 release notes

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2207 release for your Azure Stack Edge devices. Features and issues that correspond to a specific model of Azure Stack Edge are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they're added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2207** release, which maps to software version number **2.2.2037.5375**. This software can be applied to your device if you're running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The 2207 release has the following features and enhancements:

- **Kubernetes version update** - This release contains a Kubernetes version update from 1.20.9 to v1.22.6.

Known issues in 2207 release

The following table provides a summary of known issues in this release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features are available in preview: - Clustering and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU devices only. - VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R only. - Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, and Multi-process service (MPS) for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R.	These features will be generally available in later releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
2.	Drive replacement	In this release, if there is a need to replace the drive on your Azure Stack Edge Pro 2 device, contact Microsoft Support to help you with a seamless drive replacement.	
3.	Jumbo frames	When deploying an Azure Stack Edge Pro 2 2-node cluster, enable Jumbo Frames on the network switches in your environment for a better device performance.	

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none"> - In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. - Download <code>sqlcmd</code> on your client machine from SQL command utility. - Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. - Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. These actions can result in the updated sections of the blob to not get updated in the cloud. <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: can't create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	<p>When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:</p> <pre>Azcopy <other arguments> --cap-mbps 2000</pre>	<p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> - Only block blobs are supported. Page blobs aren't supported. - There's no snapshot or copy API support. - Hadoop workload ingestion through <code>distcp</code> isn't supported as it uses the copy operation heavily. 	

No.	Feature	Issue	Workaround/Comments
6.	NFS share connection	If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.	If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You'll need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.
8.	Kubernetes cluster	Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller .	
9.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Don't use reserved IPs.

No.	Feature	Issue	Workaround/Comments
10.	Kubernetes	Kubernetes doesn't currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
11.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device .
12.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts can't be bound to paths in IoT Edge containers. If possible, map the parent directory.
13.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates aren't picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedged</code> and <code>edgehub</code> pods.
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	The following scenarios in the local UI may be affected. <ul style="list-style-type: none">- Status column in Certificates page.- Security tile in Get started page.- Configuration tile in Overview page.

No.	Feature	Issue	Workaround/Comments
15.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	
16.	Web proxy	NTLM authentication-based web proxy isn't supported.	
17.	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
18.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
19.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources aren't deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
20.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
21.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that don't exist on the network.	

No.	Feature	Issue	Workaround/Comments
22.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it isn't possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create one VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available one GPU.
23.	Custom script VM extension	<p>There's a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103.</p> <p>If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> - Connect to the Windows VM using remote desktop protocol (RDP). - Make sure that the <code>waappagent.exe</code> is running on the machine: <code>Get-Process WaAppAgent</code> - If the <code>waappagent.exe</code> isn't running, restart the <code>rdagent</code> service: <code>Get-Service RdAgent Restart-Service</code>. Wait for 5 minutes. - While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. - After you kill the process, the process starts running again with the newer version. - Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <code>Get-Process WindowsAzureGuestAgent fl ProductVersion</code>. - Set up custom script extension on Windows VM.
24.	Multi-Process Service (MPS)	When the device software and the Kubernetes cluster are updated, the MPS setting isn't retained for the workloads.	Re-enable MPS and redeploy the workloads that were using MPS.
25.	Wi-Fi	Wi-Fi doesn't work on Azure Stack Edge Pro 2 in this release.	This functionality may be available in a future release.

Next steps

- [Update your device](#)

Azure Stack Edge 2205 release notes

9/21/2022 • 9 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2205 release for your Azure Stack Edge devices. Features and issues that correspond to a specific model of Azure Stack Edge are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they're added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2205** release, which maps to software version number **2.2.1983.5094**. This software can be applied to your device if you're running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The 2205 release has the following features and enhancements:

- **Kubernetes changes** - Beginning this release, compute enablement is moved to a dedicated Kubernetes page in the local UI.
- **Generation 2 virtual machines** - Starting this release, Generation 2 virtual machines can be deployed on Azure Stack Edge. For more information, see [Supported VM sizes and types](#).
- **GPU extension update** - In this release, the GPU extension packages are updated. These updates will fix some issues that were encountered in a previous release during the installation of the extension. For more information, see how to [Update GPU extension of your Azure Stack Edge](#).
- **No IP option** - Going forward, there's an option to not set an IP for a network interface on your Azure Stack Edge device. For more information, see [Configure network](#).

Issues fixed in 2205 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	GPU Extension installation	In the previous releases, there were issues that caused the GPU extension installation to fail. These issues are described in Troubleshooting GPU extension issues . These are fixed in the 2205 release and both the Windows and Linux installation packages are updated. More information on 2205 specific installation changes is covered in Install GPU extension on your Azure Stack Edge device .

NO.	FEATURE	ISSUE
2.	HPN VMs	In the previous release, the Standard_F12_HPN could only support one network interface and couldn't be used for Multi-Access Edge Computing (MEC) deployments. This issue is fixed in this release.

Known issues in 2205 release

The following table provides a summary of known issues in this release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features are available in preview: - Clustering and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU devices only. - VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R only. - Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, and Multi-process service (MPS) for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R.	These features will be generally available in later releases.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none"> - In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. - Download <code>sqlcmd</code> on your client machine from SQL command utility. - Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. - Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. These actions can result in the updated sections of the blob to not get updated in the cloud. <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre data-bbox="1117 1823 1431 2088">hcuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: can't create directory 'test': Permission denied</pre>

No.	Feature	Issue	Workaround/Comments
4.	Blob Storage ingestion	<p>When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:</p> <pre>Azcopy <other arguments> --cap-mbps 2000</pre>	<p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> - Only block blobs are supported. Page blobs aren't supported. - There's no snapshot or copy API support. - Hadoop workload ingestion through <code>distcp</code> isn't supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You'll need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Kubernetes	<p>Port 31000 is reserved for Kubernetes Dashboard.</p> <p>Port 31001 is reserved for Edge container registry.</p> <p>Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.</p>	Don't use reserved IPs.
10.	Kubernetes	<p>Kubernetes doesn't currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.</p>	<p>To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses.</p> <p>For more information, see IP address sharing.</p>
11.	Kubernetes cluster	<p>Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.</p>	<p>For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device.</p>
12.	Kubernetes	<p>File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.</p>	<p>IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts can't be bound to paths in IoT Edge containers. If possible, map the parent directory.</p>
13.	Kubernetes	<p>If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates aren't picked up.</p>	<p>To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands. Restart <code>iotedged</code> and <code>edgehub</code> pods.</p>

No.	Feature	Issue	Workaround/Comments
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> - Status column in Certificates page. - Security tile in Get started page. - Configuration tile in Overview page.
15.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	
16.	Web proxy	NTLM authentication-based web proxy isn't supported.	
17.	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
18.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
19.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources aren't deleted from the Kubernetes cluster.	<p>To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration.</p>
20.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	

No.	Feature	Issue	Workaround/Comments
21.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that don't exist on the network.	
22.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it isn't possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create one VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available one GPU.
23.	Custom script VM extension	<p>There's a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103.</p> <p>If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> - Connect to the Windows VM using remote desktop protocol (RDP). - Make sure that the <code>waappagent.exe</code> is running on the machine: <code>Get-Process WaAppAgent</code> - If the <code>waappagent.exe</code> isn't running, restart the <code>rdagent</code> service: <code>Get-Service RdAgent Restart-Service</code>. Wait for 5 minutes. - While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. - After you kill the process, the process starts running again with the newer version. - Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <code>Get-Process WindowsAzureGuestAgent fl ProductVersion</code>. - Set up custom script extension on Windows VM.
24.	Multi-Process Service (MPS)	When the device software and the Kubernetes cluster are updated, the MPS setting isn't retained for the workloads.	Re-enable MPS and redeploy the workloads that were using MPS.

No.	Feature	Issue	Workaround/Comments
25.	Wi-Fi	Wi-Fi doesn't work on Azure Stack Edge Pro 2 in this release.	This functionality may be available in a future release.
26.	Device capacity	If you updated to this release from an older build, the device capacity didn't show up in the Azure portal. If a VM was provisioned in the Azure portal, the capacity metrics would update and display.	To sync the metrics on the Azure portal, create a VM and then delete it.

Next steps

- [Update your device](#)

Azure Stack Edge 2203 release notes

9/21/2022 • 9 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2203 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they're added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2203** release, which maps to software version number **2.2.1902.4561**. This software can be applied to your device if you're running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The 2203 release has the following features and enhancements:

- **Kubernetes version update** - This release contains a Kubernetes version update from 1.20.9 to 1.21.7.
- **VM improvements** - A new VM size F12_HPN was added in this release.

Known issues in 2203 release

The following table provides a summary of known issues in this release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features are available in preview: - Clustering and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU devices only. - VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R only. - Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, and Multi-process service (MPS) for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R.	These features will be generally available in later releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
2.	HPN VMs	For this release, the Standard_F12_HPN can only support one network interface and can't be used for Multi-Access Edge Computing (MEC) deployments.	
3.	Device capacity	If you update to this release from an older build, the device capacity doesn't show up in the Azure portal. If a VM is provisioned in the Azure portal, the capacity metrics are updated and displayed.	To sync the metrics on the Azure portal, create a VM and then delete it.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none"> - In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. - Download <code>sqlcmd</code> on your client machine from SQL command utility. - Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. - Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. These actions can result in the updated sections of the blob to not get updated in the cloud. <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:	<pre>Azcopy <other arguments> --cap-mbps 2000</pre> <p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> - Only block blobs are supported. Page blobs aren't supported. - There's no snapshot or copy API support. - Hadoop workload ingestion through <code>distcp</code> isn't supported as it uses the copy operation heavily. 	

No.	Feature	Issue	Workaround/Comments
6.	NFS share connection	If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.	If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You'll need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.
8.	Kubernetes cluster	Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller .	
9.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Don't use reserved IPs.

No.	Feature	Issue	Workaround/Comments
10.	Kubernetes	Kubernetes doesn't currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
11.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device .
12.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts can't be bound to paths in IoT Edge containers. If possible, map the parent directory.
13.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates aren't picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedged</code> and <code>edgehub</code> pods.
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	The following scenarios in the local UI may be affected. <ul style="list-style-type: none">- Status column in Certificates page.- Security tile in Get started page.- Configuration tile in Overview page.

No.	Feature	Issue	Workaround/Comments
15.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	
16.	Web proxy	NTLM authentication-based web proxy isn't supported.	
17.	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
18.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
19.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources aren't deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
20.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
21.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that don't exist on the network.	

No.	Feature	Issue	Workaround/Comments
22.	Compute and Kubernetes	<p>If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it isn't possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.</p>	<p>If your device has 2 GPUs, then you can create one VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available one GPU.</p>
23.	Custom script VM extension	<p>There's a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> - Connect to the Windows VM using remote desktop protocol (RDP). - Make sure that the <code>waappagent.exe</code> is running on the machine: <code>Get-Process WaAppAgent</code> - If the <code>waappagent.exe</code> isn't running, restart the <code>rdagent</code> service: <code>Get-Service RdAgent Restart-Service</code>. Wait for 5 minutes. - While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. - After you kill the process, the process starts running again with the newer version. - Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <code>Get-Process WindowsAzureGuestAgent fl ProductVersion</code>. - Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
24.	GPU VMs	<p>Prior to this release, GPU VM lifecycle wasn't managed in the update flow. Hence, when updating to 2103 release, GPU VMs aren't stopped automatically during the update. You'll need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
25.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting isn't retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>
26.	Wi-Fi	<p>Wi-Fi doesn't work on Azure Stack Edge Pro 2 in this release.</p>	<p>This functionality may be available in a future release.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2202 release notes

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2202 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2202** release, which maps to software version number **2.2.1868.4470**. This software can be applied to your device if you are running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The 2202 release has the following features and enhancements:

- **Introduction of Azure Stack Edge Pro 2** - This release introduces Azure Stack Edge Pro 2, a new generation of an AI-enabled edge computing device offered as a service from Microsoft. For more information, see [What is Azure Stack Edge Pro 2?](#)
- **Clustering support** - This release introduces clustering support for Azure Stack Edge. You can now deploy a two-node device cluster in addition to a single node device. The clustering feature is in preview and is available only for the Azure Stack Edge Pro GPU devices.
For more information, see [What is clustering on Azure Stack Edge?](#).
- **Password reset extension** - Starting this release, password reset extension for both Windows and Linux virtual machines (VMs) are enabled.
- **VM improvements** - A new VM size F12 was added in this release.
- **Multi-Access Edge Computing (MEC) and Virtual Network Functions (VNF) improvements:**
 - In this release, VM create and delete for VNF create and delete were parallelized. This has significantly reduced the creation time for VNFs that contain multiple VMs.
 - The VHD ingestion job resource clean up was moved out of VNF create and delete. This reduced the VNF creation and deletion times.
- **Updates for Azure Arc and Edge container registry** - Azure Arc and Edge container registry versions were updated. For more information, see [About updates](#).
- **Security fixes** - Starting this release, a pod security policy is set up on the Kubernetes cluster on your Azure Stack Edge device. If you are using root privileges in your containerized solution, you may experience some change in the behavior. No action is required on your part.

Issues fixed in 2202 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	Azure Arc	In the previous releases, there was a bug in the proxy implementation that resulted in Azure Arc not functioning properly. In this version, a web proxy bypass list was added to the Azure Arc <i>no_proxy</i> list.

Known issues in 2202 release

The following table provides a summary of known issues in this release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features are available in preview: - Clustering and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU devices only. - VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R only. - Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, and Multi-process service (MPS) for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R.	These features will be generally available in later releases.
2.	Update	For a two-node cluster, in rare instances the update may fail.	If the update fails and you see a message indicating that updates are available, retry updating your device. If the update fails and no updates are available, and your device continues to be in maintenance mode, contact Microsoft Support to determine next steps.
3.	Wi-Fi	Wi-Fi does not work on Azure Stack Edge Pro 2 in this release.	This functionality may be available in a future release.
4.	VPN	VPN feature shows up in the local web UI but this feature is not supported for this device.	This issue will be addressed in a future release.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none"> - In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. - Download <code>sqlcmd</code> on your client machine from SQL command utility. - Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. - Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd".</code> After this, steps 3-4 from the current documentation should be identical.
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. These actions can result in the updated sections of the blob to not get updated in the cloud. <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre data-bbox="1110 1823 1421 2120">hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>

No.	Feature	Issue	Workaround/Comments
4.	Blob Storage ingestion	<p>When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:</p> <pre>Azcopy <other arguments> --cap-mbps 2000</pre>	<p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> - Only block blobs are supported. Page blobs are not supported. - There is no snapshot or copy API support. - Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Kubernetes	<p>Port 31000 is reserved for Kubernetes Dashboard.</p> <p>Port 31001 is reserved for Edge container registry.</p> <p>Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.</p>	Do not use reserved IPs.
10.	Kubernetes	<p>Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.</p>	<p>To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses.</p> <p>For more information, see IP address sharing.</p>
11.	Kubernetes cluster	<p>Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.</p>	<p>For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device.</p>
12.	Kubernetes	<p>File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.</p>	<p>IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.</p>
13.	Kubernetes	<p>If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.</p>	<p>To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands. Restart <code>iotedged</code> and <code>edgehub</code> pods.</p>

No.	Feature	Issue	Workaround/Comments
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
15.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	
16.	Web proxy	NTLM authentication-based web proxy is not supported.	
17.	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
18.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
19.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	<p>To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration.</p>
20.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	

No.	Feature	Issue	Workaround/Comments
21.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
22.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.
23.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> - Connect to the Windows VM using remote desktop protocol (RDP). - Make sure that the <code>waappagent.exe</code> is running on the machine: <code>Get-Process WaAppAgent</code>. - If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <code>Get-Service RdAgent Restart-Service</code>. Wait for 5 minutes. - While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. - After you kill the process, the process starts running again with the newer version. - Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <code>Get-Process WindowsAzureGuestAgent fl ProductVersion</code>. - Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
24.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
25.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2111 release notes

9/21/2022 • 10 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2111 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2111** release, which maps to software version number **2.2.1777.4088**. This software can be applied to your device if you are running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The Azure Stack Edge 2111 release has bug fixes for Multi-Access Edge Compute (MEC) deployments.

Issues fixed in 2111 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	Multi-Access Edge Compute	In previous releases, the Azure Stack Edge device did not send VNF operation results back to the Azure Network Function Manager, owing to the MEC Operation Manager (a component of MEC agent) being reset.
2.	Multi-Access Edge Compute	On Mellanox ConnectX-4 Lx Ethernet Adapter, the maximum number of virtual functions was set to 8 in the earlier releases. Beginning 2111, the default number of virtual functions per port is increased to 32.
3.	Multi-Access Edge Compute	If Azure Stack Edge is running 2106, and a Network Function Device resource is created, the device is then updated to 2110. If you deploy the Network Functions, the deployment will fail. The virtual network is not created after the device is updated to 2110. The failure does not occur if there is an existing Network Functions deployment on Azure Stack Edge.

NO.	FEATURE	ISSUE
4.	Multi-Access Edge Compute	Azure Stack Edge was updated to version 2110 while the Network Functions VMs were running. In these instances, the update may fail with the following error in the event log: <i>The network interface "Mellanox ConnectX-4 Lx Ethernet Adapter" has begun resetting. There will be a momentary disruption in network connectivity while the hardware resets. Reason: The network driver did not respond to an OID request in a timely fashion. This network interface has reset 3 time(s) since it was last initialized.</i>

Known issues in 2111 release

The following table provides a summary of known issues in the 2111 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS), and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ol style="list-style-type: none"> 1. In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. 2. Download <code>sqlcmd</code> on your client machine from SQL command utility. 3. Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. 4. Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre data-bbox="1128 1275 1414 1349">hcsuser@ubuntu-vm:~/nfstest\$ mkdir test</pre> <p>mkdir: cannot create directory 'test': Permission denied</p>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: <pre data-bbox="810 1626 1080 1700">Azcopy <other arguments> --cap-mbps 2000</pre>	If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Kubernetes	<p>Port 31000 is reserved for Kubernetes Dashboard.</p> <p>Port 31001 is reserved for Edge container registry.</p> <p>Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.</p>	Do not use reserved IPs.
10.	Kubernetes	<p>Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.</p>	<p>To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses.</p> <p>For more information, see IP address sharing.</p>
11.	Kubernetes cluster	<p>Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.</p>	<p>For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device.</p>
12.	Kubernetes	<p>File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.</p>	<p>IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.</p>
13.	Kubernetes	<p>If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.</p>	<p>To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands. Restart <code>iotedged</code> and <code>edgehub</code> pods.</p>

No.	Feature	Issue	Workaround/Comments
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
15.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	
16.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
17.	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
18.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
19.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	<p>To allow the deletion of resources when they're deleted from the git repository, set</p> <div style="border: 1px solid black; padding: 2px;"><code>--sync-garbage-collection</code></div> <p>in Arc OperatorParams. For more information, see Delete a configuration.</p>
20.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
21.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
22.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.

No.	Feature	Issue	Workaround/Comments
23.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ol style="list-style-type: none"> 1. Connect to the Windows VM using remote desktop protocol (RDP). 2. Make sure that the <code>waappagent.exe</code> is running on the machine: <pre>Get-Process WaAppAgent</pre> 3. If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <pre>Get-Service RdAgent Restart-Service</pre> Wait for 5 minutes. 4. While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. 5. After you kill the process, the process starts running again with the newer version. 6. Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <pre>Get-Process WindowsAzureGuestAgent f1 ProductVersion</pre> 7. Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
24.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
25.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2110 release notes

9/21/2022 • 13 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2110 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2110** release, which maps to software version number **2.2.1758.4034**. This software can be applied to your device if you are running at least Azure Stack Edge 2106 (2.2.1636.3457) software.

What's new

The following new features are available in the Azure Stack Edge 2110 release.

- **Windows updates and security fixes** - The [latest cumulative update \(LCU\) for Windows and September security fixes](#) were rolled into the updates package for Azure Stack Edge.
- **Remote support** - In this release, you can enable remote support on your Azure Stack Edge device to allow Microsoft Support to diagnose and remediate issues by accessing your device remotely. When you enable this feature, you provide consent for the level of access and the duration of access. For more information, see [Enable remote support and diagnostics for Azure Stack Edge](#).
- **High-performance network virtual machines** - Beginning this release, high-performance network virtual machines can be deployed on your Azure Stack Edge device. For more information, see [Deploy high-performance network virtual machines on Azure Stack Edge](#).
- **Certificates for Edge container registry and Kubernetes dashboard** - Certificates for Edge container registry and Kubernetes dashboard are now supported. You can create and upload certificates via the local UI. For more information, see [Kubernetes certificates](#) and [Upload Kubernetes certificates](#).
- **Metallb in BGP mode** - Starting this release, you can configure load balancing on your Azure Stack Edge device using MetalLB via Border Gateway Protocol (BGP). Configuration is done by connecting to the PowerShell interface of the device and then running specific cmdlets. For more information, see [Configure load balancing with MetalLB on your Azure Stack Edge device](#).

Issues fixed in 2110 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
-----	---------	-------

No.	Feature	Issue
1.	Azure Arc enabled Kubernetes	For the GA release, Azure Arc enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc enabled Kubernetes.
2.	Azure Arc enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.
3.	IoT Edge	Modules deployed through IoT Edge can't use host network.
4.	Kubernetes + update	Earlier software versions such as 2008 releases have a race condition update issue that causes the update to fail with ClusterConnectionException.
5.	Kubernetes Dashboard	<i>Https</i> endpoint for Kubernetes Dashboard with SSL certificate is not supported.
6.	VMs	Static IP duplication check is added for VM management NIC during VNF deployment. Explicit error message is returned.
7.	VMs	IP reservation check was removed for first four IP addresses in address space.
8.	Multi-Access Edge Compute	Fixed local Azure Resource Manager token expiration issue during VNF deployment. In earlier releases, when VHD download took a long time, the VNF deployment would fail as the Azure Resource Manager token would expire.
9.	Multi-Access Edge Compute	A timeout was added for Azure Resource Manager calls during VNF deployment. In earlier releases, VNF deployment took a long time, if Azure Resource Manager calls were not successful.
10.	Multi-Access Edge Compute	Multi-Access Edge Compute cleans up Azure Resource Manager template deployments after VHD download completes. In earlier releases, the user would hit deployment quota exceeded error after many VNF deployments. Default quota was 800 deployments per resource group.

Known issues in 2110 release

The following table provides a summary of known issues in the 2110 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS), and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.
2.	Certificates	Alerts related to signing chain certificates aren't removed from the portal even after uploading new signing chain certificates.	

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
-----	---------	-------	---------------------

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ol style="list-style-type: none"> 1. In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. 2. Download <code>sqlcmd</code> on your client machine from SQL command utility. 3. Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. 4. Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ol style="list-style-type: none"> 1. Create blob in cloud. Or delete a previously uploaded blob from the device. 2. Refresh blob from the cloud into the appliance using the refresh functionality. 3. Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre data-bbox="1133 1275 1425 1356">hcsuser@ubuntu-vm:~/nfstest\$ mkdir test</pre> <p>mkdir: cannot create directory 'test': Permission denied</p>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: <pre data-bbox="815 1626 1101 1702">Azcopy <other arguments> --cap-mbps 2000</pre>	If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Kubernetes	<p>Port 31000 is reserved for Kubernetes Dashboard.</p> <p>Port 31001 is reserved for Edge container registry.</p> <p>Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.</p>	Do not use reserved IPs.
10.	Kubernetes	<p>Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.</p>	<p>To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses.</p> <p>For more information, see IP address sharing.</p>
11.	Kubernetes cluster	<p>Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.</p>	<p>For more information, see Run existing IoT Edge modules from Azure Stack Edge Pro FPGA devices on Azure Stack Edge Pro GPU device.</p>
12.	Kubernetes	<p>File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.</p>	<p>IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.</p>
13.	Kubernetes	<p>If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.</p>	<p>To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands. Restart <code>iotedged</code> and <code>edgehub</code> pods.</p>

No.	Feature	Issue	Workaround/Comments
14.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
15.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
16	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.
17.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event Grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
18.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	<p>To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration.</p>
19.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
20.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	

No.	Feature	Issue	Workaround/Comments
21.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.
22.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ol style="list-style-type: none"> 1. Connect to the Windows VM using remote desktop protocol (RDP). 2. Make sure that the <code>waappagent.exe</code> is running on the machine: <code>Get-Process WaAppAgent</code> 3. If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <code>Get-Service RdAgent Restart-Service</code>. Wait for 5 minutes. 4. While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. 5. After you kill the process, the process starts running again with the newer version. 6. Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <code>Get-Process WindowsAzureGuestAgent fl ProductVersion</code> 7. Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
23.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
24.	Multi-Process Service (MPS)	When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

No.	Feature	Issue	Workaround/Comments
25.	Multi-Access Edge Compute (MEC)	<p>If Azure Stack Edge is running 2106, and a Network Function Device resource is created and the Azure Stack Edge is then updated to 2110, when you deploy the Network Function, the deployment will fail. The virtual network is not being created after the device is updated to 2110. The failure does not occur if there is an existing Network Function deployment on Azure Stack Edge.</p>	<p>To work around this issue, re-register the same device resource using the Invoke-MecRegister cmdlet on your Azure Stack Edge and use the activation key from the Azure Stack Edge resource. Alternatively, you can create virtual switches via the following commands:</p> <ul style="list-style-type: none"> • <pre>Add-HcsExternalVirtualSwitch -InterfaceAlias Port5 - WaitForSwitchCreation \$true - switchName mec-vswitch-LAN - SupportsAcceleratedNetworking \$true</pre> • <pre>Add-HcsExternalVirtualSwitch -InterfaceAlias Port6 - WaitForSwitchCreation \$true - switchName mec-vswitch-WAN - SupportsAcceleratedNetworking \$true</pre>
26.	Multi-Access Edge Compute (MEC)	<p>Azure Stack Edge was updated to version 2110 while the Network Functions VMs were running. In these instances, the update may fail when trying to stop the virtual machines that are connected to the Mellanox Ethernet adapter. The following error is seen in the event log: <i>The network interface "Mellanox ConnectX-4 Lx Ethernet Adapter" has begun resetting. There will be a momentary disruption in network connectivity while the hardware resets.</i> Reason: <i>The network driver did not respond to an OID request in a timely fashion. This network interface has reset 3 time(s) since it was last initialized.</i></p>	<p>To work around this issue, reboot your Azure Stack Edge and retry updating the device.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2106 release notes

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2106 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2106** release, which maps to software version number **2.2.1636.3457**. This software can be applied to your device if you are running at least Azure Stack Edge 2010 (2.1.1377.2170) software.

What's new

The following new features are available in the Azure Stack Edge 2106 release.

- **Windows updates and security fixes** - The [latest cumulative update \(LCU\) for Windows and June security fixes](#) were rolled into the updates package for Azure Stack Edge.
- **Bug fixes for Azure Private Multi-Access Edge Compute** - Multiple issues were fixed for Azure Private MEC deployments.
 - Issues related to guest VM health monitoring such as link flapping, errors in boot log, and reboots.
 - Memory resource consumption over time.
 - Mellanox driver, firmware, and tools.
 - Tools to debug VM-related issues and network health check.
 - Issues that caused Single root I/O virtualization (SR-IOV) VM outbound packets or the traffic from LAN/WAN VM NetAdapters to be dropped.
- **Log collection improvements** - This release has log collection improvements related to Azure Stack Edge update scenarios.

Issues fixed in 2106 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	Azure Private MEC	VM net adapter link status flaps at boot time and periodically.
2.	Azure Private MEC	VFToPF DHCP redirect flag when used on Mellanox network interfaces can cause the packets to be dropped.

NO.	FEATURE	ISSUE
3.	Azure Private MEC	The Mellanox network interface driver, firmware, and tools need to be upgraded to version 2.60.
4.	VM	The cmdlet <code>Get-VMGuestLogs</code> available for the collection of VM guest logs when connecting via the PowerShell interface of the device fails.
5.	Azure Private MEC	When web proxy is configured, the web proxy bypass setting causes VM provisioning failure.
6.	Azure Private MEC	For MEC/NFM deployments prior to the 2105 update, you may face this rare issue where traffic from LAN/WAN VM NetAdapters is dropped. In 2106, this issue is fixed by setting the enableIPForwarding to true on VM LAN/WAN network interfaces, regardless of whether the VMs were created before 2105 or after 2105 release.
7.	Azure Private MEC	Single root I/O virtualization (SR-IOV) VM's outbound packets may be dropped by the Mellanox network interfaces (Port 5 and Port 6 on the device) when a combination of Mellanox driver, SR-IOV Virtual Functions (VF) and vftopfDHCPRedirect feature is used. In 2106, the issue is fixed by disabling the vftopfDHCPRedirect feature.

Known issues in 2106 release

The following table provides a summary of known issues in the 2106 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, Azure Arc-enabled Kubernetes, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS), and Multi-Access Edge Computing (MEC) for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none">• In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply.• Download <code>sqlcmd</code> on your client machine from SQL command utility.• Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address.• Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:	<pre>Azcopy <other arguments> --cap-mbps 2000</pre> <p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Azure Arc-enabled Kubernetes	For the GA release, Azure Arc-enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc-enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc-enabled Kubernetes.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Apply device software and Kubernetes updates. 2. Connect to the PowerShell interface of the device. 3. Remove the existing Azure Arc agent. Type: <code>Remove-HcsKubernetesAzureArcAgent</code> 4. Deploy Azure Arc to a new resource. Do not use an existing Azure Arc resource.
10.	Azure Arc-enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.	
11.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Do not use reserved IPs.
12.	Kubernetes	Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
13.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device .

No.	Feature	Issue	Workaround/Comments
14.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.
15.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedge</code> and <code>edgehub</code> pods.
16.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
17.	IoT Edge	Modules deployed through IoT Edge can't use host network.	
18.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
19.	Kubernetes + update	Earlier software versions such as 2008 releases have a race condition update issue that causes the update to fail with <code>ClusterConnectionException</code> .	Using the newer builds should help avoid this issue. If you still see this issue, the workaround is to retry the upgrade, and it should work.
20	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.

No.	Feature	Issue	Workaround/Comments
21.	Kubernetes Dashboard	<i>Https</i> endpoint for Kubernetes Dashboard with SSL certificate is not supported.	
22.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
23.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
24.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
25.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
26.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.

No.	Feature	Issue	Workaround/Comments
27.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> • Connect to the Windows VM using remote desktop protocol (RDP). • Make sure that the <code>waappagent.exe</code> is running on the machine: <pre>Get-Process WaAppAgent</pre> • If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <pre>Get-Service RdAgent Restart-Service</pre> Wait for 5 minutes. • While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. • After you kill the process, the process starts running again with the newer version. • Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <pre>Get-Process WindowsAzureGuestAgent f1 ProductVersion</pre> • Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
28.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
29.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2105 release notes

9/21/2022 • 12 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2105 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2105** release, which maps to software version number **2.2.1606.3320**. This software can be applied to your device if you are running at least Azure Stack Edge 2010 (2.1.1377.2170) software.

What's new

The following new features are available in the Azure Stack Edge 2105 release.

- **Virtual Local Area Network (VLAN) configuration support** - In this release, the virtual local area network (VLAN) configuration can be changed by connecting to the PowerShell interface of the device. For more information, see [Create vLANS on virtual switch](#).
- **IP Forwarding support** - Beginning this release, IP forwarding is supported for network interfaces attached to Virtual Machines (VMs).
 - IP forwarding enables VMs to receive network traffic from an IP not assigned to any of the IP configurations assigned to a network interface on the VM.
 - IP forwarding also lets VMs send network traffic with a different source IP address than the one assigned to the IP configurations for the VM's network interface.For more information, see [Enable or disable IP forwarding](#).
- **Kubernetes improvements** - In this release, several enhancements related to Kubernetes have been made.
 - The following Kubernetes version updates are available:
 - Kubernetes server version: v1.20.2
 - IoT Edge version: 0.1.0-beta14
 - Azure Arc-enabled Kubernetes version: 1.1
 - Azure Arc-enabled Kubernetes now has support for various clouds, logging is improved and the cmdlet experience via the PowerShell interface has changed.
 - Diagnostics and telemetry fixes have been made.
 - Proactive log collection is enhanced for compute logs.
- **Support for Az cmdlets** - Starting this release, the Az cmdlets are available (in preview) when connecting to the local Azure Resource Manager of the device or when deploying VM workloads. For more information, see [Az cmdlets](#).

- **Enable remote PowerShell session over HTTP** - Starting this release, you can enable a remote PowerShell session into a device over *http* via the local UI. For more information, see how to [Enable Remote PowerShell over http](#) for your device.

Issues fixed in 2105 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	VM	Failure during DHCP lease renewal should not cause network interface record to be removed.
2.	VM	Monitoring improvements to resolve locking issue when provisioning VMs.

Known issues in 2105 release

The following table provides a summary of known issues in the 2105 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, Azure Arc-enabled Kubernetes, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS), Network Function Manager for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
2.	Multi-access Edge Compute (MEC)/Network Function Manager (NFM) deployments	<p>For MEC/NFM deployments prior to the 2105 update, you may face this rare issue where traffic from LAN/WAN VM NetAdapters is dropped.</p> <p>On your Azure Stack Edge device, Port 5 and Port 6 are connected to the Mellanox network interface card that allows for accelerated networking. The accelerated networking allows the LAN/WAN traffic from Port 5 and Port 6 to bypass the hypervisor layer and the virtual switch, and directly reach the physical switch.</p> <p>You can disable the accelerated networking by disabling the Virtual Functions (VF) device on the LAN/WAN network interfaces. All the networking traffic from the VMs will now traverse the hypervisor layer that performs security checks. If your application sends traffic using arbitrary unicast source IP address (which is not the IP for VM NetAdapter), the security checks cause the traffic to be dropped (as it seems to be originating from arbitrary IPs that aren't specified in the Virtual Networking Functions contract).</p>	<p>To work around this problem, you can hold off on the 2105 update and wait for the next release that has a fix for this issue.</p> <p>Alternatively, you could apply the 2105 update on your Azure Stack Edge device and redeploy the same VNF. The VNFs that are deployed after the 2105 update do not require the fix.</p>

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
-----	---------	-------	---------------------

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Create-the-sql-database.</p> <ul style="list-style-type: none"> In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. Download <code>sqlcmd</code> on your client machine from SQL command utility. Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. Final command will look like this: <code>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</code>. After this, steps 3-4 from the current documentation should be identical.

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: Azcopy <other arguments> --cap-mbps 2000	If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Azure Arc-enabled Kubernetes	For the GA release, Azure Arc-enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc-enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc-enabled Kubernetes.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Apply device software and Kubernetes updates. 2. Connect to the PowerShell interface of the device. 3. Remove the existing Azure Arc agent. Type: <code>Remove-HcsKubernetesAzureArcAgent</code> 4. Deploy Azure Arc to a new resource. Do not use an existing Azure Arc resource.
10.	Azure Arc-enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.	
11.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Do not use reserved IPs.
12.	Kubernetes	Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
13.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device .

No.	Feature	Issue	Workaround/Comments
14.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.
15.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedge</code> and <code>edgehub</code> pods.
16.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
17.	IoT Edge	Modules deployed through IoT Edge can't use host network.	
18.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
19.	Kubernetes + update	Earlier software versions such as 2008 releases have a race condition update issue that causes the update to fail with <code>ClusterConnectionException</code> .	Using the newer builds should help avoid this issue. If you still see this issue, the workaround is to retry the upgrade, and it should work.
20	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.

No.	Feature	Issue	Workaround/Comments
21.	Kubernetes Dashboard	<i>Https</i> endpoint for Kubernetes Dashboard with SSL certificate is not supported.	
22.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
23.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
24.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
25.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
26.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.

No.	Feature	Issue	Workaround/Comments
27.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> • Connect to the Windows VM using remote desktop protocol (RDP). • Make sure that the <code>waappagent.exe</code> is running on the machine: <pre>Get-Process WaAppAgent</pre> • If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <pre>Get-Service RdAgent Restart-Service</pre> Wait for 5 minutes. • While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. • After you kill the process, the process starts running again with the newer version. • Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <pre>Get-Process WindowsAzureGuestAgent f1 ProductVersion</pre> • Set up custom script extension on Windows VM.

No.	Feature	Issue	Workaround/Comments
28.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>
29.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

Next steps

- [Update your device](#)

Azure Stack Edge 2103 release notes

9/21/2022 • 11 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2103 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2103** release, which maps to software version number **2.2.1540.2890**. This software can be applied to your device if you are running at least Azure Stack Edge 2010 (2.1.1377.2170) software.

What's new

The following new features are available in the Azure Stack Edge 2103 release.

- **New features for Virtual Machines** - Beginning this release, you can perform the following management operations on the virtual machines via the Azure portal:
 - Add or remove multiple network interfaces to an existing VM.
 - Add or remove multiple disks to an existing VM.
 - Resize the VM.
 - Add custom data while deploying a Windows or a Linux VM.You can also [Connect to the VM console on your device](#) and troubleshoot any VM issues.
- **Connect to PowerShell interface via https** - Starting this release, you will no longer be able to open a remote PowerShell session into a device over *http*. By default, *https* will be used for all the sessions. For more information, see how to [Connect to the PowerShell interface](#) of your device.
- **Improvements for Compute** - Several enhancements and improvements were made including those for:
 - **Overall compute platform quality.** This release has bug fixes to improve the overall compute platform quality. See the [Issues fixed in 2103 release](#).
 - **Compute platform components.** Security updates were applied to Compute VM image. IoT Edge and Azure Arc for Kubernetes versions were also updated.
 - **Diagnostics.** A new API is released to check resource and network conditions. You can connect to the PowerShell interface of the device and use the `Test-HcsKubernetesStatus` command to verify the network readiness of the device.
 - **Log collection** that would lead to improved debugging.
 - **Alerting infrastructure** that will allow you to detect IP address conflicts for compute IP addresses.
 - **Mix workload** of Kubernetes and local Azure Resource Manager.
- **Proactive logging by default** - Starting this release, proactive log collection is enabled by default on your device. This feature allows Microsoft to collect logs proactively based on the system health indicators to help efficiently troubleshoot any device issues. For more information, see [Proactive log](#)

collection on your device.

Issues fixed in 2103 release

The following table lists the issues that were release noted in previous releases and fixed in the current release.

NO.	FEATURE	ISSUE
1.	Kubernetes	Edge container registry does not work when web proxy is enabled.
2.	Kubernetes	Edge container registry does not work with IoT Edge modules.

Known issues in 2103 release

The following table provides a summary of known issues in the 2103 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Kubernetes cloud management, Azure Arc-enabled Kubernetes, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS) for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.

No.	Feature	Issue	Workaround/Comments
2.	GPU VMs	<p>Prior to this release, GPU VM lifecycle was not managed in the update flow. Hence, when updating to 2103 release, GPU VMs are not stopped automatically during the update. You will need to manually stop the GPU VMs using a <code>stop-stayProvisioned</code> flag before you update your device. For more information, see Suspend or shut down the VM.</p> <p>All the GPU VMs that are kept running before the update, are started after the update. In these instances, the workloads running on the VMs aren't terminated gracefully. And the VMs could potentially end up in an undesirable state after the update.</p> <p>All the GPU VMs that are stopped via the <code>stop-stayProvisioned</code> before the update, are automatically started after the update.</p> <p>If you stop the GPU VMs via the Azure portal, you'll need to manually start the VM after the device update.</p>	<p>If running GPU VMs with Kubernetes, stop the GPU VMs right before the update.</p> <p>When the GPU VMs are stopped, Kubernetes will take over the GPUs that were used originally by VMs.</p> <p>The longer the GPU VMs are in stopped state, higher the chances that Kubernetes will take over the GPUs.</p>

No.	Feature	Issue	Workaround/Comments
3.	Custom script VM extension	<p>There is a known issue in the Windows VMs that were created in an earlier release and the device was updated to 2103. If you add a custom script extension on these VMs, the Windows VM Guest Agent (Version 2.7.41491.901 only) gets stuck in the update causing the extension deployment to time out.</p>	<p>To work around this issue:</p> <ul style="list-style-type: none"> Connect to the Windows VM using remote desktop protocol (RDP). Make sure that the <code>waappagent.exe</code> is running on the machine: <pre>Get-Process WaAppAgent</pre> If the <code>waappagent.exe</code> is not running, restart the <code>rdagent</code> service: <pre>Get-Service RdAgent Restart-Service</pre> Wait for 5 minutes. While the <code>waappagent.exe</code> is running, kill the <code>WindowsAzureGuest.exe</code> process. After you kill the process, the process starts running again with the newer version. Verify that the Windows VM Guest Agent version is 2.7.41491.971 using this command: <pre>Get-Process WindowsAzureGuestAgent f1 ProductVersion</pre> Set up custom script extension on Windows VM.
4.	Multi-Process Service (MPS)	<p>When the device software and the Kubernetes cluster are updated, the MPS setting is not retained for the workloads.</p>	<p>Re-enable MPS and redeploy the workloads that were using MPS.</p>

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Tutorial: Store data at the edge with SQL Server databases.</p> <ul style="list-style-type: none"> In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. Download <code>sqlcmd</code> on your client machine from sqlcmd Utility Connect to your compute interface IP address (the port that was enabled), adding a <code>,1401</code> to the end of the address. Final command will look like this: <pre>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</pre> <p>After this, steps 3-4 from the current documentation should be identical.</p>

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument:	<pre>Azcopy <other arguments> --cap-mbps 2000</pre> <p>If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.</p>

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Azure Arc-enabled Kubernetes	For the GA release, Azure Arc-enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc-enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc-enabled Kubernetes.	Follow these steps: <ol style="list-style-type: none"> 1. Apply device software and Kubernetes updates. 2. Connect to the PowerShell interface of the device. 3. Remove the existing Azure Arc agent. Type: <code>Remove-HcsKubernetesAzureArcAgent</code> 4. Deploy Azure Arc to a new resource. Do not use an existing Azure Arc resource.
10.	Azure Arc-enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.	
11.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Do not use reserved IPs.
12.	Kubernetes	Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
13.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device .

No.	Feature	Issue	Workaround/Comments
14.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.
15.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedge</code> and <code>edgehub</code> pods.
16.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
17.	IoT Edge	Modules deployed through IoT Edge can't use host network.	
18.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
19.	Kubernetes + update	Earlier software versions such as 2008 releases have a race condition update issue that causes the update to fail with <code>ClusterConnectionException</code> .	Using the newer builds should help avoid this issue. If you still see this issue, the workaround is to retry the upgrade, and it should work.
20	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
21.	Kubernetes Dashboard	<i>Https</i> endpoint for Kubernetes Dashboard with SSL certificate is not supported.	
22.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
23.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
24.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	
25.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
26.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.

Next steps

- [Update your device](#)

Azure Stack Edge 2101 release notes

9/21/2022 • 9 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

The following release notes identify the critical open issues and the resolved issues for the 2101 release for your Azure Stack Edge devices. These release notes are applicable for Azure Stack Edge Pro GPU, Azure Stack Edge Pro R, and Azure Stack Edge Mini R devices. Features and issues that correspond to a specific model are called out wherever applicable.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge 2101** release, which maps to software version number **2.2.1473.2521**.

What's new

The following new features are available in the Azure Stack Edge 2101 release.

- **General availability of Azure Stack Edge Pro R and Azure Stack Edge Mini R devices** - Starting with this release, Azure Stack Edge Pro R and Azure Stack Edge Mini R devices will be available. For more information, see [What is Azure Stack Edge Pro R](#) and [What is Azure Stack Edge Mini R](#).
- **Cloud management of Virtual Machines** - Beginning this release, you can create and manage the virtual machines on your device via the Azure portal. For more information, see [Deploy VMs via the Azure portal](#).
- **Integration with Azure Monitor** - You can now use Azure Monitor to monitor containers from the compute applications that run on your device. The Azure Monitor metrics store is not supported in this release. For more information, see how to [Enable Azure Monitor on your device](#).
- **Edge container registry** - In this release, an Edge container registry is available that provides a repository at the edge on your device. You can use this registry to store and manage container images. For more information, see [Enable Edge container registry](#).
- **Virtual Private Network (VPN)** - Use VPN to provide another layer of encryption for the data that flows between the devices and the cloud. VPN is available only on Azure Stack Edge Pro R and Azure Stack Edge Mini R. For more information, see how to [Configure VPN on your device](#).
- **Rotate encryption-at-rest keys** - You can now rotate the encryption-at-rest keys that are used to protect the drives on your device. This feature is available only for Azure Stack Edge Pro R and Azure Stack Edge Mini R devices. For more information, see [Rotate encryption-at-rest keys](#).
- **Proactive logging** - Starting this release, you can enable proactive log collection on your device based on the system health indicators to help efficiently troubleshoot any device issues. For more information, see [Proactive log collection on your device](#).

Known issues in 2101 release

The following table provides a summary of known issues in the 2101 release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
-----	---------	-------	---------------------

No.	Feature	Issue	Workaround/Comments
1.	Preview features	For this release, the following features: Local Azure Resource Manager, VMs, Cloud management of VMs, Azure Arc-enabled Kubernetes, VPN for Azure Stack Edge Pro R and Azure Stack Edge Mini R, Multi-process service (MPS) for Azure Stack Edge Pro GPU - are all available in preview.	These features will be generally available in later releases.
2.	Kubernetes Dashboard	<i>Https</i> endpoint for Kubernetes Dashboard with SSL certificate is not supported.	
3.	Kubernetes	Edge container registry does not work when web proxy is enabled.	The functionality will be available in a future release.
4.	Kubernetes	Edge container registry does not work with IoT Edge modules.	
5.	Kubernetes	Kubernetes doesn't support ":" in environment variable names that are used by .NET applications. This is also required for Event grid IoT Edge module to function on Azure Stack Edge device and other applications. For more information, see ASP.NET core documentation .	Replace ":" by double underscore. For more information, see Kubernetes issue
6.	Azure Arc + Kubernetes cluster	By default, when resource <code>yamls</code> are deleted from the Git repository, the corresponding resources are not deleted from the Kubernetes cluster.	To allow the deletion of resources when they're deleted from the git repository, set <code>--sync-garbage-collection</code> in Arc OperatorParams. For more information, see Delete a configuration .
7.	NFS	Applications that use NFS share mounts on your device to write data should use Exclusive write. That ensures the writes are written to the disk.	

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
8.	Compute configuration	Compute configuration fails in network configurations where gateways or switches or routers respond to Address Resolution Protocol (ARP) requests for systems that do not exist on the network.	
9.	Compute and Kubernetes	If Kubernetes is set up first on your device, it claims all the available GPUs. Hence, it is not possible to create Azure Resource Manager VMs using GPUs after setting up the Kubernetes.	If your device has 2 GPUs, then you can create 1 VM that uses the GPU and then configure Kubernetes. In this case, Kubernetes will use the remaining available 1 GPU.

Known issues from previous releases

The following table provides a summary of known issues carried over from the previous releases.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
-----	---------	-------	---------------------

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Tutorial: Store data at the edge with SQL Server databases.</p> <ul style="list-style-type: none"> In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. Download <code>sqlcmd</code> on your client machine from sqlcmd Utility Connect to your compute interface IP address (the port that was enabled), adding a <code>,1401</code> to the end of the address. Final command will look like this: <pre>sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd"</pre> <p>After this, steps 3-4 from the current documentation should be identical.</p>

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes to the device aren't allowed, writes by the NFS client fail with a "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: <code>Azcopy <other arguments> --cap-mbps 2000</code>	If these limits aren't provided for AzCopy, it could potentially send a large number of requests to the device, resulting in issues with the service.

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute isn't used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside a replication controller without specifying a replica set, these pods won't be restored automatically after the device update. You will need to restore these pods. A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
9.	Azure Arc-enabled Kubernetes	For the GA release, Azure Arc-enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc-enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc-enabled Kubernetes.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Apply device software and Kubernetes updates. 2. Connect to the PowerShell interface of the device. 3. Remove the existing Azure Arc agent. Type: <code>Remove-HcsKubernetesAzureArcAgent</code> 4. Deploy Azure Arc to a new resource. Do not use an existing Azure Arc resource.
10.	Azure Arc-enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.	
11.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Port 31001 is reserved for Edge container registry. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Do not use reserved IPs.
12.	Kubernetes	Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
13.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device .

No.	Feature	Issue	Workaround/Comments
14.	Kubernetes	File-based bind mounts aren't supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.
15.	Kubernetes	If you bring your own certificates for IoT Edge and add those certificates on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedge</code> and <code>edgehub</code> pods.
16.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
17.	IoT Edge	Modules deployed through IoT Edge can't use host network.	
18.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
19.	Kubernetes + update	Earlier software versions such as 2008 releases have a race condition update issue that causes the update to fail with <code>ClusterConnectionException</code> .	Using the newer builds should help avoid this issue. If you still see this issue, the workaround is to retry the upgrade, and it should work.
20	Internet Explorer	If enhanced security features are enabled, you may not be able to access local web UI pages.	Disable enhanced security, and restart your browser.

Next steps

- [Update your device](#)

Azure Stack Edge Pro with GPU General Availability (GA) release notes

9/21/2022 • 7 minutes to read • [Edit Online](#)

APPLIES TO:  Azure Stack Edge Pro - GPU

The following release notes identify the critical open issues and the resolved issues for general availability (GA) release for your Azure Stack Edge Pro devices with GPU.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Azure Stack Edge Pro device, carefully review the information contained in the release notes.

This article applies to the **Azure Stack Edge Pro 2010** release which maps to software version number **2.1.1377.2170**.

What's new

The following new features are available in the Azure Stack Edge 2010 release.

- **Storage classes** - In this release, Storage classes are available that let you dynamically provision storage. For more information, see [Kubernetes storage management on your Azure Stack Edge Pro GPU device](#).
- **Kubernetes dashboard with metrics server** - In this release, a Kubernetes Dashboard is added with a metrics server add-on. You can use the dashboard to get an overview of the applications running on your Azure Stack Edge Pro device, view status of Kubernetes cluster resources, and see any errors that have occurred on the device. The Metrics server aggregates the CPU and memory usage across Kubernetes resources on the device. For more information, see [Use Kubernetes dashboard to monitor your Azure Stack Edge Pro GPU device](#).
- **Azure Arc-enabled Kubernetes on Azure Stack Edge Pro** - Beginning this release, you can deploy application workloads on your Azure Stack Edge Pro device via Azure Arc-enabled Kubernetes. Azure Arc is a hybrid management tool that allows you to deploy applications on your Kubernetes clusters. For more information, see [Deploy workloads via Azure Arc on your Azure Stack Edge Pro device](#).

Known issues

The following table provides a summary of known issues for the Azure Stack Edge Pro device.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
1.	Preview features	For this GA release, the following features: Local Azure Resource Manager, VMs, Kubernetes, Azure Arc-enabled Kubernetes, Multi-Process service (MPS) for GPU - are all available in preview for your Azure Stack Edge Pro device.	These features will be generally available in a later release.

No.	Feature	Issue	Workaround/Comments
2.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Tutorial: Store data at the edge with SQL Server databases.</p> <ul style="list-style-type: none"> • In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. • Download sqlcmd utility on your client machine. • Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. • Final command will look like this: sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd". <p>After this, steps 3-4 from the current documentation should be identical.</p>

No.	Feature	Issue	Workaround/Comments
3.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
4.	Throttling	During throttling, if new writes are not allowed into the device, writes done by NFS client fail with "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
5.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: Azcopy <other arguments> --cap-mbps 2000	If these limits are not provided for AzCopy, then it could potentially send a large number of requests to the device and result in issues with the service.

No.	Feature	Issue	Workaround/Comments
6.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
7.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute is not used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
8.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside of a replication controller without specifying a replica set, then these pods will not be automatically restored after the device update. You will need to restore these pods.</p> <p>A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
9.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	

No.	Feature	Issue	Workaround/Comments
10.	Azure Arc-enabled Kubernetes	For the GA release, Azure Arc-enabled Kubernetes is updated from version 0.1.18 to 0.2.9. As the Azure Arc-enabled Kubernetes update is not supported on Azure Stack Edge device, you will need to redeploy Azure Arc-enabled Kubernetes.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Apply device software and Kubernetes updates. 2. Connect to the PowerShell interface of the device. 3. Remove the existing Azure Arc agent. Type: <code>Remove-HcsKubernetesAzureArcAgent</code> 4. Deploy Azure Arc to a new resource. Do not use an existing Azure Arc resource.
11.	Azure Arc-enabled Kubernetes	Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.	
12.	Kubernetes	Port 31000 is reserved for Kubernetes Dashboard. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.	Do not use reserved IPs.
13.	Kubernetes	Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.	To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing .
14.	Kubernetes cluster	Existing Azure IoT Edge marketplace modules may require modifications to run on IoT Edge on Azure Stack Edge device.	For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device .

No.	Feature	Issue	Workaround/Comments
15.	Kubernetes	File-based bind mounts are not supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.	IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory and thus file-based bind mounts cannot be bound to paths in IoT Edge containers. If possible, map the parent directory.
16.	Kubernetes	If you bring your own certificates for IoT Edge and add those on your Azure Stack Edge device after the compute is configured on the device, the new certificates are not picked up.	To work around this problem, you should upload the certificates before you configure compute on the device. If the compute is already configured, Connect to the PowerShell interface of the device and run IoT Edge commands . Restart <code>iotedge</code> and <code>edgehub</code> pods.
17.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.
17.	IoT Edge	Modules deployed through IoT Edge can't use host network.	
18.	Compute + Kubernetes	Compute/Kubernetes does not support NTLM web proxy.	
19.	Compute + web proxy + update	If you have compute configured with web proxy, then compute update may fail.	We recommend that you disable compute before the update.

Next steps

- [Prepare to deploy Azure Stack Edge Pro device with GPU](#)

Azure Stack Edge Pro with GPU Preview release notes

9/21/2022 • 6 minutes to read • [Edit Online](#)

APPLIES TO:  Azure Stack Edge Pro - GPU

The following release notes identify the critical open issues and the resolved issues for 2008 preview release for your Azure Stack Edge Pro devices with GPU.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Azure Stack Edge Pro device, carefully review the information contained in the release notes.

This article applies to the following software release - **Azure Stack Edge Pro 2008**.

What's new

The following new features were added in Azure Stack Edge 2008 release. Depending on the specific preview software version you are running, you may see a subset of these features.

- **Storage classes** - In the previous release, you could only statically provision storage via SMB or NFS shares for stateful applications deployed on the Kubernetes cluster running on your Azure Stack Edge Pro device. In this release, Storage classes were added that let dynamically provision storage. For more information, see [Kubernetes storage management on your Azure Stack Edge Pro GPU device](#).
- **Kubernetes dashboard with metrics server** - In this release, a Kubernetes Dashboard is added with a metrics server add-on. You can use the dashboard to get an overview of the applications running on your Azure Stack Edge Pro device, view status of Kubernetes cluster resources, and see any errors that have occurred on the device. The Metrics server aggregates the CPU and memory usage across Kubernetes resources on the device. For more information, see [Use Kubernetes dashboard to monitor your Azure Stack Edge Pro GPU device](#).
- **Azure Arc for Azure Stack Edge Pro** - Beginning this release, you can deploy application workloads on your Azure Stack Edge Pro device via Azure Arc. Azure Arc is a hybrid management tool that allows you to deploy applications on your Kubernetes clusters. For more information, see [Deploy workloads via Azure Arc on your Azure Stack Edge Pro device](#).

Known issues

The following table provides a summary of known issues for the Azure Stack Edge Pro device.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS
			S

No.	Feature	Issue	Workaround/Comments
1.	Azure Stack Edge Pro + Azure SQL	Creating SQL database requires Administrator access.	<p>Do the following steps instead of Steps 1-2 in Tutorial: Store data at the edge with SQL Server databases.</p> <ul style="list-style-type: none"> • In the local UI of your device, enable compute interface. Select Compute > Port # > Enable for compute > Apply. • Download sqlcmd utility on your client machine. • Connect to your compute interface IP address (the port that was enabled), adding a ",1401" to the end of the address. • Final command will look like this: sqlcmd -S {Interface IP},1401 -U SA -P "Strong!Passw0rd". <p>After this, steps 3-4 from the current documentation should be identical.</p>

No.	Feature	Issue	Workaround/Comments
2.	Refresh	Incremental changes to blobs restored via Refresh are NOT supported	<p>For Blob endpoints, partial updates of blobs after a Refresh, may result in the updates not getting uploaded to the cloud. For example, sequence of actions such as:</p> <ul style="list-style-type: none"> • Create blob in cloud. Or delete a previously uploaded blob from the device. • Refresh blob from the cloud into the appliance using the refresh functionality. • Update only a portion of the blob using Azure SDK REST APIs. <p>These actions can result in the updated sections of the blob to not get updated in the cloud.</p> <p>Workaround: Use tools such as robocopy, or regular file copy through Explorer or command line, to replace entire blobs.</p>
3.	Throttling	During throttling, if new writes are not allowed into the device, writes done by NFS client fail with "Permission Denied" error.	<p>The error will show as below:</p> <pre>hcsuser@ubuntu-vm:~/nfstest\$ mkdir test mkdir: cannot create directory 'test': Permission denied</pre>
4.	Blob Storage ingestion	When using AzCopy version 10 for Blob storage ingestion, run AzCopy with the following argument: Azcopy <other arguments> --cap-mbps 2000	If these limits are not provided for AzCopy, then it could potentially send a large number of requests to the device and result in issues with the service.

No.	Feature	Issue	Workaround/Comments
5.	Tiered storage accounts	<p>The following apply when using tiered storage accounts:</p> <ul style="list-style-type: none"> Only block blobs are supported. Page blobs are not supported. There is no snapshot or copy API support. Hadoop workload ingestion through <code>distcp</code> is not supported as it uses the copy operation heavily. 	
6.	NFS share connection	<p>If multiple processes are copying to the same share, and the <code>nolock</code> attribute is not used, you may see errors during the copy.</p>	<p>The <code>nolock</code> attribute must be passed to the mount command to copy files to the NFS share. For example:</p> <pre>C:\Users\aseuser mount -o anon \\10.1.1.211\mnt\vms Z:</pre>
7.	Kubernetes cluster	<p>When applying an update on your device that is running a Kubernetes cluster, the Kubernetes virtual machines will restart and reboot. In this instance, only pods that are deployed with replicas specified are automatically restored after an update.</p>	<p>If you have created individual pods outside of a replication controller without specifying a replica set, then these pods will not be automatically restored after the device update. You will need to restore these pods.</p> <p>A replica set replaces pods that are deleted or terminated for any reason, such as node failure or disruptive node upgrade. For this reason, we recommend that you use a replica set even if your application requires only a single pod.</p>
8.	Kubernetes cluster	<p>Kubernetes on Azure Stack Edge Pro is supported only with Helm v3 or later. For more information, go to Frequently asked questions: Removal of Tiller.</p>	
9.	Azure Arc + Azure Stack Edge Pro	<p>Azure Arc deployments are not supported if web proxy is configured on your Azure Stack Edge Pro device.</p>	

No.	Feature	Issue	Workaround/Comments
10.	Kubernetes	<p>Port 31000 is reserved for Kubernetes Dashboard. Similarly, in the default configuration, the IP addresses 172.28.0.1 and 172.28.0.10, are reserved for Kubernetes service and Core DNS service respectively.</p>	Do not use reserved IPs.
11.	Kubernetes	<p>Kubernetes does not currently allow multi-protocol LoadBalancer services. For example, a DNS service that would have to listen on both TCP and UDP.</p>	<p>To work around this limitation of Kubernetes with MetalLB, two services (one for TCP, one for UDP) can be created on the same pod selector. These services use the same sharing key and spec.loadBalancerIP to share the same IP address. IPs can also be shared if you have more services than available IP addresses. For more information, see IP address sharing.</p>
12.	Kubernetes cluster	<p>Existing Azure IoT Edge marketplace modules will not run on the Kubernetes cluster as the hosting platform for IoT Edge on Azure Stack Edge device.</p>	<p>The modules will need to be modified before these are deployed on the Azure Stack Edge device. For more information, see Modify Azure IoT Edge modules from marketplace to run on Azure Stack Edge device.</p>
13.	Kubernetes	<p>File-based bind mounts are not supported with Azure IoT Edge on Kubernetes on Azure Stack Edge device.</p>	<p>IoT Edge uses a translation layer to translate <code>ContainerCreate</code> options to Kubernetes constructs. Creating <code>Binds</code> maps to <code>hostpath</code> directory or create and thus file-based bind mounts cannot be bound to paths in IoT Edge containers.</p>
14.	Kubernetes	<p>If you bring your own certificates for IoT Edge and add those on your Azure Stack Edge device, the new certificates are not picked up as part of the Helm charts update.</p>	<p>To workaround this problem, Connect to the PowerShell interface of the device. Restart <code>iotedged</code> and <code>edgehub</code> pods.</p>

No.	Feature	Issue	Workaround/Comments
15.	Certificates	In certain instances, certificate state in the local UI may take several seconds to update.	<p>The following scenarios in the local UI may be affected.</p> <ul style="list-style-type: none"> • Status column in Certificates page. • Security tile in Get started page. • Configuration tile in Overview page.

Next steps

- [Prepare to deploy Azure Stack Edge Pro device with GPU](#)

Azure Policy built-in definitions for Azure Stack Edge

9/21/2022 • 2 minutes to read • [Edit Online](#)

This page is an index of [Azure Policy](#) built-in policy definitions for Azure Stack Edge. For additional Azure Policy built-ins for other services, see [Azure Policy built-in definitions](#).

The name of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Version** column to view the source on the [Azure Policy GitHub repo](#).

Azure Stack Edge

NAME (AZURE PORTAL)	DESCRIPTION	EFFECT(S)	VERSION (GITHUB)
Azure Stack Edge devices should use double-encryption	To secure the data at rest on the device, ensure it's double-encrypted, the access to data is controlled, and once the device is deactivated, the data is securely erased off the data disks. Double encryption is the use of two layers of encryption: BitLocker XTS-AES 256-bit encryption on the data volumes and built-in encryption of the hard drives. Learn more in the security overview documentation for the specific Stack Edge device.	audit, Audit, deny, Deny, disabled, Disabled	1.1.0

Next steps

- See the built-ins on the [Azure Policy GitHub repo](#).
- Review the [Azure Policy definition structure](#).
- Review [Understanding policy effects](#).

What is Azure Stack Edge Pro FPGA?

9/21/2022 • 4 minutes to read • [Edit Online](#)

IMPORTANT

Azure Stack Edge Pro FPGA devices will reach end-of-life in February 2024. If you are considering new deployments, we recommend that you explore [Azure Stack Edge Pro GPU](#) devices for your workloads.

Azure Stack Edge Pro with FPGA is an AI-enabled edge computing device with network data transfer capabilities. This article provides you an overview of the Azure Stack Edge Pro with FPGA solution, benefits, key capabilities, and deployment scenarios.

Azure Stack Edge Pro with FPGA is a Hardware-as-a-service solution. Microsoft ships you a cloud-managed device with a built-in Field Programmable Gate Array (FPGA) that enables accelerated AI-inferencing and has all the capabilities of a network storage gateway.

Azure Data Box Edge is rebranded as Azure Stack Edge.

Use cases

Here are the various scenarios where Azure Stack Edge Pro FPGA can be used for rapid Machine Learning (ML) inferencing at the edge and preprocessing data before sending it to Azure.

- **Inference with Azure Machine Learning** - With Azure Stack Edge Pro FPGA, you can run ML models to get quick results that can be acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models. For more information on how to use the Azure ML hardware accelerated models on the Azure Stack Edge Pro FPGA device, see [Deploy Azure ML hardware accelerated models on Azure Stack Edge Pro FPGA](#).
- **Preprocess data** - Transform data before sending it to Azure to create a more actionable dataset. Preprocessing can be used to:
 - Aggregate data.
 - Modify data, for example to remove personal data.
 - Subset data to optimize storage and bandwidth, or for further analysis.
 - Analyze and react to IoT Events.
- **Transfer data over network to Azure** - Use Azure Stack Edge Pro FPGA to easily and quickly transfer data to Azure to enable further compute and analytics or for archival purposes.

Key capabilities

Azure Stack Edge Pro FPGA has the following capabilities:

CAPABILITY	DESCRIPTION
Accelerated AI inferencing	Enabled by the built-in FPGA.
Computing	Allows analysis, processing, filtering of data.
High performance	High-performance compute and data transfers.

CAPABILITY	DESCRIPTION
Data access	Direct data access from Azure Storage Blobs and Azure Files using cloud APIs for additional data processing in the cloud. Local cache on the device is used for fast access of most recently used files.
Cloud-managed	Device and service are managed via the Azure portal.
Offline upload	Disconnected mode supports offline upload scenarios.
Supported protocols	Support for standard SMB and NFS protocols for data ingestion. For more information on supported versions, see Azure Stack Edge Pro FPGA system requirements .
Data refresh	Ability to refresh local files with the latest from cloud.
Encryption	BitLocker support to locally encrypt data and secure data transfer to cloud over <i>https</i> .
Bandwidth throttling	Throttle to limit bandwidth usage during peak hours.
ExpressRoute	Added security through ExpressRoute. Use peering configuration where traffic from local devices to the cloud storage endpoints travels over the ExpressRoute. For more information, see ExpressRoute overview .

Components

The Azure Stack Edge Pro FPGA solution comprises of Azure Stack Edge resource, Azure Stack Edge Pro FPGA physical device, and a local web UI.

- **Azure Stack Edge Pro FPGA physical device:** A 1U rack-mounted server supplied by Microsoft that can be configured to send data to Azure.
- **Azure Stack Edge resource:** A resource in the Azure portal that lets you manage an Azure Stack Edge Pro FPGA device from a web interface that you can access from different geographic locations. Use the Azure Stack Edge resource to create and manage resources, manage shares, and view and manage devices and alerts.

As Azure Stack Edge Pro FPGA approaches its end of life, no orders for new Azure Stack Edge Pro FPGA devices are being filled. If you're a new customer, we recommend that you explore using Azure Stack Edge Pro - GPU devices for your workloads. For more information, go to [What is Azure Stack Edge Pro with GPU](#). For information about ordering an Azure Stack Edge Pro with GPU device, go to [Create a new resource for Azure Stack Edge Pro - GPU](#).

If you're an existing customer, you can still create a new Azure Stack Edge resource if you need to replace or reset your existing Azure Stack Edge Pro FPGA device. For instructions, go to [Create an order for your Azure Stack Edge Pro FPGA device](#).

- **Azure Stack Edge Pro FPGA local web UI** - Use the local web UI to run diagnostics, shut down and restart the Azure Stack Edge Pro FPGA device, view copy logs, and contact Microsoft Support to file a service request.

For information about using the web-based UI, go to [Use the web-based UI to administer your Azure](#)

Region availability

Azure Stack Edge Pro FPGA physical device, Azure resource, and target storage account to which you transfer data do not all have to be in the same region.

- **Resource availability** - For a list of all the regions where the Azure Stack Edge resource is available, see [Azure products available by region](#). Azure Stack Edge Pro FPGA can also be deployed in the Azure Government Cloud. For more information, see [What is Azure Government?](#).
- **Destination Storage accounts** - The storage accounts that store the data are available in all Azure regions. The regions where the storage accounts store Azure Stack Edge Pro FPGA data should be located close to where the device is located for optimum performance. A storage account located far from the device results in long latencies and slower performance.

Azure Stack Edge service is a non-regional service. For more information, see [Regions and Availability Zones in Azure](#). Azure Stack Edge service does not have dependency on a specific Azure region, making it resilient to zone-wide outages and region-wide outages.

Next steps

- Review the [Azure Stack Edge Pro FPGA system requirements](#).
- Understand the [Azure Stack Edge Pro FPGA limits](#).
- Deploy [Azure Stack Edge Pro FPGA](#) in Azure portal.

Tutorial: Prepare to deploy Azure Stack Edge Pro FPGA

9/21/2022 • 6 minutes to read • [Edit Online](#)

This is the first tutorial in the series of deployment tutorials that are required to completely deploy Azure Stack Edge Pro FPGA. This tutorial describes how to prepare the Azure portal to deploy an Azure Stack Edge resource.

You need administrator privileges to complete the setup and configuration process. The portal preparation takes less than 10 minutes.

In this tutorial, you learn how to:

- Create a new resource
- Get the activation key

If you don't have an Azure subscription, create a [free account](#) before you begin.

Get started

To deploy Azure Stack Edge Pro FPGA, refer to the following tutorials in the prescribed sequence.

#	IN THIS STEP	USE THESE DOCUMENTS
1.	Prepare the Azure portal for Azure Stack Edge Pro FPGA	Create and configure your Azure Stack Edge resource before you install an Azure Stack Box Edge physical device.
2.	Install Azure Stack Edge Pro FPGA	Unpack, rack, and cable the Azure Stack Edge Pro FPGA physical device.
3.	Connect, set up, and activate Azure Stack Edge Pro FPGA	Connect to the local web UI, complete the device setup, and activate the device. The device is ready to set up SMB or NFS shares.
4.	Transfer data with Azure Stack Edge Pro FPGA	Add shares and connect to shares via SMB or NFS.
5.	Transform data with Azure Stack Edge Pro FPGA	Configure compute modules on the device to transform the data as it moves to Azure.

You can now begin to set up the Azure portal.

Prerequisites

Following are the configuration prerequisites for your Azure Stack Edge resource, your Azure Stack Edge Pro FPGA device, and the datacenter network.

For the Azure Stack Edge resource

Before you begin, make sure that:

- Your Microsoft Azure subscription is enabled for an Azure Stack Edge resource. Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#). Pay-as-you-go subscriptions aren't supported.
- RBAC roles: You have the following role assignments in Azure role-based access control (RBAC):
 - To create Azure Stack Edge, IoT Hub, and Azure storage resources, a user must have the Contributor or Owner role at resource group scope.
 - To assign the Contributor role to a user at resource group scope, you must have the Owner role at subscription scope.

For detailed steps, see [Assign Azure roles using the Azure portal](#).

- Resource providers: The following resource providers are registered:
 - To create an Azure Stack Edge/Data Box Gateway resource, make sure the `Microsoft.DataBoxEdge` provider is registered.
 - To create an IoT Hub resource, make sure the `Microsoft.Devices` provider is registered.
 - To create an Azure Storage resource, make sure Azure Storage is registered. The Azure Storage Resource Provider (SRP) is by default a registered resource provider, but in some cases registration may be needed.

To register a resource provider, you must have been assigned the related RBAC role, above.

For information on how to register, see [Register resource provider](#).

- You have admin or user access to Azure Active Directory Graph API. For more information, see [Azure Active Directory Graph API](#).
- You have your Microsoft Azure storage account with access credentials.
- You are not blocked by any Azure Policy assignment set up by your system administrator. For more information about Azure Policy, see [Quickstart: Create a policy assignment to identify non-compliant resources](#).

For the Azure Stack Edge Pro FPGA device

Before you deploy a physical device, make sure that:

- You've reviewed the safety information that was included in the shipment package.
- You have a 1U slot available in a standard 19" rack in your datacenter for rack mounting the device.
- You have access to a flat, stable, and level work surface where the device can rest safely.
- The site where you intend to set up the device has standard AC power from an independent source or a rack power distribution unit (PDU) with an uninterruptible power supply (UPS).
- You have access to a physical device.

For the datacenter network

Before you begin, make sure that:

- The network in your datacenter is configured per the networking requirements for your Azure Stack Edge Pro FPGA device. For more information, see [Azure Stack Edge Pro FPGA System Requirements](#).
- For normal operating conditions of your Azure Stack Edge Pro FPGA, you have:
 - A minimum of 10 Mbps download bandwidth to ensure the device stays updated.
 - A minimum of 20 Mbps dedicated upload and download bandwidth to transfer files.

Create new resource for existing device

If you're an existing Azure Stack Edge Pro FPGA customer, use the following procedure to create a new resource if you need to replace or reset your existing device.

If you're a new customer, we recommend that you explore using Azure Stack Edge Pro - GPU devices for your workloads. For more information, go to [What is Azure Stack Edge Pro with GPU](#). For information about ordering an Azure Stack Edge Pro with GPU device, go to [Create a new resource for Azure Stack Edge Pro - GPU](#).

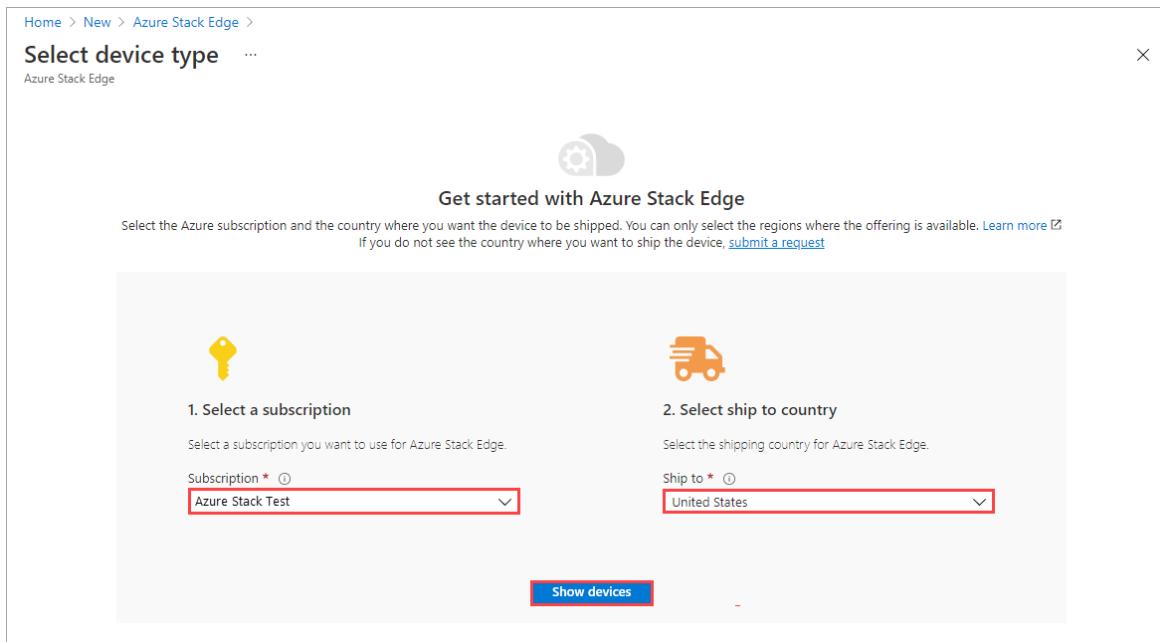
To create a new Azure Stack Edge resource for an existing device, take the following steps in the Azure portal.

1. Use your Microsoft Azure credentials to sign in to:

- The Azure portal at this URL: <https://portal.azure.com>.
- Or, the Azure Government portal at this URL: <https://portal.azure.us>. For more details, go to [Connect to Azure Government using the portal](#).

2. Select **+ Create a resource**. Search for and select **Azure Stack Edge**. Then select **Create**.

3. Select the subscription for the Azure Stack Edge Pro FPGA device and the country to ship the device to in **Ship to**.



4. In the list of device types that is displayed, select **Azure Stack Edge Pro - FPGA**. Then choose **Select**.

The **Azure Stack Edge Pro - FPGA** device type is only displayed if you have an existing device. If you need to order a new device, go to [Create a new resource for Azure Stack Edge Pro - GPU](#).

Select device type

Azure Stack Edge

X

Select the Azure subscription and the country where you will set up the device. [Learn more](#)

1. Select a subscription * ⓘ

Fleet Manager Dogfood

2. Select ship to country * ⓘ

United States

Show devices

Azure Stack Edge

Azure Stack Edge Pro - GPU
Azure managed physical edge compute device
[Device specifications ⓘ](#)

1U rack mount device with network data transfer capabilities
 Hardware accelerated ML using Nvidia T4 GPU
 Azure Private Edge Zones enabled

Starting from
Per device per month excludes shipping

Select

Azure Stack Edge Pro - FPGA
Azure managed physical edge compute device
[Device specifications ⓘ](#)

1U rack mount device with network data transfer capabilities
 Hardware accelerated ML using Intel Arria 10 FPGA

Per device per month excludes shipping

Select

Azure Stack Edge Pro R
Rugged, physical edge compute device
[Device specifications ⓘ](#)

Portable, server class device with network data transfer capabilities
 Hardware accelerated ML using Nvidia T4 GPU
 Specialized rugged casing tailored for harsh environments

Starting from
Per device per month excludes shipping

Select**5. On the Basics tab:****a. Enter or select the following Project details.**

SETTING	VALUE
Subscription	This value is automatically populated based on the earlier selection. Subscription is linked to your billing account.
Resource group	Select an existing group or create a new group. Learn more about Azure Resource Groups .

b. Enter or select the following Instance details.

SETTING	VALUE
Name	A friendly name to identify the resource. The name has from 2 and 50 characters, including letters, numbers, and hyphens. Name starts and ends with a letter or a number.
Region	For a list of all the regions where the Azure Stack Edge resource is available, see Azure products available by region . If using Azure Government, all the government regions are available as shown in the Azure regions . Choose a location closest to the geographical region where you want to deploy your device.

c. Select Review + create.

Home > New > Azure Stack Edge > Select device type >

Create a resource and order a device

Azure Stack Edge Pro - FPGA

Basics Tags Review + create

Info As per the [announcement](#), existing FPGA devices will be receiving critical security updates and fixes until end of retirement. Placing of new orders is not supported.

Create an Azure resource. [Learn more](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription [Fleet Manager Dogfood](#)

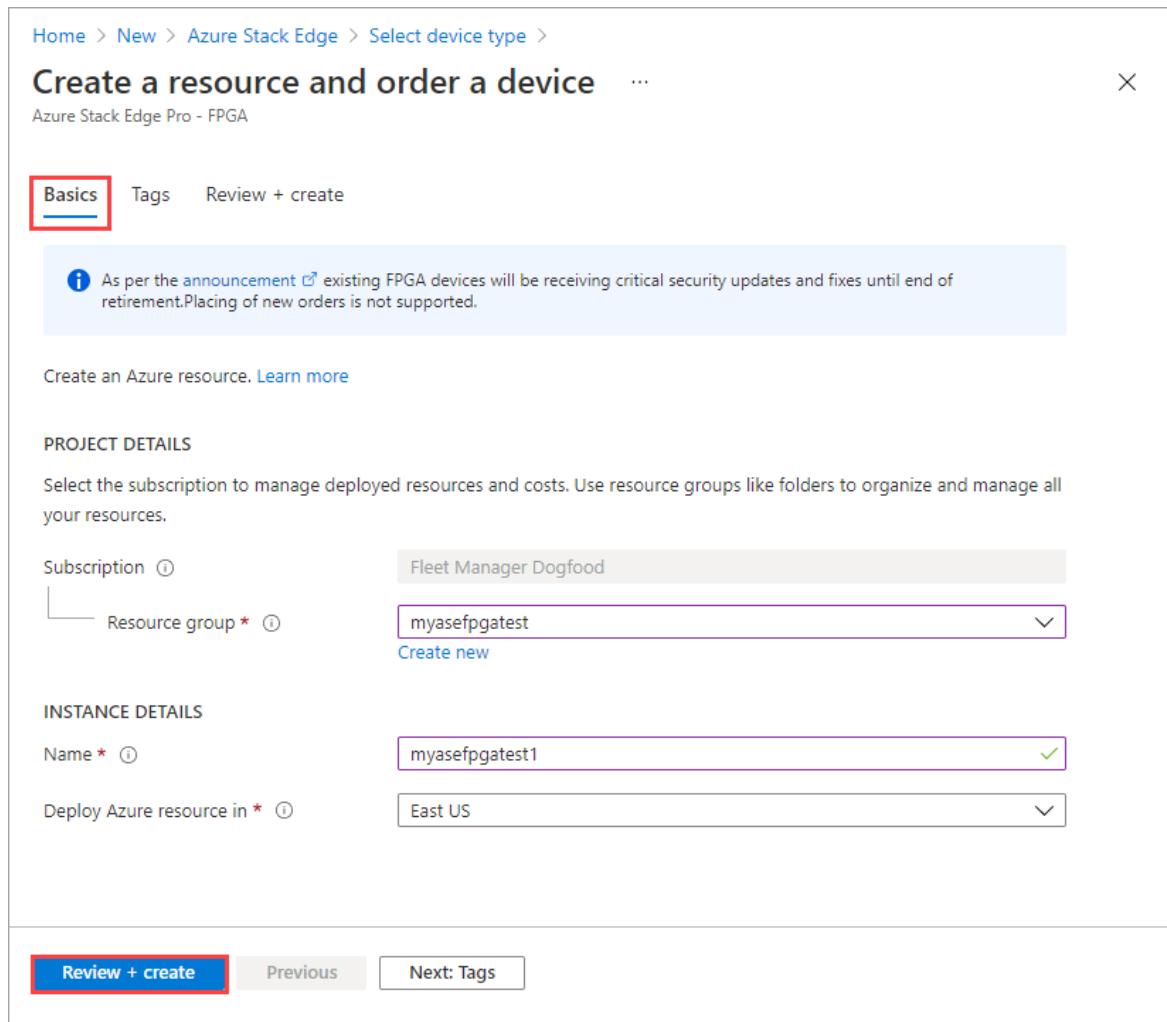
Resource group * [myasefpgatest](#) [Create new](#)

INSTANCE DETAILS

Name * [myasefpgatest1](#)

Deploy Azure resource in * [East US](#)

Review + create Previous Next: Tags



6. On the **Review + create** tab, review the **Terms of use**, **Pricing details**, and the details for your resource. Then select **Create**.

Home > New > Azure Stack Edge > Select device type >

Create a resource and order a device

Azure Stack Edge Pro - FPGA

All validations have passed.

Basics Tags Review + create

MODEL DETAILS

Azure Stack Edge Pro - FPGA

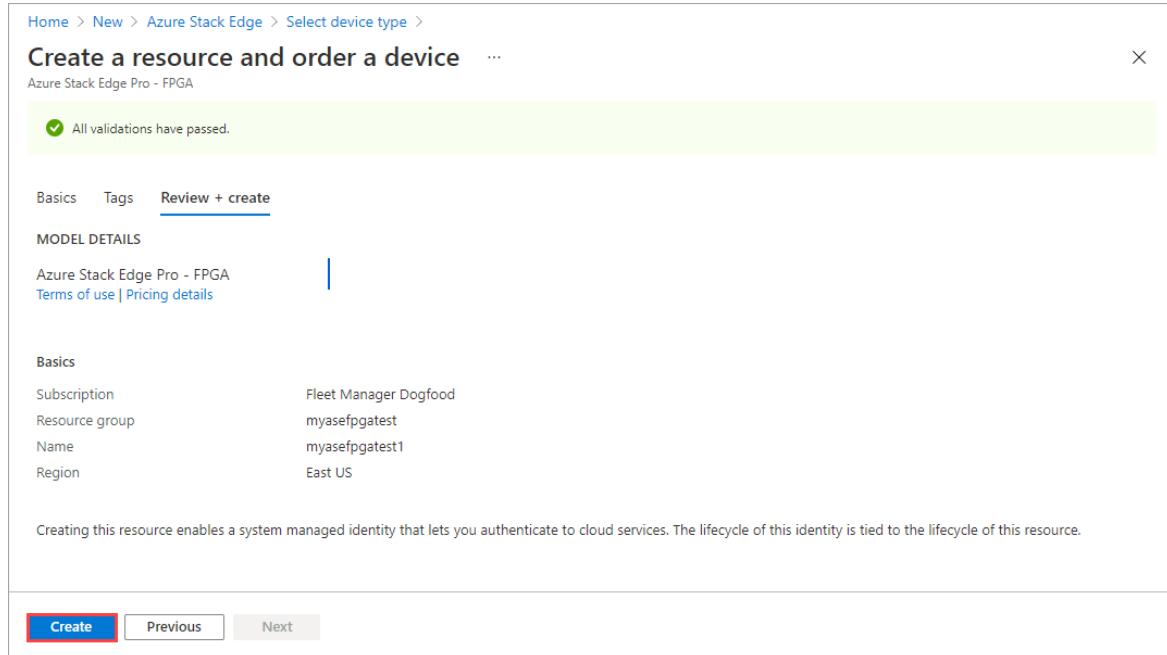
[Terms of use](#) | [Pricing details](#)

Basics

Subscription	Fleet Manager Dogfood
Resource group	myasefpgatest
Name	myasefpgatest1
Region	East US

Creating this resource enables a system managed identity that lets you authenticate to cloud services. The lifecycle of this identity is tied to the lifecycle of this resource.

Create Previous Next



7. The resource creation takes a few minutes. After the resource is successfully created and deployed, you're notified. Select **Go to resource**.

Your deployment is complete

Go to resource

Deployment name: MyAzureStackEdge1
Subscription: AzureStackTest
Resource group: azurestack2etest

DEPLOYMENT DETAILS (Download)

Start time: 3/7/2019, 10:39:30 AM
Duration: 1 minute 9 seconds
Correlation ID: 4df8d7ed-41d7-4920-b1b8-1f8bfd7ecc55

RESOU...	TYPE	STATUS	OPERAT...
MyAzureSt...	Microso...	OK	Operation
MyAzureSt...	Microso...	OK	Operation

Additional Resources

- Windows Server 2016 VM Quickstart tutorial
- Cosmos DB Quickstart tutorial
- Web App Quickstart tutorial
- SQL Database Quickstart tutorial
- Storage Account Quickstart tutorial

After the order is placed, Microsoft reviews the order and contacts you (via email) with shipping details.

Device is not activated. Click 'Device setup' to review the prerequisites and configure your device.

We are reviewing the order you placed. After the review, Microsoft will reach out to you via email with shipping details. Billing starts 14 days after the device is shipped.

Get the activation key

After the Azure Stack Edge resource is up and running, you'll need to get the activation key. This key is used to activate and connect your Azure Stack Edge Pro FPGA device with the resource. You can get this key now while you are in the Azure portal.

1. Go to the resource that you created, and select **Overview**. You'll see a notification to the effect that your order is being processed.

The screenshot shows the Azure Stack Edge device management interface. The left sidebar lists various management options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (IoT Edge, Cloud storage gateway), Monitoring (Device events, Alerts, Metrics), Automation (Tasks (preview)), and Support + troubleshooting. The main content area has a red box around the 'Overview' tab. Below it, a message states: 'Your order is being processed! Microsoft is reviewing your order. We will inform you via email once the device is shipped. Your billing starts 14 days after the shipment.' Another red box highlights a section titled 'While your device arrives...' with instructions: '1 Configure your infrastructure to activate your device. See [configuration steps](#). 2 After activation, deploy services on your device to speed up data processing time.'

- After the order is processed and the device is on your way, the **Overview** updates. Accept the default **Azure Key Vault name** or enter a new one. Select **Generate activation key**. Select the copy icon to copy the key and save it for later use.

The screenshot shows the same Azure Stack Edge device management interface as the previous one, but the 'Generate activation key' button in the 'Activate device once it arrives' section is now highlighted with a red box. The rest of the interface remains the same, including the sidebar and the 'Your device is on its way...' message.

IMPORTANT

- The activation key expires three days after it is generated.
- If the key has expired, generate a new key. The older key is not valid.

Next steps

In this tutorial, you learned about Azure Stack Edge Pro FPGA topics such as:

- Create a new resource
- Get the activation key

Advance to the next tutorial to learn how to install Azure Stack Edge Pro FPGA.

[Install Azure Stack Edge Pro FPGA](#)

Tutorial: Install Azure Stack Edge Pro FPGA

9/21/2022 • 7 minutes to read • [Edit Online](#)

This tutorial describes how to install a Azure Stack Edge Pro FPGA physical device. The installation procedure involves unpacking, rack mounting, and cabling the device.

The installation can take around two hours to complete.

In this tutorial, you learn how to:

- Unpack the device
- Rack mount the device
- Cable the device

Prerequisites

The prerequisites for installing a physical device as follows:

For the Azure Stack Edge resource

Before you begin, make sure that:

- You've completed all the steps in [Prepare to deploy Azure Stack Edge Pro FPGA](#).
 - You've created a Azure Stack Edge resource to deploy your device.
 - You've generated the activation key to activate your device with the Azure Stack Edge resource.

For the Azure Stack Edge Pro FPGA physical device

Before you deploy a device:

- Make sure that the device rests safely on a flat, stable, and level work surface.
- Verify that the site where you intend to set up has:
 - Standard AC power from an independent source

-OR-

- A rack power distribution unit (PDU) with an uninterruptible power supply (UPS)
- An available 1U slot on the rack on which you intend to mount the device

For the network in the datacenter

Before you begin:

- Review the networking requirements for deploying Azure Stack Edge Pro FPGA, and configure the datacenter network per the requirements. For more information, see [Azure Stack Edge Pro FPGA networking requirements](#).
- Make sure that the minimum Internet bandwidth is 20 Mbps for optimal functioning of the device.

Unpack the device

This device is shipped in a single box. Complete the following steps to unpack your device.

1. Place the box on a flat, level surface.
2. Inspect the box and the packaging foam for crushes, cuts, water damage, or any other obvious damage. If the

box or packaging is severely damaged, don't open it. Contact Microsoft Support to help you assess whether the device is in good working order.

3. Unpack the box. After unpacking the box, make sure that you have:

- One single enclosure Azure Stack Edge Pro FPGA device
- Two power cords
- One rail kit assembly
- A Safety, Environmental, and Regulatory Information booklet

If you didn't receive all of the items listed here, contact Azure Stack Edge Pro FPGA support. The next step is to rack mount your device.

Rack the device

The device must be installed on a standard 19-inch rack. Use the following procedure to rack mount your device on a standard 19-inch rack.

IMPORTANT

Azure Stack Edge Pro FPGA devices must be rack-mounted for proper operation.

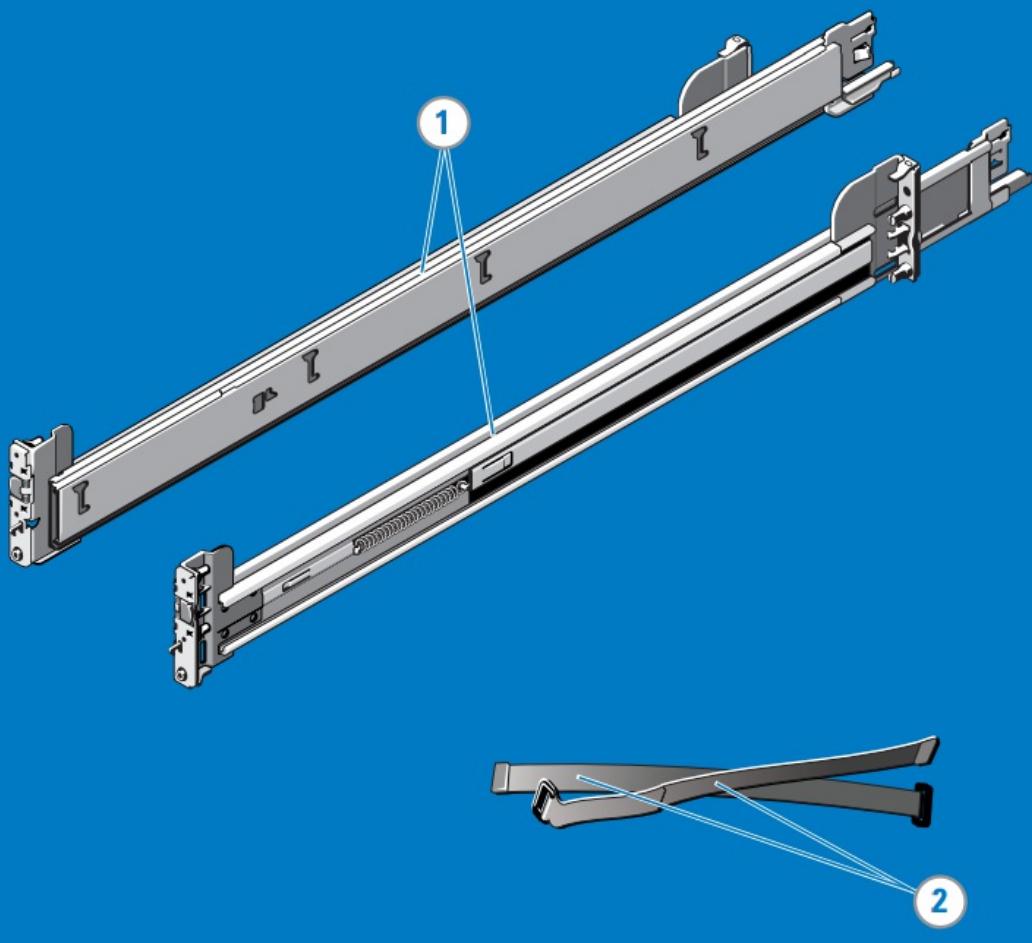
Prerequisites

- Before you begin, read the safety instructions in your Safety, Environmental, and Regulatory Information booklet. This booklet was shipped with the device.
- Begin installing the rails in the allotted space that is closest to the bottom of the rack enclosure.
- For the toolled rail mounting configuration:
 - You need to supply eight screws: #10-32, #12-24, #M5, or #M6. The head diameter of the screws must be less than 10 mm (0.4").
 - You need a flat-tipped screwdriver.

Identify the rail kit contents

Locate the components for installing the rail kit assembly:

1. Two A7 Dell ReadyRails II sliding rail assemblies
2. Two hook and loop straps

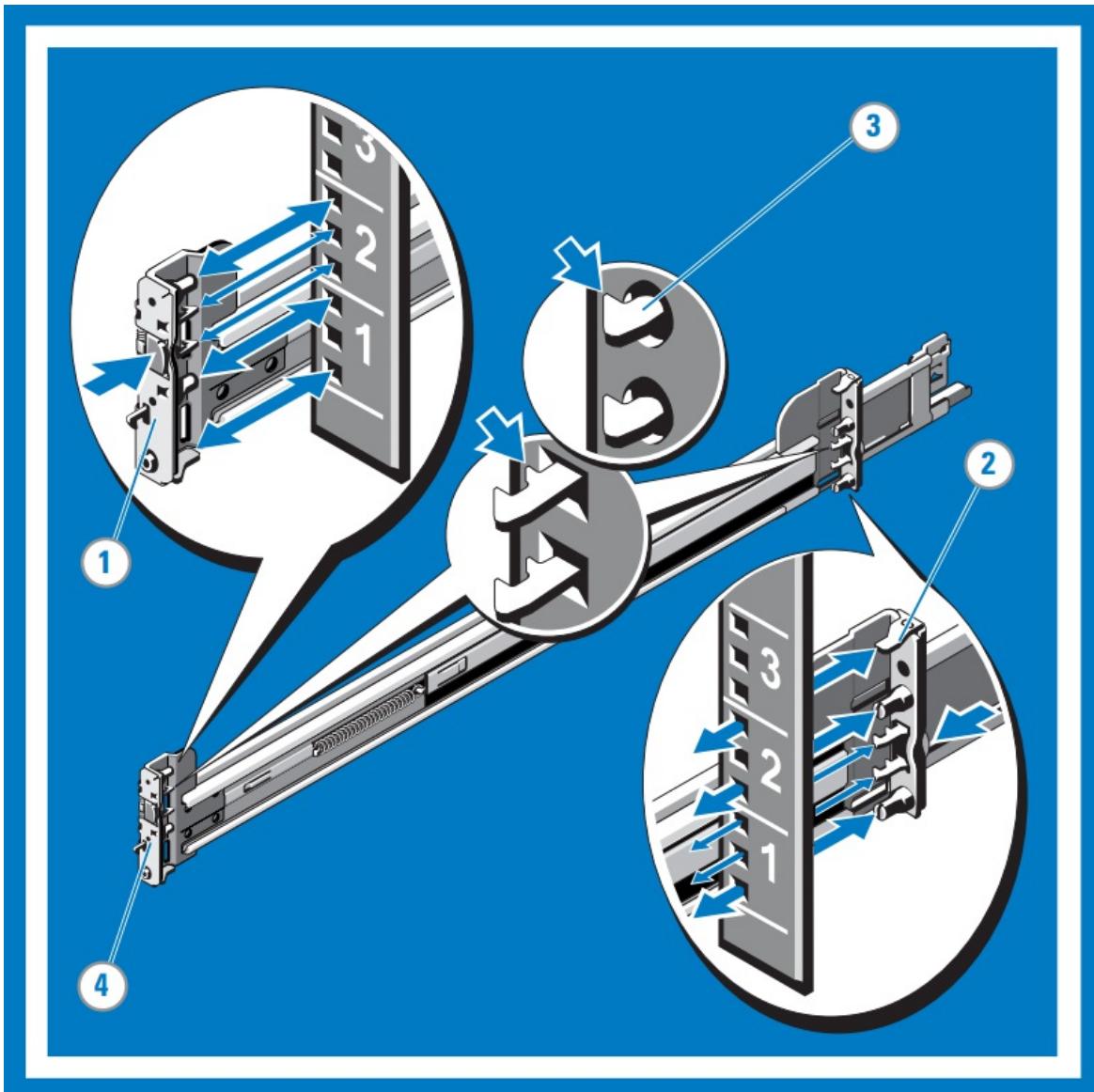


Install and remove tool-less rails (Square hole or round hole racks)

TIP

This option is tool-less because it does not require tools to install and remove the rails into the unthreaded square or round holes in the racks.

1. Position the left and right rail end pieces labeled **FRONT** facing inward and orient each end piece to seat in the holes on the front side of the vertical rack flanges.
2. Align each end piece in the bottom and top holes of the desired U spaces.
3. Engage the back end of the rail until it fully seats on the vertical rack flange and the latch clicks into place. Repeat these steps to position and seat the front-end piece on the vertical rack flange.
4. To remove the rails, pull the latch release button on the end piece midpoint and unseat each rail.

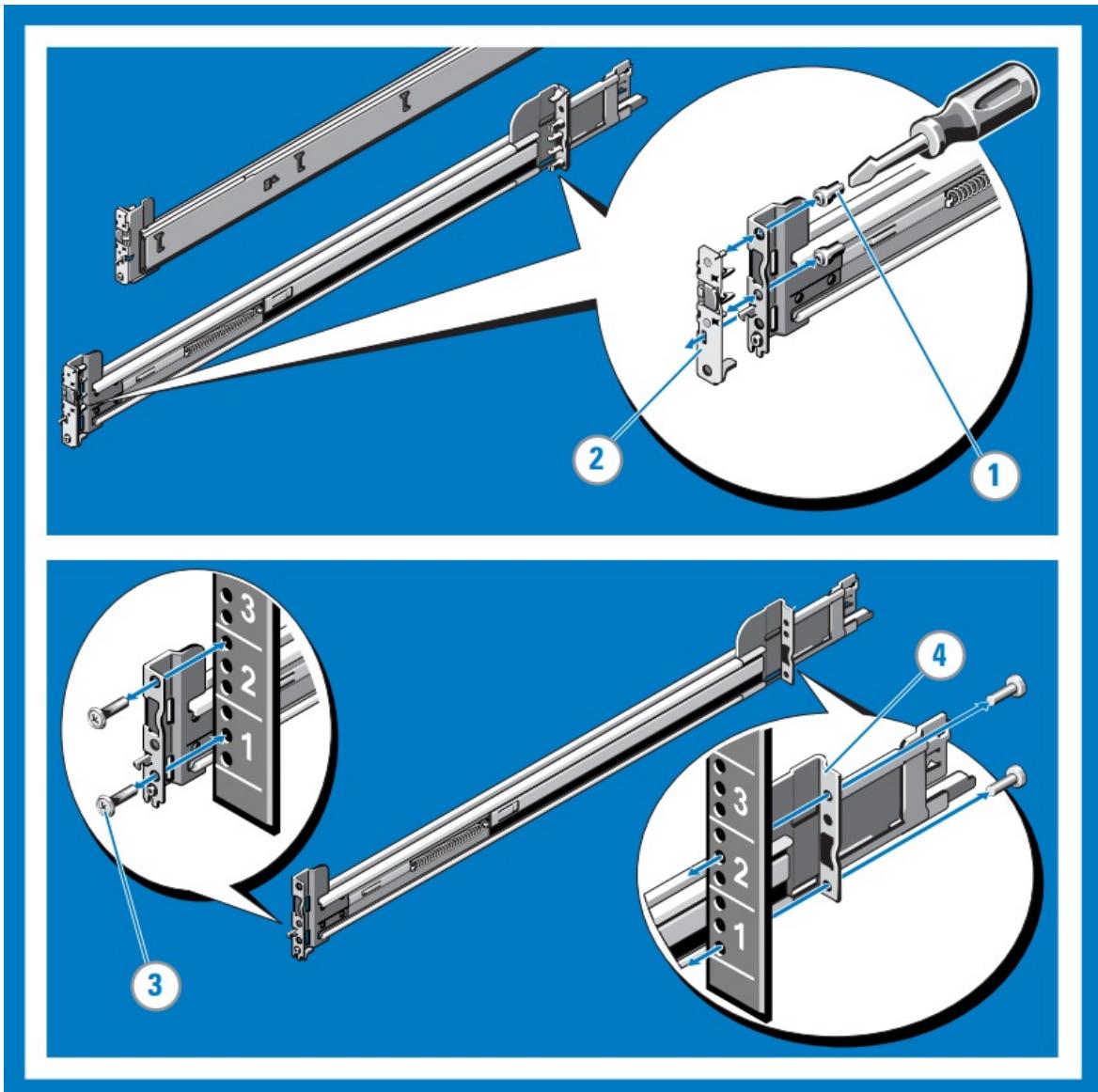


Install and remove tooled rails (Threaded hole racks)

TIP

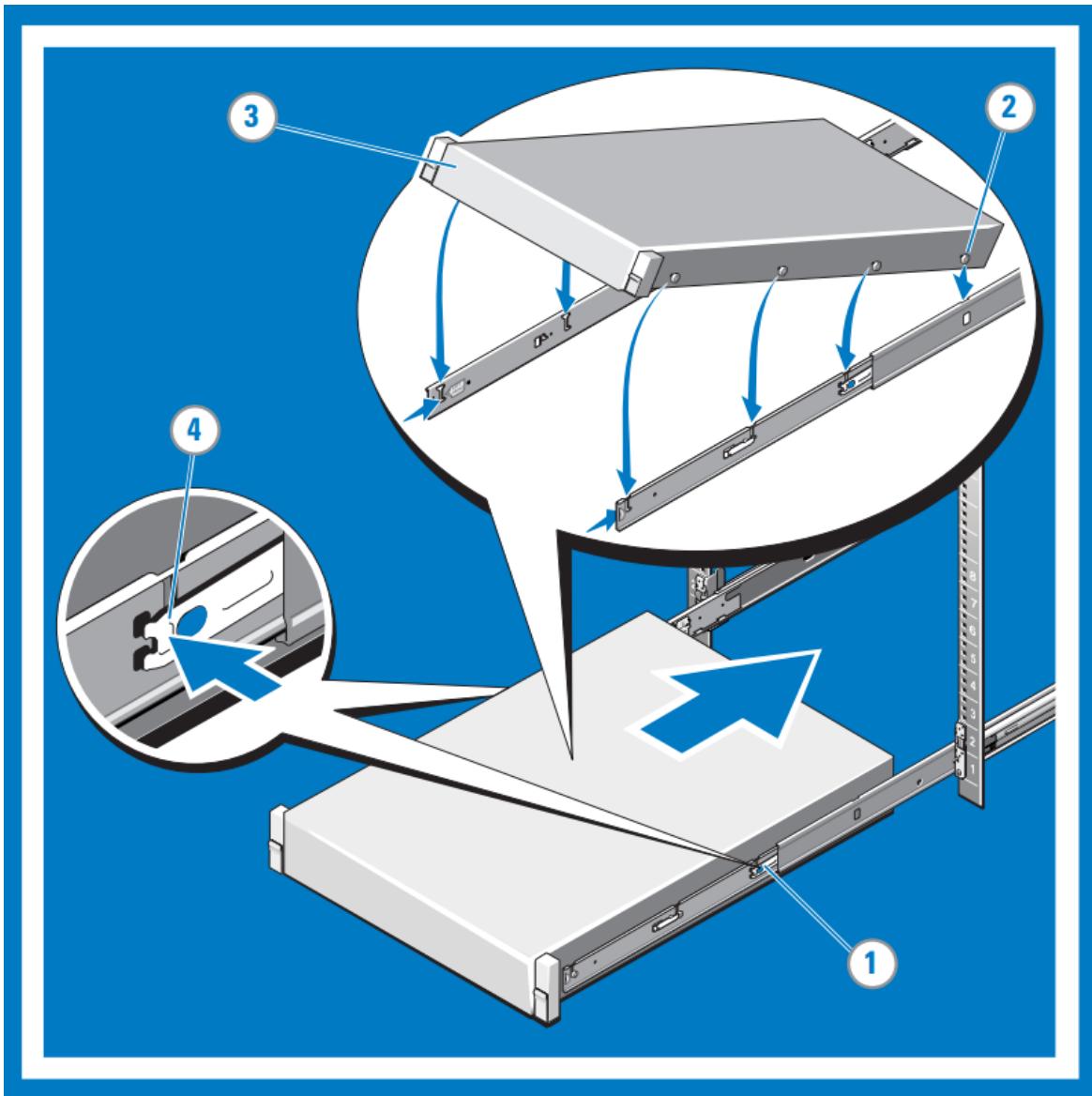
This option is tooled because it requires a tool (*a flat-tipped screwdriver*) to install and remove the rails into the threaded round holes in the racks.

1. Remove the pins from the front and rear mounting brackets using a flat-tipped screwdriver.
2. Pull and rotate the rail latch subassemblies to remove them from the mounting brackets.
3. Attach the left and right mounting rails to the front vertical rack flanges using two pairs of screws.
4. Slide the left and right back brackets forward against the rear vertical rack flanges and attach them using two pairs of screws.



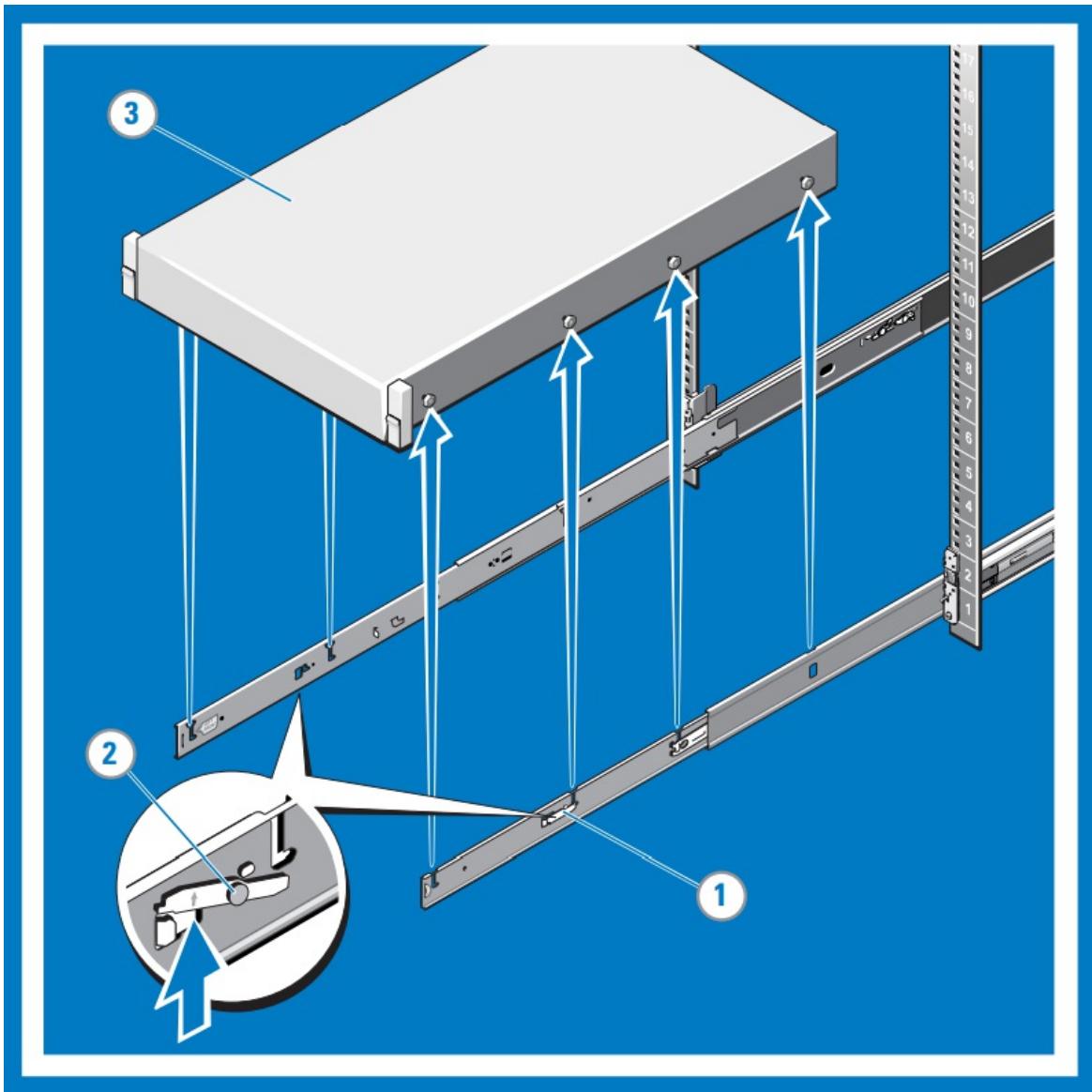
Install the system in a rack

1. Pull the inner slide rails out of the rack until they lock into place.
2. Locate the rear rail standoff on each side of the system and lower them into the rear J-slots on the slide assemblies. Rotate the system downward until all the rail standoffs are seated in the J-slots.
3. Push the system inward until the lock levers click into place.
4. Press the slide-release lock buttons on both rails and slide the system into the rack.



Remove the system from the rack

1. Locate the lock levers on the sides of the inner rails.
2. Unlock each lever by rotating it up to its release position.
3. Grasp the sides of the system firmly and pull it forward until the rail standoffs are at the front of the J-slots. Lift the system up and away from the rack and place it on a level surface.

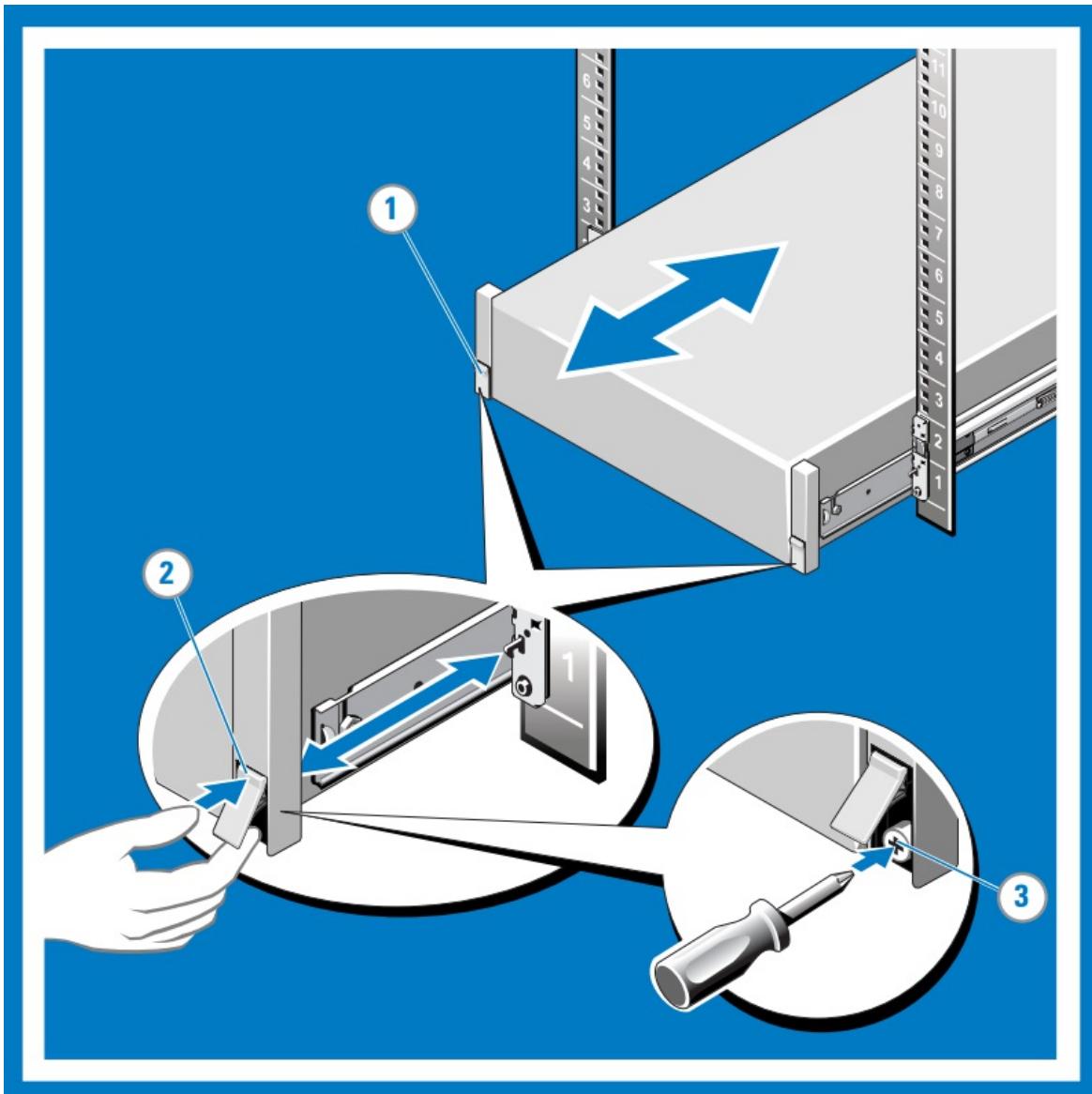


Engage and release the slam latch

NOTE

For systems not equipped with slam latches, secure the system using screws, as described in step 3 of this procedure.

1. Facing the front, locate the slam latch on either side of the system.
2. The latches engage automatically as the system is pushed into the rack and are released by pulling up on the latches.
3. To secure the system for shipment in the rack or for other unstable environments, locate the hard-mount screw under each latch and tighten each screw with a #2 Phillips screwdriver.



Cable the device

Route the cables and then cable your device. The following procedures explain how to cable your Azure Stack Edge Pro FPGA device for power and network.

Before you start cabling your device, you need the following:

- Your Azure Stack Edge Pro FPGA physical device, unpacked, and rack mounted.
- Two power cables.
- At least one 1-GbE RJ-45 network cable to connect to the management interface. There are two 1-GbE network interfaces, one management and one data, on the device.
- One 25-GbE SFP+ copper cable for each data network interface to be configured. At least one data network interface from among PORT 2, PORT 3, PORT 4, PORT 5, or PORT 6 needs to be connected to the Internet (with connectivity to Azure).
- Access to two power distribution units (recommended).

NOTE

- If you are connecting only one data network interface, we recommend that you use a 25/10-GbE network interface such as PORT 3, PORT 4, PORT 5, or PORT 6 to send data to Azure.
- For best performance and to handle large volumes of data, consider connecting all the data ports.
- The Azure Stack Edge Pro FPGA device should be connected to the datacenter network so that it can ingest data from data source servers.

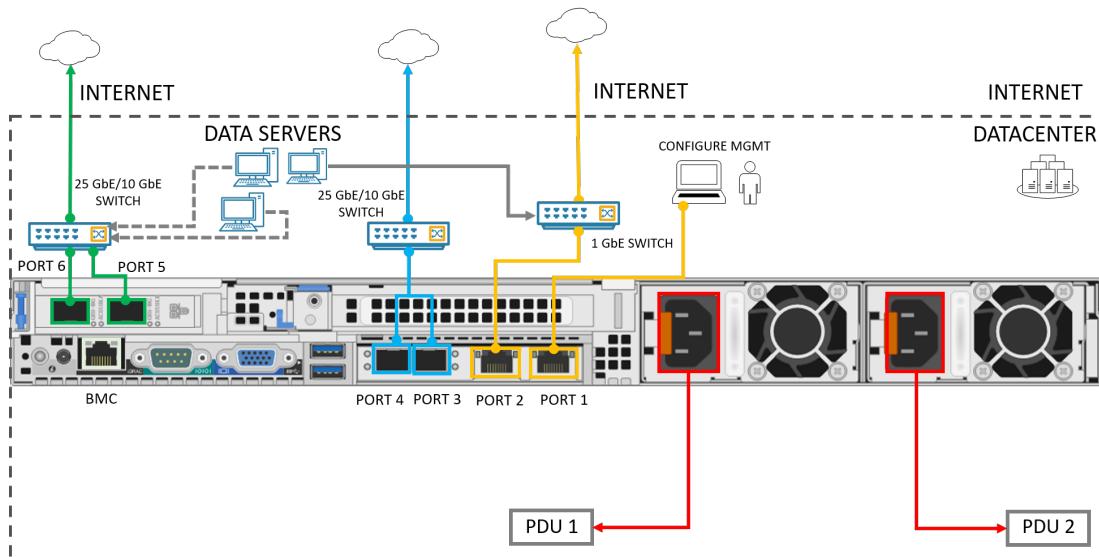
On your Azure Stack Edge Pro FPGA device:

- The front panel has disk drives and a power button.
 - There are 10 disk slots in the front of your device.
 - Slot 0 has a 240-GB SATA drive used as an operating system disk. Slot 1 is empty and slots 2 to 9 are NVMe SSDs used as data disks.
- The back plane includes redundant power supply units (PSUs).
- The back plane has six network interfaces:
 - Two 1-Gbps interfaces.
 - Four 25-Gbps interfaces that can also serve as 10-Gbps interfaces.
 - A baseboard management controller (BMC).
- The back plane has two network cards corresponding to the 6 ports:
 - QLogic FastLinQ 41264
 - QLogic FastLinQ 41262

For a full list of supported cables, switches, and transceivers for these network cards, go to [Cavium FastlinQ 41000 Series Interoperability Matrix](#).

Take the following steps to cable your device for power and network.

1. Identify the various ports on the back plane of your device.



2. Locate the disk slots and the power button on the front of the device.



3. Connect the power cords to each of the PSUs in the enclosure. To ensure high availability, install and

connect both PSUs to different power sources.

4. Attach the power cords to the rack power distribution units (PDUs). Make sure that the two PSUs use separate power sources.
5. Press the power button to turn on the device.
6. Connect the 1-GbE network interface PORT 1 to the computer that's used to configure the physical device. PORT 1 is the dedicated management interface.
7. Connect one or more of PORT 2, PORT 3, PORT 4, PORT 5, or PORT 6 to the datacenter network/Internet.
 - If connecting PORT 2, use the RJ-45 network cable.
 - For the 10/25-GbE network interfaces, use the SFP+ copper cables.

Next steps

In this tutorial, you learned about Azure Stack Edge Pro FPGA topics such as how to:

- Unpack the device
- Rack the device
- Cable the device

Advance to the next tutorial to learn how to connect, set up, and activate your device.

[Connect and set up Azure Stack Edge Pro FPGA](#)

Tutorial: Connect, set up, and activate Azure Stack Edge Pro FPGA

9/21/2022 • 6 minutes to read • [Edit Online](#)

This tutorial describes how you can connect to, set up, and activate your Azure Stack Edge Pro FPGA device by using the local web UI.

The setup and activation process can take around 20 minutes to complete.

In this tutorial, you learn how to:

- Connect to a physical device
- Set up and activate the physical device

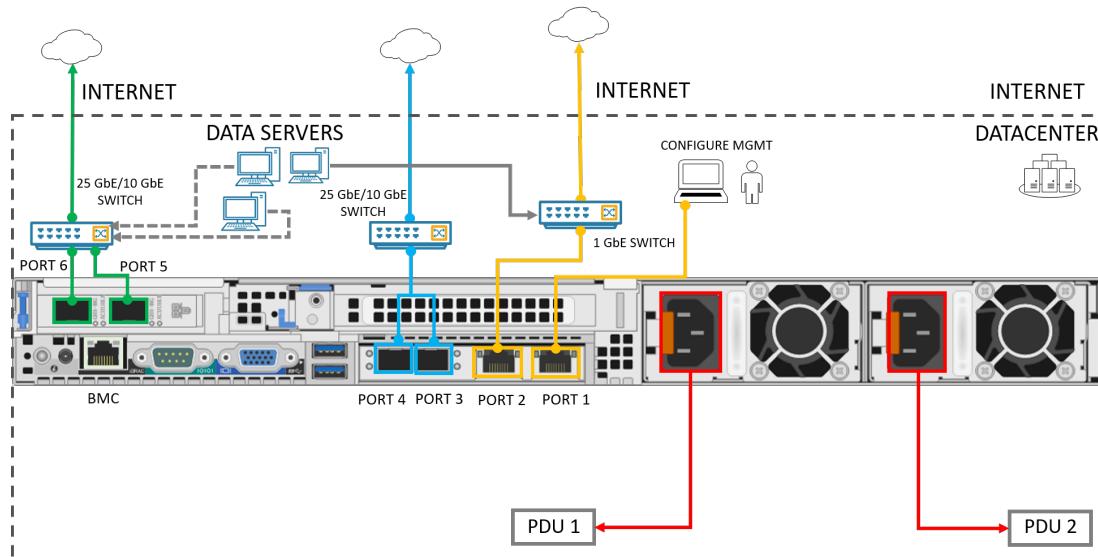
Prerequisites

Before you configure and set up your Azure Stack Edge Pro FPGA device, make sure that:

- You've installed the physical device as detailed in [Install Azure Stack Edge Pro FPGA](#).
- You have the activation key from the Azure Stack Edge service that you created to manage the Azure Stack Edge Pro FPGA device. For more information, go to [Prepare to deploy Azure Stack Edge Pro FPGA](#).

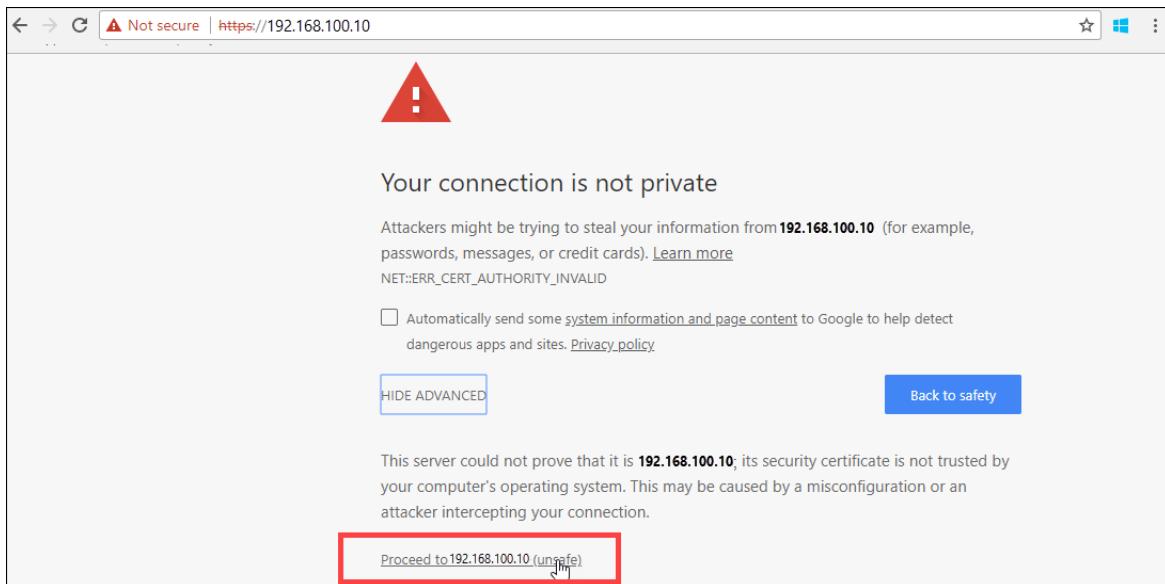
Connect to the local web UI setup

1. Configure the Ethernet adapter on your computer to connect to the Azure Stack Edge Pro FPGA device with a static IP address of 192.168.100.5 and subnet 255.255.255.0.
2. Connect the computer to PORT 1 on your device. Use the following illustration to identify PORT 1 on your device.



3. Open a browser window and access the local web UI of the device at <https://192.168.100.10>. This action may take a few minutes after you've turned on the device.

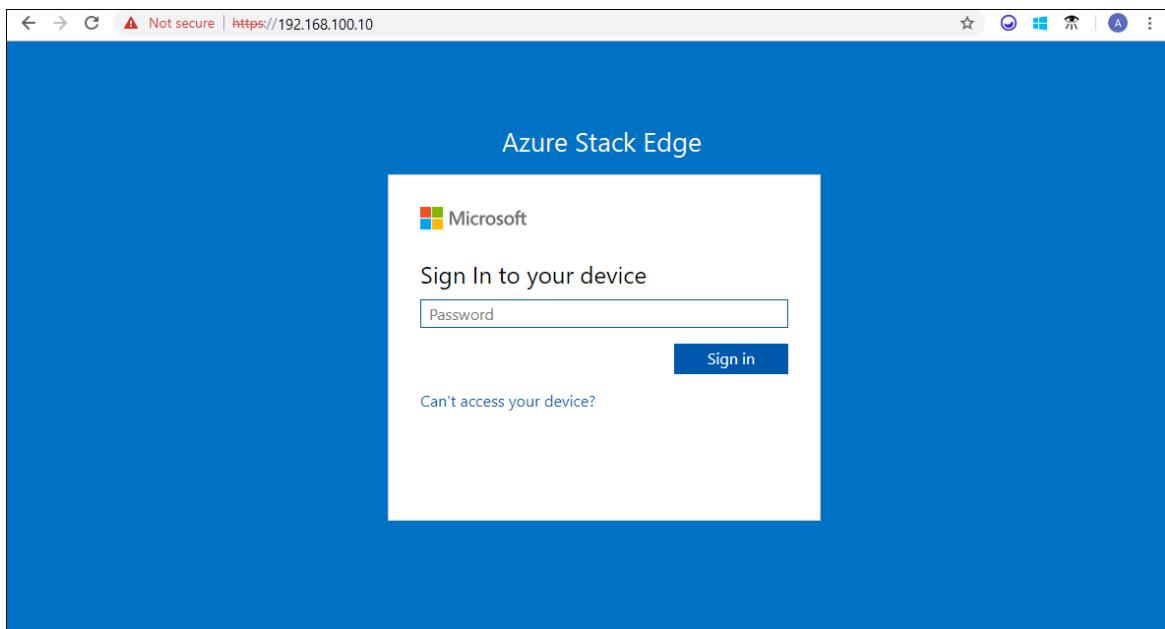
You see an error or a warning indicating that there is a problem with the website's security certificate.



4. Select **Continue to this webpage**.

These steps might vary depending on the browser you're using.

5. Sign in to the web UI of your device. The default password is *Password1*.



6. At the prompt, change the device administrator password.

The new password must contain between 8 and 16 characters. It must contain three of the following characters: uppercase, lowercase, numeric, and special characters.

You're now at the dashboard of your device.

Set up and activate the physical device

Your dashboard displays the various settings that are required to configure and register the physical device with the Azure Stack Edge service. The **Device name**, **Network settings**, **Web proxy settings**, and **Time settings** are optional. The only required settings are **Cloud settings**.

The screenshot shows the Azure Stack Edge dashboard with a red box highlighting the 'Dashboard' button in the top left. The left sidebar contains sections for Configuration (Device name, Network settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Hardware status, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The main area has three cards: 'Configuration' (Configure and activate your device, showing Network settings as Configured, Web proxy settings as Not enabled, Activation as Pending), 'Capacity' (Track device capacity usage, showing Usable capacity 11.34 TB and Available capacity 11.28 TB), and 'Device' (Monitor device health, showing Serial number 1D0QHQ2, Hardware status Healthy, Software status Healthy, and Software version 1.5.796.395).

1. In the left pane, select **Device name**, and then enter a friendly name for your device.

The friendly name must contain from 1 to 15 characters and have letters, numbers, and hyphens.

The screenshot shows the 'Device name' configuration page with a red box around the 'Device name' section in the left sidebar. The main area shows a field labeled 'Friendly name' containing 'MyAzureStackEdge1' with a checkmark, and a 'Apply settings' button below it.

2. (Optional) In the left pane, select **Network settings** and then configure the settings.

On your physical device, there are six network interfaces. PORT 1 and PORT 2 are 1-Gbps network interfaces. PORT 3, PORT 4, PORT 5, and PORT 6 are all 25-Gbps network interfaces that can also serve as 10-Gbps network interfaces. PORT 1 is automatically configured as a management-only port, and PORT 2 to PORT 6 are all data ports. The **Network settings** page is as shown below.

The screenshot shows the 'Network settings' configuration page with a red box around the 'Network settings' section in the left sidebar. It displays two network ports: Port 1 (F4-E9-D4-7C-45-37) and Port 2 (F4-E9-D4-7C-45-36). Both ports are set to 1 Gbps. Port 1 has IP settings (DHCP selected), IP address 192.168.100.10, Subnet 255.255.255.0, and RDMA mode iWarp. Port 2 has IP settings (Static selected), IP address 10.128.46.199, Subnet 255.255.252.0, Gateway 10.128.44.1, and Primary DNS 10.50.50.50.

As you configure the network settings, keep in mind:

- If DHCP is enabled in your environment, network interfaces are automatically configured. An IP address, subnet, gateway, and DNS are automatically assigned.
- If DHCP isn't enabled, you can assign static IPs if needed.
- You can configure your network interface as IPv4.

NOTE

We recommend that you do not switch the local IP address of the network interface from static to DHCP, unless you have another IP address to connect to the device. If using one network interface and you switch to DHCP, there would be no way to determine the DHCP address. If you want to change to a DHCP address, wait until after the device has registered with the service, and then change. You can then view the IPs of all the adapters in the **Device properties** in the Azure portal for your service.

3. (Optional) In the left pane, select **Web proxy settings**, and then configure your web proxy server. Although web proxy configuration is optional, if you use a web proxy, you can configure it on this page only.

The screenshot shows the Azure Stack Edge configuration interface. The left sidebar has a tree structure with sections like Configuration, Maintenance, and Troubleshooting. Under Configuration, 'Web proxy settings' is selected and highlighted with a red box. The main content area is titled 'Web proxy settings' and shows configuration options for a web proxy. It includes fields for 'Web proxy URL' (set to 'http://webproxyserver:8080'), 'Authentication' (with 'None' and 'NTLM' options, where 'None' is selected), 'Username' ('Edgewebproxyuser'), and 'Password' (redacted). At the bottom is a blue 'Apply settings' button, which is also highlighted with a red box.

On the **Web proxy settings** page, do the following:

- In the **Web proxy URL** box, enter the URL in this format: `http://host-IP address or FQDN:Port number`. HTTPS URLs are not supported.
- Under **Authentication**, select **None** or **NTLM**. If you enable compute and use IoT Edge module on your Azure Stack Edge Pro FPGA device, we recommend you set web proxy authentication to **None**. **NTLM** is not supported.
- If you're using authentication, enter a username and password.
- To validate and apply the configured web proxy settings, select **Apply settings**.

NOTE

Proxy-auto config (PAC) files are not supported. A PAC file defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL. Proxies that try to intercept and read all the traffic (then re-sign everything with their own certification) aren't compatible since the proxy's cert is not trusted. Typically transparent proxies work well with Azure Stack Edge Pro FPGA.

4. (Optional) In the left pane, select **Time settings**, and then configure the time zone and the primary and

secondary NTP servers for your device.

NTP servers are required because your device must synchronize time so that it can authenticate with your cloud service providers.

On the **Time settings** page, do the following:

- a. In the **Time zone** drop-down list, select the time zone that corresponds to the geographic location in which the device is being deployed. The default time zone for your device is PST. Your device will use this time zone for all scheduled operations.
- b. In the **Primary NTP server** box, enter the primary server for your device or accept the default value of time.windows.com.
Ensure that your network allows NTP traffic to pass from your datacenter to the internet.
- c. Optionally, in the **Secondary NTP server** box, enter a secondary server for your device.
- d. To validate and apply the configured time settings, select **Apply settings**.

The screenshot shows the 'Time settings' page in the Azure Stack Edge portal. The left sidebar has a 'Time settings' item selected, indicated by a red box. The main pane displays the configuration options: 'Time zone' set to '(UTC-08:00) Pacific Time (US & Canada)', 'Primary NTP server' set to 'time.windows.com', and 'Secondary NTP server' set to '10.10.1.1'. A large blue 'Apply settings' button at the bottom is also highlighted with a red box.

5. (Optional) In the left pane, select **Storage settings** to configure the storage resiliency on your device. This feature is currently in preview. By default, the storage on the device is not resilient and there is data loss if a data disk fails on the device. When you enable the Resilient option, the storage on the device will be reconfigured and the device can withstand the failure of one data disk with no data loss. Configuring the storage as resilient will reduce the usable capacity of your device.

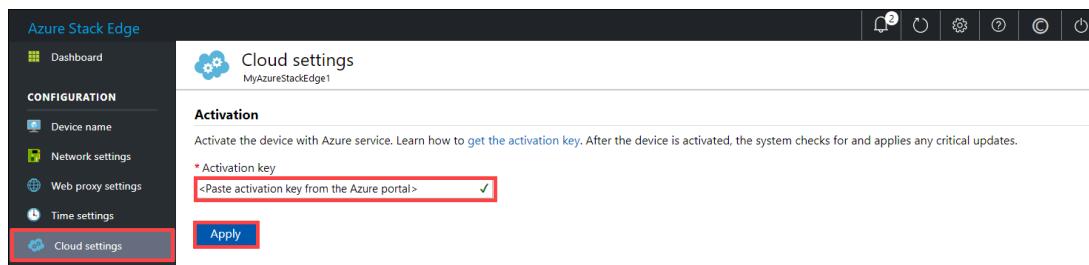
IMPORTANT

The resiliency can only be configured before you activate the device.

The screenshot shows the 'Storage settings' page in the Azure Stack Edge portal. The left sidebar has a 'Storage settings' item selected, indicated by a red box. The main pane displays the current storage resiliency as 'None' and the current usable capacity as '12.01 TB'. A dropdown menu for 'Storage resiliency' has two options: 'None' and 'Resilient', with 'Resilient' highlighted with a red box. A large blue 'Apply settings' button at the bottom is also highlighted with a red box.

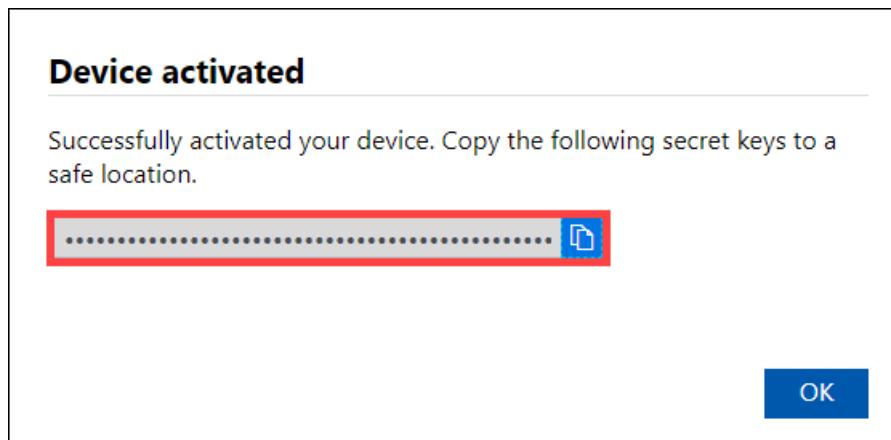
6. In the left pane, select **Cloud settings**, and then activate your device with the Azure Stack Edge service in the Azure portal.

- In the **Activation key** box, enter the activation key that you got in [Get the activation key](#) for Azure Stack Edge Pro FPGA.
- Select **Apply**.

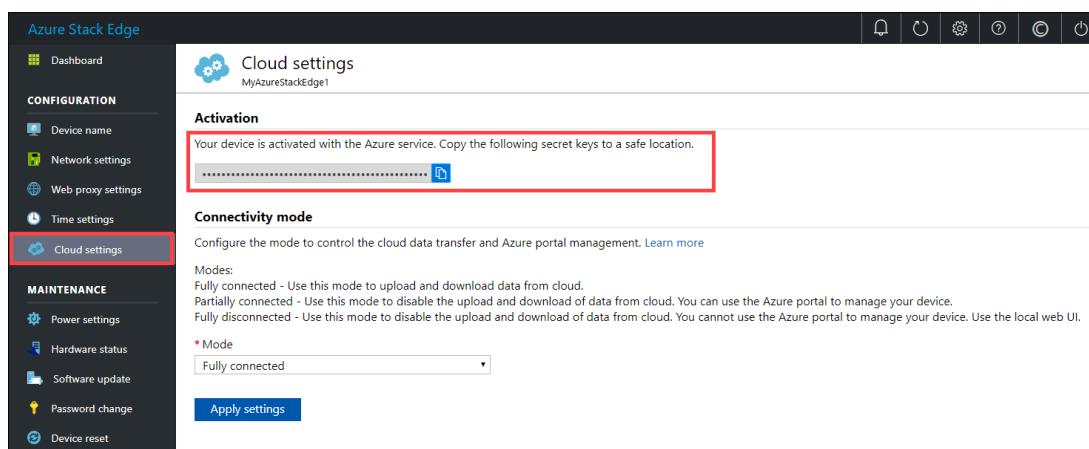


- First the device is activated. The device is then scanned for any critical updates and if available, the updates are automatically applied. You see a notification to that effect.

The dialog also has a recovery key that you should copy and save it in a safe location. This key is used to recover your data in the event the device can't boot up.



- You may need to wait several minutes after the update is successfully completed. The page updates to indicate that the device is successfully activated.



The device setup is complete. You can now add shares on your device.

Next steps

In this tutorial, you learned how to:

- Connect to a physical device

- Set up and activate the physical device

To learn how to transfer data with your Azure Stack Edge Pro FPGA device, see:

[Transfer data with Azure Stack Edge Pro FPGA.](#)

Tutorial: Transfer data with Azure Stack Edge Pro FPGA

9/21/2022 • 5 minutes to read • [Edit Online](#)

This tutorial describes how to add and connect to shares on your Azure Stack Edge Pro FPGA device. After you've added the shares, Azure Stack Edge Pro FPGA can transfer data to Azure.

This procedure can take around 10 minutes to complete.

In this tutorial, you learn how to:

- Add a share
- Connect to the share

Prerequisites

Before you add shares to Azure Stack Edge Pro FPGA, make sure that:

- You've installed your physical device as described in [Install Azure Stack Edge Pro FPGA](#).
- You've activated the physical device as described in [Connect, set up, and activate Azure Stack Edge Pro FPGA](#).

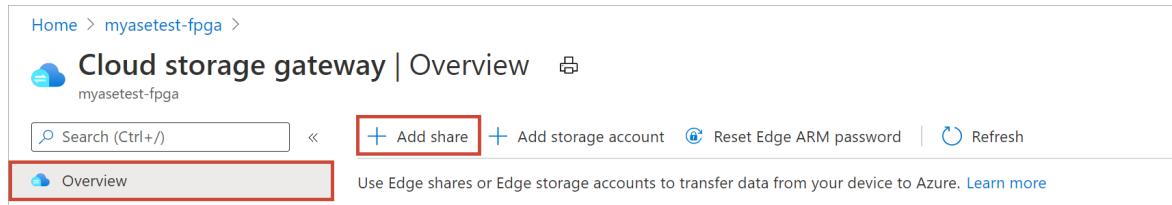
Add a share

To create a share, do the following procedure:

1. In the [Azure portal](#), select your Azure Stack Edge resource and then go to the **Overview**. Your device should be online. Select **Cloud storage gateway**.

The screenshot shows the Azure Stack Edge Pro Overview page. The left sidebar has a red box around the 'myasetest-fpga' device name. The main area has a red box around the 'Overview' tab. The 'Cloud storage gateway' section is highlighted with a red box. It contains a summary message 'Your device is running fine!', a table for 'Deployed edge services' (empty), and two cards for 'Edge services': 'IoT Edge' and 'Cloud storage gateway'. The 'Cloud storage gateway' card is also highlighted with a red box. Both cards have a 'How to get started?' link at the bottom.

2. Select **+ Add share** on the device command bar.



3. In the **Add share** pane, do the following procedure:

a. In the **Name** box, provide a unique name for your share.

The share name can have only lowercase letters, numerals, and hyphens. It must have between 3 to 63 characters and begin with a letter or a numeral. Hyphens must be preceded and followed by a letter or a numeral.

b. Select a **Type** for the share.

The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients.

Depending upon whether you choose SMB or NFS shares, the rest of the options vary slightly.

c. Provide a storage account where the share will reside.

IMPORTANT

Make sure that the Azure Storage account that you use does not have immutability policies set on it if you are using it with a Azure Stack Edge Pro FPGA or Data Box Gateway device. For more information, see [Set and manage immutability policies for blob storage](#).

d. In the **Storage service** drop-down list, select **Block Blob, Page Blob, or Files**.

The type of service you select depends on which format you want the data to use in Azure. In this example, because we want to store the data as block blobs in Azure, we select **Block Blob**. If you select **Page Blob**, make sure that your data is 512 bytes aligned. For example, a VHDX is always 512 bytes aligned.

e. Create a new blob container or use an existing one from the dropdown list. If creating a blob container, provide a container name. If a container doesn't already exist, it's created in the storage account with the newly created share name.

f. Depending on whether you've created an SMB share or an NFS share, do one of the following steps:

- **SMB share:** Under **All privilege local user**, select **Create new** or **Use existing**. If you create a new local user, enter a username and password, and then confirm the password. This action assigns permissions to the local user. After you've assigned the permissions here, you can use File Explorer to modify them.

If you select the **Allow only read operations** check box for this share data, you can specify read-only users.

Add share

X

myasetest

Share details

Name *

myasesmb1



Type * ⓘ

SMB

NFS

Use the share with Edge compute ⓘ



Configure as Edge local share ⓘ



Storage account * ⓘ



Storage service ⓘ



User details

Allow only read operations ⓘ



All privilege local user ⓘ



Create new



Use existing

User name *

Admin1



Password *

.....



Confirm password *

.....



Create

- **NFS share:** Enter the IP addresses of allowed clients that can access the share.

Add share

X

myasetest

Share details

Name *

mynfsshare



Type * ⓘ

SMB

NFS

Use the share with Edge compute ⓘ



(i)

Configure as Edge local share ⓘ



Storage account * ⓘ

mystorageaccount02



Storage service * ⓘ

Block Blob



Select blob container * ⓘ

Create new

Use existing

mynfsshare



User details

Allow only read operations ⓘ



Allowed client IP addresses

10.100.100.10



Delete

Enter an IP address.

Create

4. Select **Create** to create the share.

You're notified that the share creation is in progress. After the share is created with the specified settings, the **Shares** tile updates to reflect the new share.

Connect to the share

You can now connect to one or more of the shares that you created in the last step. Depending upon whether you have an SMB or an NFS share, the steps can vary.

Connect to an SMB share

On your Windows Server client connected to your Azure Stack Edge Pro FPGA device, connect to an SMB share by entering the commands:

1. In a command window, type:

```
net use \\<IP address of the device>\<share name> /u:<user name for the share>
```

2. When you're prompted to do so, enter the password for the share.

The sample output of this command is presented here.

```
Microsoft Windows [Version 10.0.16299.192]
(c) 2017 Microsoft Corporation. All rights reserved.

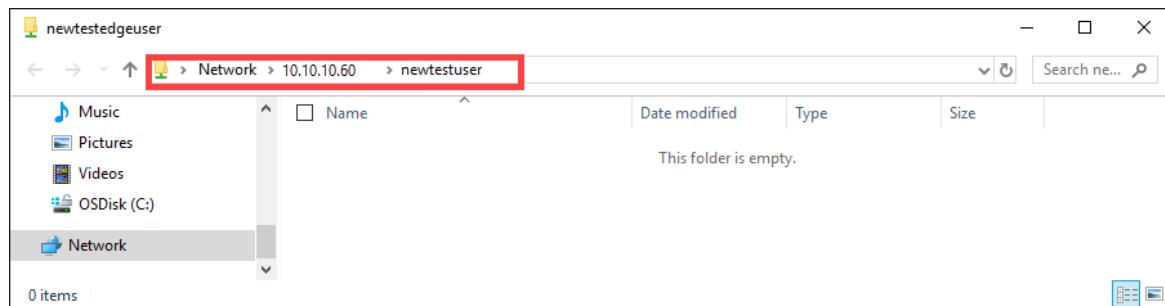
C:\Users\DataBoxEdgeUser>net use \\10.10.10.60\newtestuser /u:Tota11yNewUser
Enter the password for 'TotallyNewUser' to connect to '10.10.10.60':
The command completed successfully.

C:\Users\DataBoxEdgeUser>
```

3. On your keyboard, select Windows + R.

4. In the Run window, specify the `\\`, and then select OK.

File Explorer opens. You should now be able to view the shares that you created as folders. In File Explorer, double-click a share (folder) to view the content.



The data is written to these shares as it is generated and the device pushes the data to cloud.

Connect to an NFS share

On your Linux client connected to your Azure Stack Edge Pro FPGA device, do the following procedure:

1. Make sure that the client has NFSv4 client installed. To install NFS client, use the following command:

```
sudo apt-get install nfs-common
```

For more information, go to [Install NFSv4 client](#).

2. After the NFS client is installed, mount the NFS share that you created on your Azure Stack Edge Pro FPGA device by using the following command:

```
sudo mount -t nfs -o sec=sys,resvport <device IP>/<NFS shares on device> /home/username/<Folder on local Linux computer>
```

IMPORTANT

Use of `sync` option when mounting shares improves the transfer rates of large files. Before you mount the share, make sure that the directories that will act as mountpoints on your local computer are already created. These directories should not contain any files or subfolders.

The following example shows how to connect via NFS to a share on your Azure Stack Edge Pro FPGA device. The device IP is `10.10.10.60`. The share `mylinuxshare2` is mounted on the `ubuntuVM`. The share mount point is `/home/databoxubuntuhost/edge`.

```
sudo mount -t nfs -o sec=sys,resvport 10.10.10.60:/mylinuxshare2 /home/databoxubuntuhost/Edge
```

NOTE

The following caveats are applicable to this release:

- After a file is created in the share, renaming of the file isn't supported.
- Deleting a file from a share does not delete the entry in the storage account.

Next steps

In this tutorial, you learned about the following Azure Stack Edge Pro FPGA topics:

- Add a share
- Connect to share

To learn how to transform your data by using Azure Stack Edge Pro FPGA, advance to the next tutorial:

[Transform data with Azure Stack Edge Pro FPGA](#)

Tutorial: Transform the data with Azure Stack Edge Pro FPGA

9/21/2022 • 5 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role on your Azure Stack Edge Pro FPGA device. After you configure the compute role, Azure Stack Edge Pro FPGA can transform data before sending it to Azure.

This procedure can take around 10 to 15 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Add shares
- Add a compute module
- Verify data transform and transfer

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro FPGA device, make sure that:

- You've activated your Azure Stack Edge Pro FPGA device as described in [Connect, set up, and activate Azure Stack Edge Pro FPGA](#).

Configure compute

To configure compute on your Azure Stack Edge Pro FPGA, you'll create an IoT Hub resource.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**. In the right-pane, select **IoT Edge**.

The screenshot shows the Azure Stack Edge Overview page for the device 'myasetest-fpga'. The left sidebar lists navigation options: Home, Overview (which is selected and highlighted with a red box), Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Properties, Order details), Edge services (IoT Edge, Cloud storage gateway), Monitoring (Device events, Alerts), and Essentials. The main content area displays a message 'Your device is running fine!' and a table for 'Deployed edge services' which is currently empty. Below this is a section for 'Edge services' containing two tiles: 'IoT Edge' and 'Cloud storage gateway'. The 'IoT Edge' tile is highlighted with a red box and contains the text: 'Manage containerized application at edge and integrate with IoT Hub.' and a 'How to get started?' link. The 'Cloud storage gateway' tile contains the text: 'Seamlessly send your data to Azure Storage account.' and a 'How to get started?' link.

2. On the **Enable IoT Edge** tile, select **Add**. This enables the IoT Edge service that lets you deploy IoT Edge

modules locally on your device.

The screenshot shows the 'IoT Edge | Overview' blade for the resource 'myasetest-fpga'. The left sidebar has three items: 'Overview' (selected and highlighted with a red box), 'Modules', and 'Triggers'. The main content area is titled 'Get started with IoT Edge' and contains a section 'Enable IoT Edge service' with instructions: 'Enable IoT Edge service to deploy IoT Edge modules locally on your device.' It lists two steps: '1 Set up your on-premises network for Edge computing.' and '2 Configure your Azure subscription for cloud management.'. A large blue 'Add' button is centered below the instructions. Below the main content, there's a 'What's next' section with the text 'Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services.'

3. On the **Create IoT Edge service** blade, input the following:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can use the same subscription as that used by the Azure Stack Edge resource.
Resource group	Select a resource group for your IoT Hub resource. You can use the same resource group as that used by the Azure Stack Edge resource.
IoT Hub	Choose from New or Existing . By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource. In each case, the IoT Hub resource uses the same subscription and resource group that is used by the Azure Stack Edge resource.
Name	Enter a name for your IoT Hub resource.

Home > myasetest-fpga > IoT Edge >

Create IoT Edge service

Azure Stack Edge Pro - FPGA

Basics Review + Create

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription * ⓘ Edge Gateway Test

Resource group * ⓘ myaserg

IoT Hub * ⓘ Create new Use existing
myasetest-iothub1

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

IoT Edge device: myasetest-fpga-edge
IoT Gateway device: myasetest-fpga-storagegateway

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

4. Select **Review + Create**. The IoT Hub resource creation takes a couple minutes. After the IoT Hub resource is created, the **Overview** updates to indicate that the IoT Edge service is running.

Home > myasetest-fpga >

IoT Edge | Overview

Azure Stack Edge Pro - FPGA

Search (Ctrl+)

+ Add module + Add trigger ⏪ Refresh configuration Remove Refresh

Overview

IoT Edge service is running fine!

Start processing the data using IoT Edge modules. [Learn more](#)

Modules

IoT Edge modules are containers that run Azure services, third-party services, or your own code.
To read data from Edge local shares for processing and uploading it to cloud, add a Module. If multiple containers are deployed, which are chained together for pipeline processing, go to [Azure IoT Hub](#).

Add module

Triggers

Add triggers to start processing at a repeated interval or on file events such as creation of a file, modification of a file on a share.

Add trigger

Edge Shares

For container to store or transfer files and folders to Azure Storage account (other than temp data), create a share.

Configure Shares

Edge Storage account

For container to transfer unstructured data like binary, audio, or video streaming data to Azure Storage account, create a storage account.

Configure Storage account

Network bandwidth usage

If containers uploads data to cloud using shares, configure network bandwidth usage across multiple time-of-day schedules.

Configure Bandwidth schedule

Configuring Edge compute on myasetest... 10:44 PM
Successfully completed the operation.

When the IoT Edge service is configured on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

To confirm that the Edge compute role has been configured, select **IoT Edge service > Properties** and view the IoT device and the IoT Edge device.

The screenshot shows the 'IoT Edge | Properties' blade for the 'myasetest-fpga' resource. The left sidebar has a red box around the 'Properties' item. The main area displays the following properties:

IoT Hub	myasetest-iohub1
IoT Edge device	myasetest-fpga-edge
IoT device for storage gateway	myasetest-fpga-storagegateway
Platform	Linux

Add shares

For the simple deployment in this tutorial, you'll need two shares: one Edge share and another Edge local share.

1. Add an Edge share on the device by doing the following steps:
 - a. In your Azure Stack Edge resource, go to **IoT Edge > Shares**.
 - b. From the command bar, select **+ Add share**.
 - c. On the **Add share** blade, provide the share name and select the share type.
 - d. To mount the Edge share, select the check box for **Use the share with Edge compute**.
 - e. Select the **Storage account**, **Storage service**, an existing user, and then select **Create**.

The screenshot shows the 'Add share' blade for the 'myasetest-fpga' resource. The left sidebar has a red box around the 'Shares' item. The right pane shows the 'Add share' form with the following details:

- Share details:**
 - Name: myasesmb
 - Type: SMB (selected)
 - Use the share with Edge compute** checkbox is checked (highlighted with a red box).
- Configure as Edge local share** checkbox is unchecked.
- Storage account**: mytestsa1
- Storage service**: Block Blob
- Select blob container**: Create new (radio button selected), myasesmb
- User details:**
 - Allow only read operations checkbox is unchecked.
 - All privilege local user radio button selected.
 - User name: Admin
 - Password and Confirm password fields are filled with '*****'.

A red box highlights the 'Create' button at the bottom of the form.

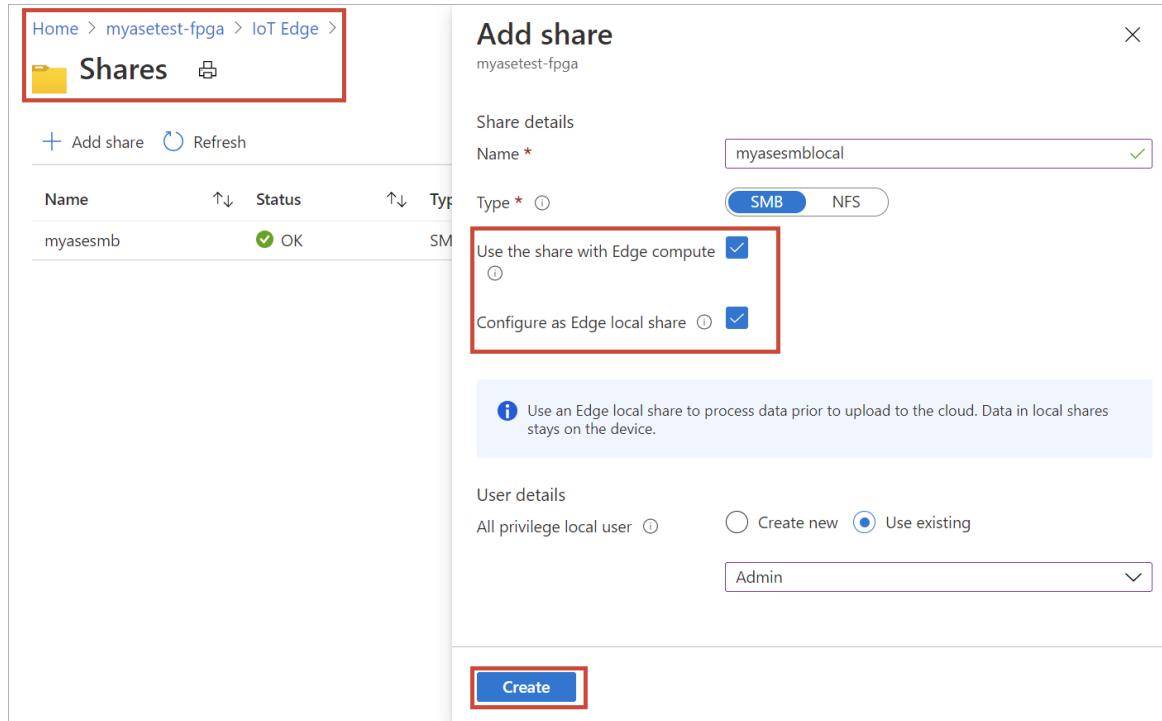
If you created a local NFS share, use the following remote sync (rsync) command option to copy files onto the share:

```
rsync <source file path> < destination file path>
```

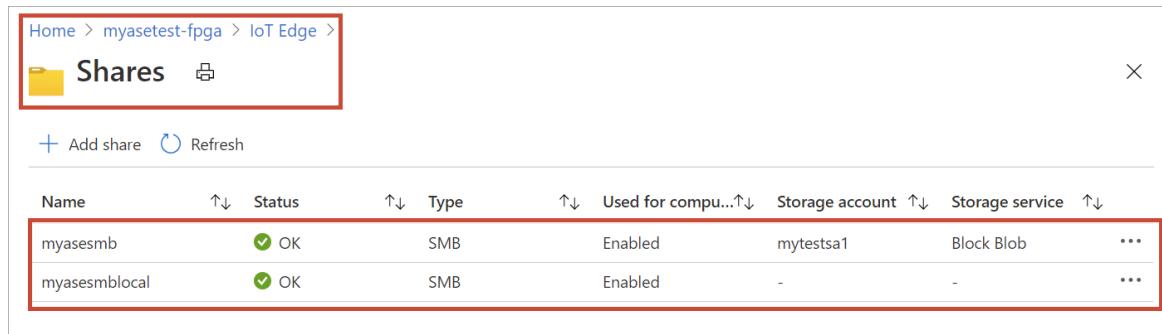
For more information about the rsync command, go to [Rsync documentation](#).

The Edge share is created, and you'll receive a successful creation notification. The share list might be updated, but you must wait for the share creation to be completed.

2. Add an Edge local share on the Edge device by repeating all the steps in the preceding step and selecting the check box for **Configure as Edge local share**. The data in the local share stays on the device.



3. Go to the **IoT Edge > Shares** to see the updated list of shares.



Add a module

You could add a custom or a pre-built module. There are no custom modules on this Edge device. To learn how to create a custom module, go to [Develop a C# module for your Azure Stack Edge Pro FPGA device](#).

In this section, you add a custom module to the IoT Edge device that you created in [Develop a C# module for your Azure Stack Edge Pro FPGA](#). This custom module takes files from an Edge local share on the Edge device and moves them to an Edge (cloud) share on the device. The cloud share then pushes the files to the Azure storage account that's associated with the cloud share.

1. Go to **IoT Edge > Modules**. From the device command bar, select **+ Add module**.
2. In the **Configure and add module** blade, input the following values:

FIELD	VALUE
-------	-------

FIELD	VALUE
Name	A unique name for the module. This module is a docker container that you can deploy to the IoT Edge device that's associated with your Azure Stack Edge Pro FPGA.
Image URI	The image URI for the corresponding container image for the module.
Credentials required	If checked, username and password are used to retrieve modules with a matching URL.
Input share	Select an input share. The Edge local share is the input share in this case. The module used here moves files from the Edge local share to an Edge share where they are uploaded into the cloud.
Output share	Select an output share. The Edge share is the output share in this case.
Trigger type	Select from File or Schedule . A file trigger fires whenever a file event occurs such as a file is written to the input share. A scheduled trigger fires up based on a schedule defined by you.
Trigger name	A unique name for your trigger.
Environment variables	Optional information that will help define the environment in which your module will run.

Configure and add module

* Name ✓

* Image URI ✓

Credentials required

* Username ✓

* Password ✓

* Input share ✓

* Output share ✓

* Trigger type ✓

* Trigger name ✓

Environment variables

<input type="text"/>	<input type="text"/>
----------------------	----------------------

Add

3. Select **Add**. The module gets added. The IoT Edge > Overview page updates to indicate that the

module is deployed.

The screenshot shows the IoT Edge Overview page for the device 'myasetest-fpga'. The 'Overview' section is highlighted with a red box. It displays the message 'IoT Edge service is running fine!' and 'Start processing the data using IoT Edge modules. [Learn more](#)'. Below this, there are two main sections: 'Modules' and 'Triggers', each with a count of 1. The 'Modules' section shows 'mymodule1'. The 'Triggers' section shows 'mytrigger1'. At the bottom, there are three configuration links: 'Configure Shares', 'Configure Storage account', and 'Configure Bandwidth schedule'.

Verify data transform and transfer

The final step is to ensure that the module is connected and running as expected. The run-time status of the module should be running for your IoT Edge device in the IoT Hub resource.

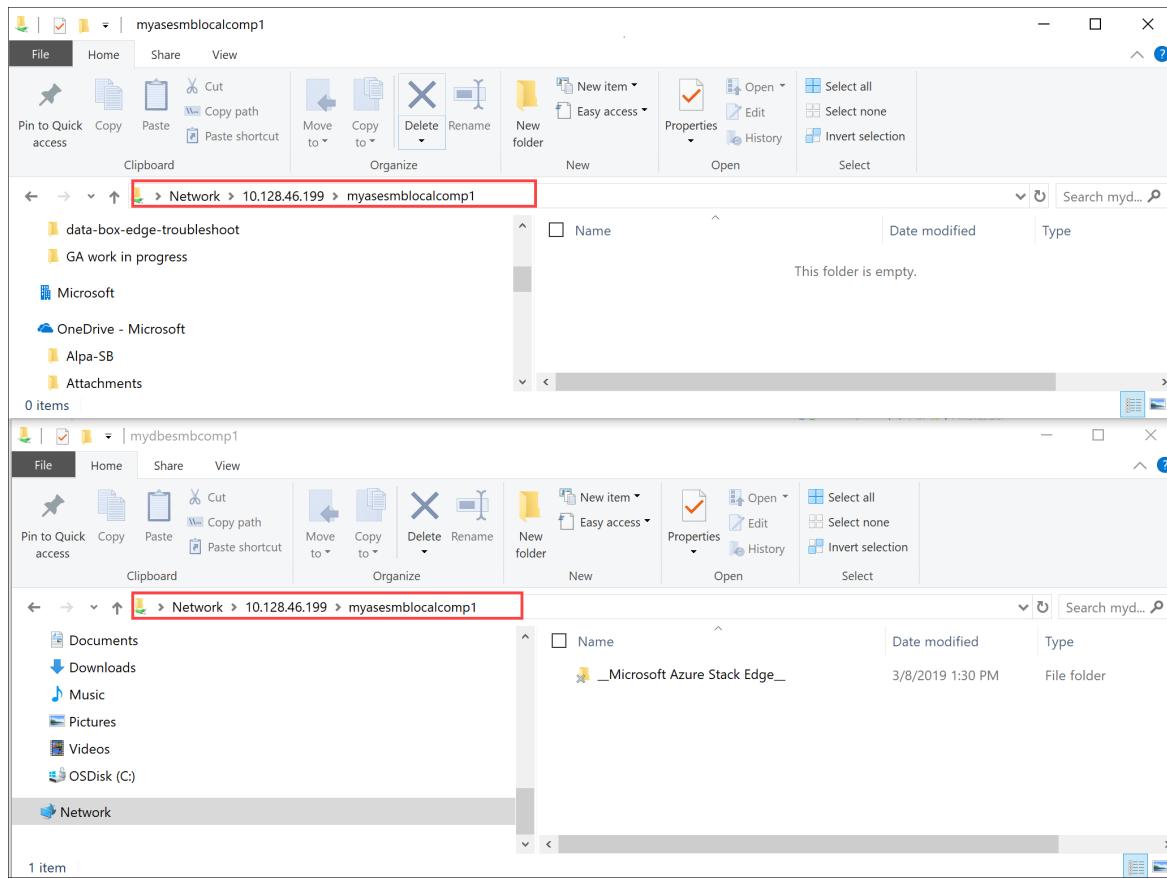
To verify that the module is running, do the following:

1. Select the **Add module** tile. This takes you to the **Modules** blade. In the list of modules, identify the module you deployed. The runtime status of the module you added should be *running*.

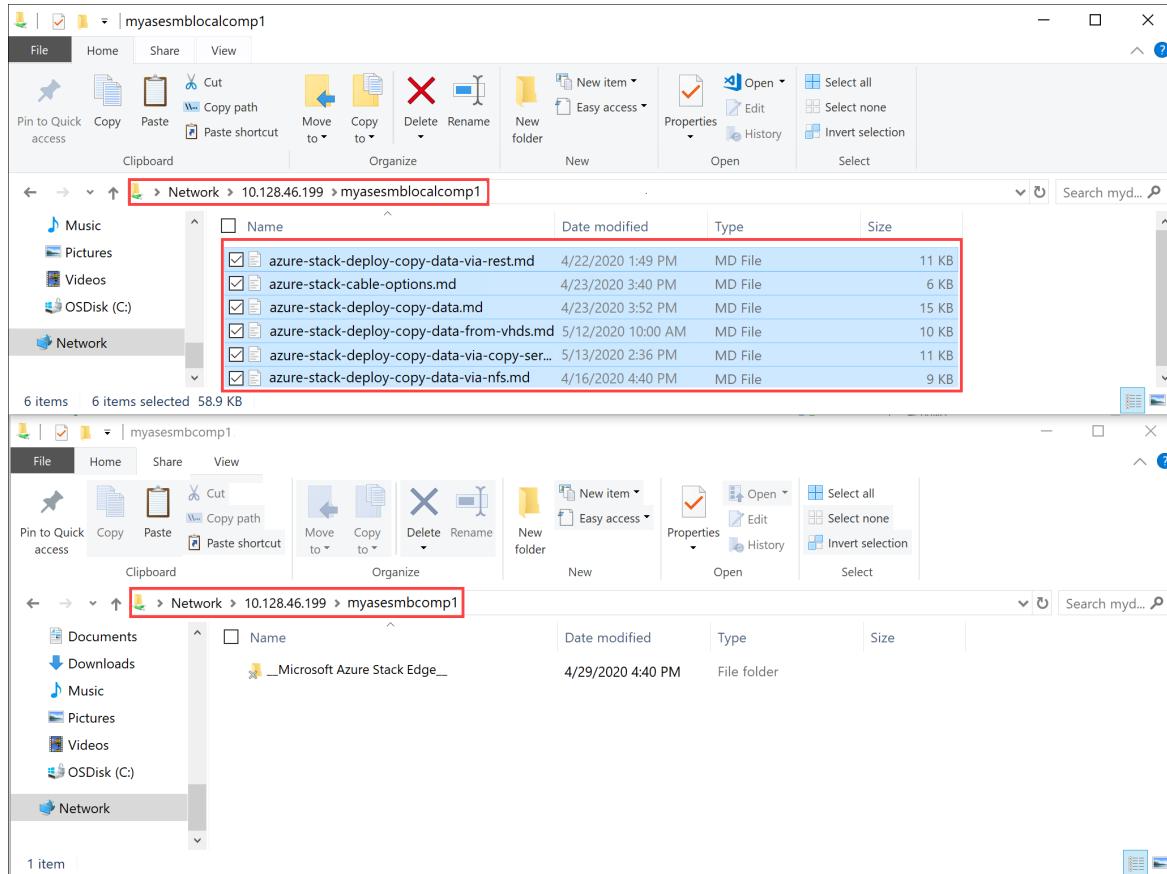
The screenshot shows the IoT Edge Modules blade. The 'Overview' section is highlighted with a red box. The 'Modules' section is also highlighted with a red box. The table lists three modules: '\$edgeAgent', '\$edgeHub', and 'mymodule1'. The 'mymodule1' row is also highlighted with a red box. The columns in the table are: Name, Type, Specified In Deploy..., Reported By Device, Runtime status, Exit code, and three ellipsis (...).

Name	Type	Specified In Deploy...	Reported By Device	Runtime status	Exit code	...
\$edgeAgent	IoT Edge System module	✓ Yes	○ No	-	-	...
\$edgeHub	IoT Edge System module	✓ Yes	○ No	-	-	...
mymodule1	IoT Edge Custom module	✓ Yes	○ No	-	-	...

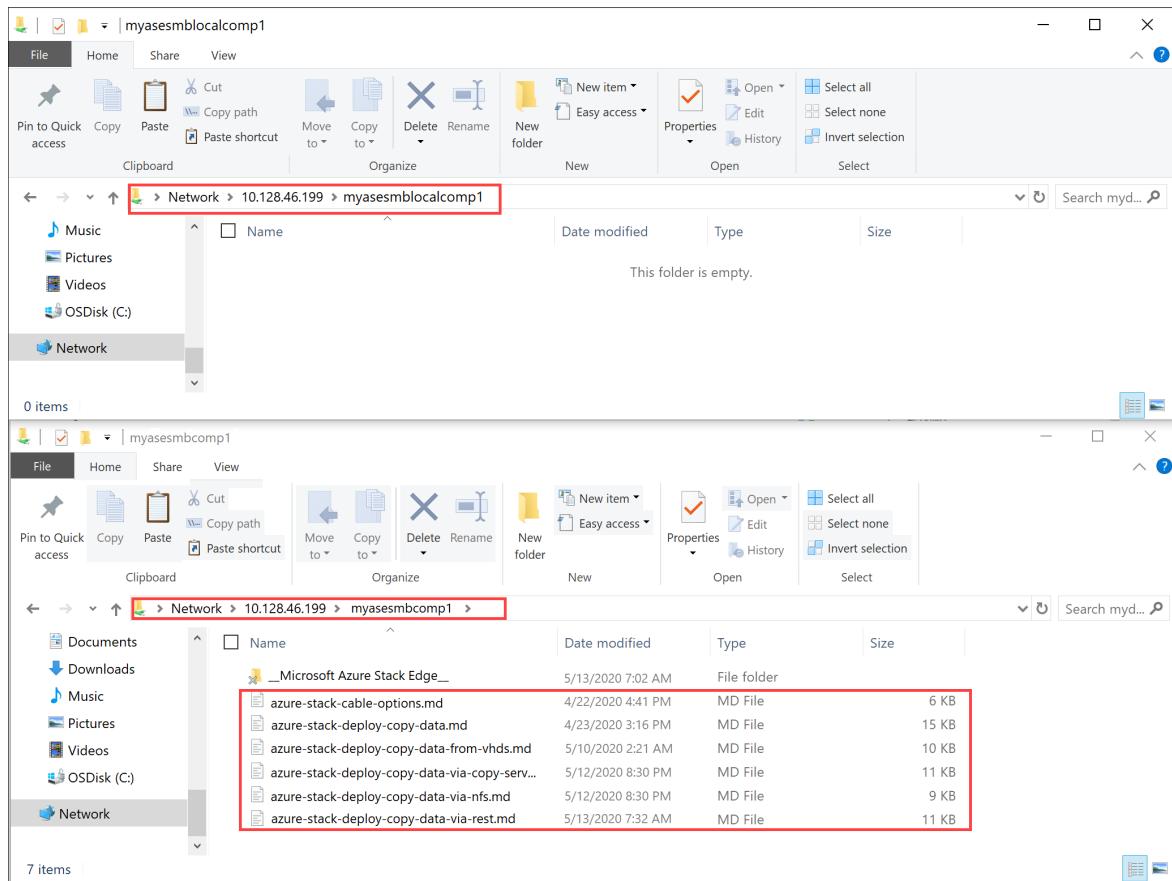
2. In File Explorer, connect to both the Edge local and Edge shares you created previously.



3. Add data to the local share.



The data gets moved to the cloud share.



The data is then pushed from the cloud share to the storage account. To view the data, go to the Storage Explorer.

You have completed the validation process.

Next steps

In this tutorial, you learned how to:

- Configure compute
- Add shares
- Add a compute module
- Verify data transform and transfer

To learn how to administer your Azure Stack Edge Pro FPGA device, see:

[Use local web UI to administer a Azure Stack Edge Pro FPGA](#)

Tutorial: Transform data with Azure Stack Edge Pro FPGA for advanced deployment flow

9/21/2022 • 8 minutes to read • [Edit Online](#)

This tutorial describes how to configure a compute role for an advanced deployment flow on your Azure Stack Edge Pro FPGA device. After you configure the compute role, Azure Stack Edge Pro FPGA can transform data before sending it to Azure.

Compute can be configured for simple or advanced deployment flow on your device.

CRITERIA	SIMPLE DEPLOYMENT	ADVANCED DEPLOYMENT
Intended for	IT administrators	Developers
Type	Use Azure Stack Edge service to deploy modules	Use IoT Hub service to deploy modules
Modules deployed	Single	Chained or multiple modules

This procedure can take around 20 to 30 minutes to complete.

In this tutorial, you learn how to:

- Configure compute
- Add shares
- Add a trigger
- Add a compute module
- Verify data transform and transfer

Prerequisites

Before you set up a compute role on your Azure Stack Edge Pro FPGA device, make sure that:

- You've activated your Azure Stack Edge Pro FPGA device as described in [Connect, set up, and activate Azure Stack Edge Pro FPGA](#).

Configure compute

To configure compute on your Azure Stack Edge Pro FPGA, you'll create an IoT Hub resource.

1. In the Azure portal of your Azure Stack Edge resource, go to **Overview**. In the right-pane, select the **IoT Edge** tile.

Home > myasetest-fpga

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Properties

Order details

Edge services

IoT Edge

Cloud storage gateway

Monitoring

Device events

Alerts

Update device

Reset device password

Return device

Feedback

Delete

Refresh

JSON View

Your device is running fine!

Deployed edge services

Name	Status
No deployed services	

Edge services

IoT Edge

Manage containerized application at edge and integrate with IoT Hub.

[How to get started?](#)

Cloud storage gateway

Seamlessly send your data to Azure Storage account.

[How to get started?](#)

2. On the **Enable IoT Edge service** tile, select **Add**. This action enables IoT Edge service that lets you deploy IoT Edge modules locally on your device.

Home > myasetest-fpga >

IoT Edge | Overview

Overview

Modules

Triggers

Properties

Search (Ctrl+ /)

Add module

Add trigger

Refresh configuration

Remove

Refresh

Get started with IoT Edge

Enable IoT Edge service

Enable IoT Edge service to deploy IoT Edge modules locally on your device.

To enable the service:

1 Set up your on-premises network for Edge computing.
2 Configure your Azure subscription for cloud management.

Add

Steps to deploy IoT Edge services

What's next

Deploy and manage IoT Edge modules from Azure using Azure IoT Edge services.

3. On the **Create IoT Edge service**, input the following:

FIELD	VALUE
Subscription	Select a subscription for your IoT Hub resource. You can select the same subscription as that used by the Azure Stack Edge resource.
Resource group	Enter a name for the resource group for your IoT Hub resource. You can select the same resource group as that used by the Azure Stack Edge resource.

FIELD	VALUE
IoT Hub	Choose from New or Existing . By default, a Standard tier (S1) is used to create an IoT resource. To use a free tier IoT resource, create one and then select the existing resource.
Name	Accept the default or enter a name for your IoT Hub resource.

Home > myasetest-fpga > IoT Edge > **Create IoT Edge service** Azure Stack Edge Pro - FPGA

Basics Review + Create

Connect the device to a new standard tier (S1) Azure IoT Hub. To use a free tier, select an existing IoT Hub resource. [Learn more](#)

Subscription *	Edge Gateway Test
Resource group *	myaserg
IoT Hub *	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing <input type="text" value="myasetest-iothub1"/>

It takes time to create a new IoT Hub. Under the new IoT Hub, an IoT Edge device and IoT device are configured. [Pricing details for IoT Hub](#).

IoT Edge device: myasetest-fpga-edge
IoT Gateway device: myasetest-fpga-storagegateway

Only Linux container image types are supported.

Review + Create Previous Next: Review + Create

4. Select **Review + Create**. The IoT Hub resource creation takes a couple minutes. After the IoT Hub resource is created, the **Overview** updates to indicate that the IoT Edge service is running.

When the IoT Edge service is configured on the Edge device, it creates two devices: an IoT device and an IoT Edge device. Both devices can be viewed in the IoT Hub resource. An IoT Edge Runtime is also running on this IoT Edge device. At this point, only the Linux platform is available for your IoT Edge device.

To confirm that the Edge compute role has been configured, select **IoT Edge service > Properties** and view the IoT device and the IoT Edge device.

Home > myasetest-fpga > IoT Edge

IoT Edge | Properties Azure Stack Edge Pro - FPGA

Search (Ctrl+ /) Refresh

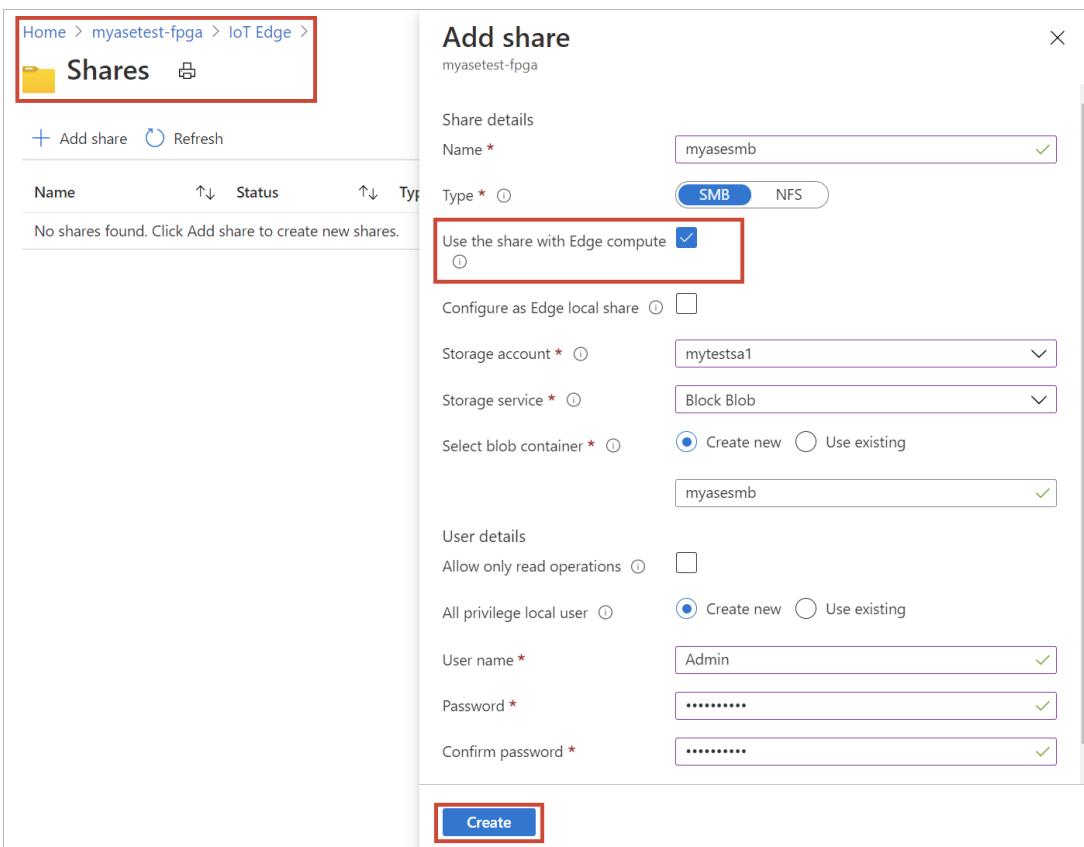
- Overview
- Modules
- Triggers
- Properties**

IoT Hub	myasetest-iothub1
IoT Edge device	myasetest-fpga-edge
IoT device for storage gateway	myasetest-fpga-storagegateway
Platform	Linux

Add shares

For the advanced deployment in this tutorial, you'll need two shares: one Edge share and another Edge local share.

1. Add an Edge share on the device by doing the following steps:
 - a. In your Azure Stack Edge resource, go to **IoT Edge > Shares**.
 - b. On the **Shares** page, from the command bar, select **+ Add share**.
 - c. On the **Add share** blade, provide the share name and select the share type.
 - d. To mount the Edge share, select the check box for **Use the share with Edge compute**.
 - e. Select the **Storage account**, **Storage service**, an existing user, and then select **Create**.



After the Edge share is created, you'll receive a successful creation notification. The share list is updated to reflect the new share.

2. Add an Edge local share on the Edge device by repeating all the steps in the preceding step and selecting the check box for **Configure as Edge local share**. The data in the local share stays on the device.

Add share

Share details

Name * myasesmblocal

Type * SMB

Use the share with Edge compute

Configure as Edge local share

User details

All privilege local user Create new Use existing Admin

Create

- On the **Shares** blade, you see the updated list of shares.

Name	Status	Type	Used for compute	Storage account	Storage service
myasesmb	OK	SMB	Enabled	mytestsa1	Block Blob
myasesmblocal	OK	SMB	Enabled	-	-

- To view the properties of the newly created local share, select the share from the list. In the **Local mount point for Edge compute modules** box, copy the value corresponding to this share.

You'll use this local mount point when you deploy the module.

myasesmb

Status OK

Type SMB

Mounted (Used for compute) Enabled

Storage account mytestsa1

Storage account container myasesmb

Last updated time -

Last update error logs -

Local mount point for Edge compute modules /home/databox-edge/hostgatewayshares/myasesmb

Select users Admin

- To view the properties of the Edge share that you created, select the share from the list. In the **Local mount point for Edge compute modules** box, copy the value corresponding to this share.

You'll use this local mount point when you deploy the module.

Add a trigger

1. Go to your Azure Stack Edge resource and then go to **IoT Edge > Triggers**. Select **+ Add trigger**.

2. In the **Add trigger** blade, input the following values.

FIELD	VALUE
Trigger name	A unique name for your trigger.
Trigger type	Select File trigger. A file trigger fires whenever a file event occurs such as a file is written to the input share. A scheduled trigger on the other hand, fires up based on a schedule defined by you. For this example, we need a file trigger.
Input share	Select an input share. The Edge local share is the input share in this case. The module used here moves files from the Edge local share to an Edge share where they are uploaded into the cloud.

Add trigger

X

Triggers help invoke functions in a module. Triggers can be file event or scheduled. [Learn more](#)

Name *

mytrigger1



Type * ⓘ

File (When file is written to input share)



Input Edge local share * ⓘ

myasesmblocal



Add

3. You are notified after the trigger is created. The list of triggers is updated to display the newly created trigger. Select the trigger you just created.

The screenshot shows the 'IoT Edge | Triggers' page. The left sidebar has links for Home, myasetest-fpga, IoT Edge, Overview, Modules, Triggers (which is selected and highlighted with a red box), and Properties. The main area has a search bar, a 'Add trigger' button, a refresh button, and a filter bar. A table lists the trigger: Name: mytrigger1, Type: File, Associated share: myasesmblocal. The 'mytrigger1' row is also highlighted with a red box.

4. Copy and save the sample route. You will modify this sample route and use it later in the IoT Hub.

```
"samplerroute": "FROM /* WHERE topic = 'mydbesmbedge-localshare1' INTO  
BrokeredEndpoint(\"/modules/modulename/inputs/input1\")"
```

mytrigger1

X

myasetest-fpga

Delete

Type

File

Associated share

myasesmblocal

Example route for Edge compute module

```
"samplerroute": "FROM /* WHERE topic =  
'myasesmblocal' INTO  
BrokeredEndpoint(\"/modules/modulename/  
put1\")"
```

Copy to clipboard

Add a module

There are no custom modules on this Edge device. You could add a custom or a pre-built module. To learn how to create a custom module, go to [Develop a C# module for your Azure Stack Edge Pro FPGA device](#).

In this section, you add a custom module to the IoT Edge device that you created in [Develop a C# module for your Azure Stack Edge Pro FPGA](#). This custom module takes files from an Edge local share on the Edge device and moves them to an Edge (cloud) share on the device. The cloud share then pushes the files to the Azure storage account that's associated with the cloud share.

1. Go to your Azure Stack Edge resource and then go to **IoT Edge > Overview**. On the **Modules** tile, select **Go to Azure IoT Hub**.

The screenshot shows the Azure Stack Edge Overview page. The top navigation bar includes 'Home > myasetest-fpga > IoT Edge | Overview'. Below the navigation is a search bar and a toolbar with buttons for 'Add module', 'Add trigger', 'Refresh configuration', 'Remove', and 'Refresh'. A message 'IoT Edge service is running fine!' is displayed. The left sidebar has links for 'Overview', 'Modules', 'Triggers', and 'Properties'. The main area has a 'Modules' card with a sub-section about IoT Edge modules being containers for Azure services. A callout box highlights the 'Add module' button. Below this are sections for 'Edge Shares' and 'Edge Storage account'. The right side has a 'Triggers' card with a 'Add trigger' button. At the bottom, there are 'Configure Shares' and 'Configure Storage account' buttons.

2. In your IoT Hub resource, go to **IoT Edge device** and then select your IoT Edge device.

The screenshot shows the Azure IoT Hub MyIoTHubService1 - IoT Edge page. The top navigation bar includes 'Home > MyIoTHubService1 - IoT Edge'. Below the navigation is a search bar and a toolbar with buttons for 'Add an IoT Edge device', 'Add an IoT Edge deployment', 'Refresh', and 'Delete'. A message about deploying services to on-premises devices is displayed. The left sidebar has links for 'Locks', 'Export template', 'Explorers' (Query explorer, IoT devices), 'Automatic Device Management' (IoT Edge, IoT device configuration), 'Messaging' (File upload, Message routing), 'Resiliency', and 'Manual failover (preview)'. The main area has tabs for 'IoT Edge devices' (selected) and 'IoT Edge deployments'. Below is a table titled 'IoT Edge devices' with columns: Field, Operator, Value, and a checkbox. A query editor is shown below the table. The table lists one device: 'myazurestackedge1-e...' with a checked checkbox. The table also has columns for DEVICE ID, RUNTIME RESPONSE, IOT EDGE MODULE COUNT, CONNECTED CLIENT COU..., and DEPLOYMENT COUNT.

3. On **Device details**, select **Set Modules**.

Device details

myazurystackedge1-edge

Save Set modules Manage child devices Device twin Regenerate keys Refresh

Device ID: myazurystackedge1-edge

Primary key: [REDACTED]

Secondary key: [REDACTED]

Connection string (primary key): [REDACTED]

Connection string (secondary key): [REDACTED]

Connect this device to an IoT hub: Enable Disable

Edge runtime response: N/A

Modules IoT Edge hub connections Deployments

Verify that your modules are included in the deployment, and whether your modules have been reported by the device. Click Set modules to change the modules that appear. Each device can host a maximum of 20 modules.

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CODE
\$edgeAgent	IoT Edge System module	<input checked="" type="radio"/> No	<input checked="" type="checkbox"/> Yes	running	0
\$edgeHub	Module Identity	N/A	N/A	N/A	N/A

4. Under Add Modules, do the following:

- Enter the name, address, user name, and password for the container registry settings for the custom module. The name, address, and listed credentials are used to retrieve modules with a matching URL. To deploy this module, under **Deployment modules**, select **IoT Edge module**. This IoT Edge module is a docker container that you can deploy to the IoT Edge device that's associated with your Azure Stack Edge Pro FPGA device.

Home > MyIoTHubService1 - IoT Edge > Device details > Set modules

Set modules

1 Add Modules (optional) 2 Specify Routes (optional) 3 Review Deployment

Container Registry Settings

NAME	ADDRESS	USER NAME	PASSWORD
filmove	edgecompute.azurecr.io	edgecompute	<Password>

Deployment Modules

+ Add Delete

IoT Edge Module DESIRED STATUS

Azure Stream Analytics Module

Azure Machine Learning Module

Previous Next Submit

- Specify the settings for the IoT Edge custom module. Input the following values.

FIELD	VALUE
Name	A unique name for the module. This module is a docker container that you can deploy to the IoT Edge device associated with your Azure Stack Edge Pro FPGA.
Image URI	The image URI for the corresponding container image for the module.
Credentials required	If checked, username and password are used to retrieve modules with a matching URL.

In the **Container Create Options** box, enter the local mount points for the Edge modules that you copied in the preceding steps for the Edge share and Edge local share.

IMPORTANT

The paths used here are mounted into your container, so they must match what the functionality in your container expects. If you're following [Create a custom module](#), the code specified in that module expects the copied paths. Do not modify these paths.

In the **Container Create Options** box, you can paste the following sample:

```
{
  "HostConfig":
  {
    "Binds":
    [
      "/home/hcsshares/mydbesmbedge-localshare1:/home/input",
      "/home/hcsshares/mydbesmbedge-share1:/home/output"
    ]
  }
}
```

Provide any environmental variables used for your module. Environmental variables provide optional information that help define the environment in which your module runs.

IoT Edge Custom Modules

Specify the settings for an IoT Edge custom module. [Learn how to create a module.](#)

Name filemove ✓

Image URI edgecompute.azurecr.io/filemovemodule2:0.0.3-amd64 ✓

Environment Variables

NAME	VALUE

Container Create Options

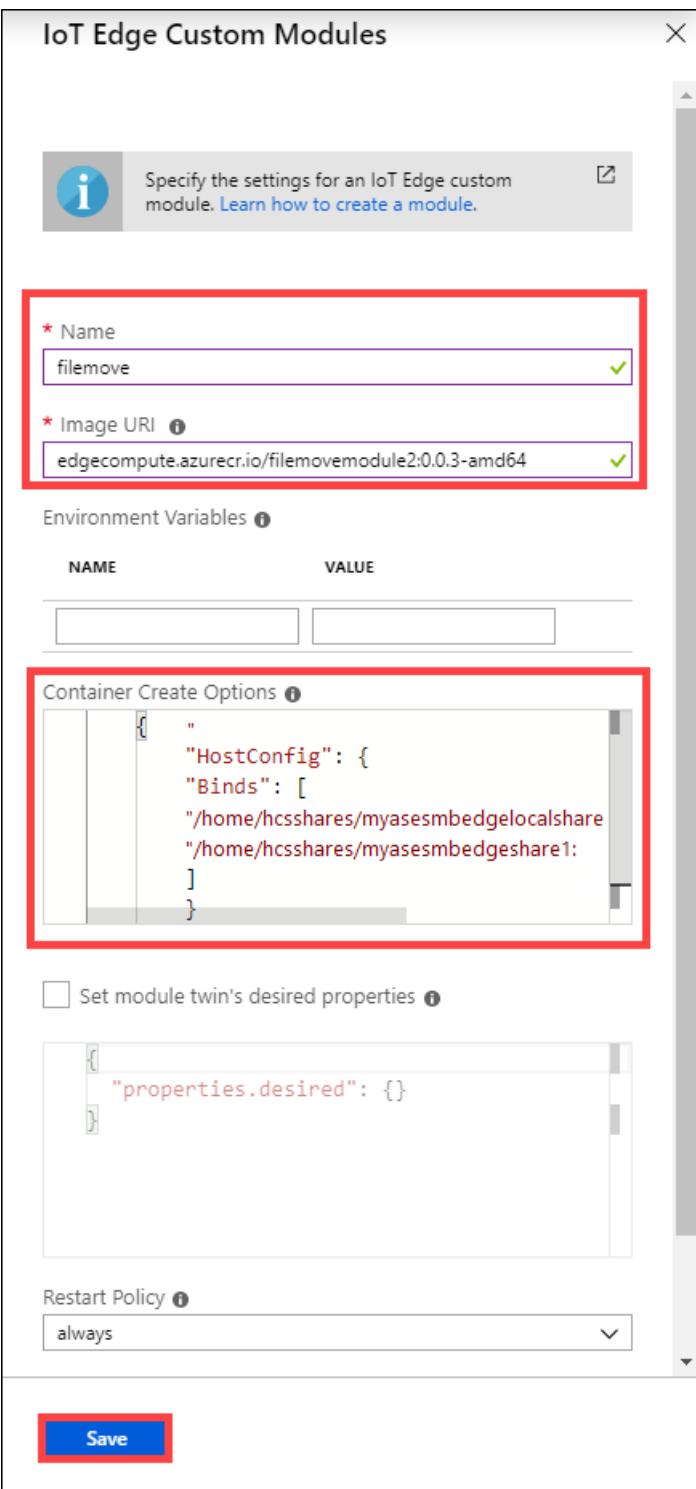
```
[{"HostConfig": {"Binds": ["/home/hcsshares/myasesmbedgelocalshare", "/home/hcsshares/myasesmbedgeshare1"]}]}
```

Set module twin's desired properties

```
[{"properties.desired": {}}]
```

Restart Policy always

Save



c. If necessary, configure the advanced Edge runtime settings, and then click **Next**.

You can specify credentials to container registries hosting module images. Listed credentials are used to retrieve modules with a matching URL. The Edge Agent will report error 500 if it can't find a container registry setting for a module.

Container Registry Settings

NAME	ADDRESS	USER NAME	PASSWORD
filenmove	edgecompute.azurecr.io	edgecompute	<Password>

An IoT Edge module is a Docker container you can deploy to IoT Edge devices. It communicates with other modules and sends data to the IoT Edge runtime. Using this UI you can import Azure Service IoT Edge modules or specify the settings for an IoT Edge module. Setting modules on each device will be counted towards the quota and throttled based on the IoT Hub tier and units. For example, for S1 tier, modules can be set 10 times per second if no other updates are happening in the IoT Hub.

Deployment Modules

NAME		DESIRED STATUS
<input checked="" type="checkbox"/>	filenmove	running

[Configure advanced Edge Runtime settings](#)

Previous [Next](#) Submit

5. Under Specify Routes, set routes between modules.

You can set routes between modules, which gives you the flexibility to send messages where they need to go without the need for additional services to process messages or to write additional code.

```

1 {
2   "routes": {
3     "route": "FROM /messages/* INTO $upstream"
4   }
5 }
```

Previous [Next](#) Submit

You can replace `route` with the following route string that you copied earlier. In this example, enter the name of the local share that will push data to the cloud share. Replace the `modulename` with the name of the module. Select **Next**.

```
"route": "FROM /* WHERE topic = 'mydbesmbedgelocalshare1' INTO
BrokeredEndpoint(\"/modules/filenmove/inputs/input1\")"
```

You can set routes between modules, which gives you the flexibility to send messages where they need to go without the need for additional services to process messages or to write additional code.

```

1 {
2   "routes": {
3     "route": "FROM /* WHERE topic = 'myasesmbedgelocalshare1' INTO BrokeredEndpoint(\"/modules/filenmove/inputs/input1\")"
4   }
5 }
```

Previous [Next](#) Submit

6. Under Review deployment, review all the settings, and then select **Submit** to submit the module for deployment.

Below is a summary of the current deployment.

```

1   "modulesContent": {
2     "$edgeAgent": {
3       "properties.desired": {
4         "modules": {
5           "filemove": {
6             "settings": {
7               "image": "edgecompute.azurecr.io/filemove:0.0.1-amd64",
8               "createOptions": "{\"HostConfig\":{\"Binds\":[\"/home/hccshares/myasesembedgeshare1:/home/LocalShare\", \"/home/hccshares/myasesembedgeshare1:/home/CloudShare\"]}}"
9             },
10            "type": "docker",
11            "status": "running",
12            "restartPolicy": "always",
13            "version": "1.0"
14          }
15        }
16      }

```

Submit

This action starts the module deployment. After the deployment is complete, the **Runtime status** of module is **running**.

Device details
myazurystackedge1-edge

Save Set modules Manage child devices Device twin Regenerate keys Refresh

Device Id: myazurystackedge1-edge

Primary key: ***** Copy Reset

Secondary key: ***** Copy Reset

Connection string (primary key): ***** Copy Reset

Connection string (secondary key): ***** Copy Reset

Connect this device to an IoT hub: Enable Disable

Edge runtime response: N/A Copy

Modules IoT Edge hub connections Deployments

Verify that your modules are included in the deployment, and whether your modules have been reported by the device. Click Set modules to change the modules that appear. Each device can host a maximum of 20 modules.

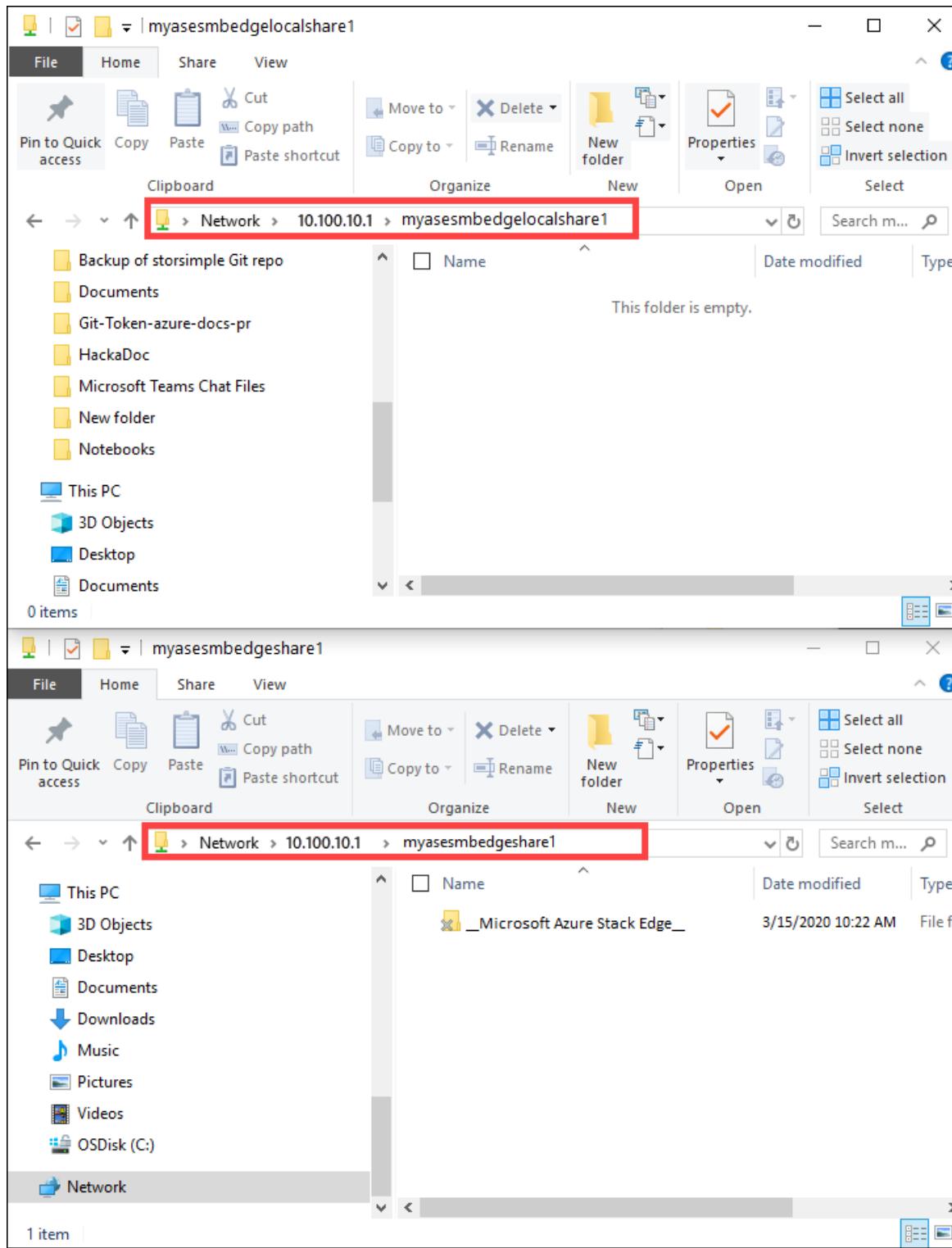
NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CODE
\$edgeAgent	IoT Edge System module	✓ Yes	✓ Yes	running	0
\$edgeHub	IoT Edge System module	✓ Yes	✓ Yes	running	0
filermove	IoT Edge Custom module	✓ Yes	✓ Yes	running	0

Verify data transform, transfer

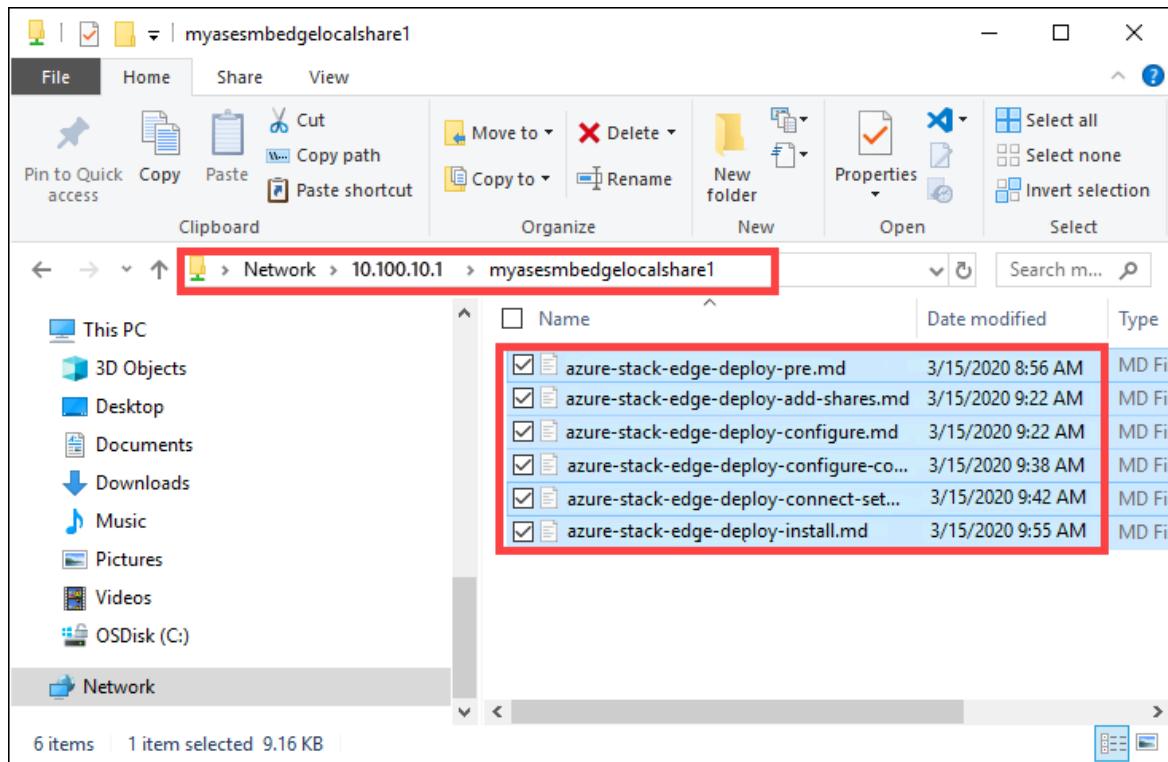
The final step is to ensure that the module is connected and running as expected. The run-time status of the module should be running for your IoT Edge device in the IoT Hub resource.

Take the following steps to verify data transform and transfer to Azure.

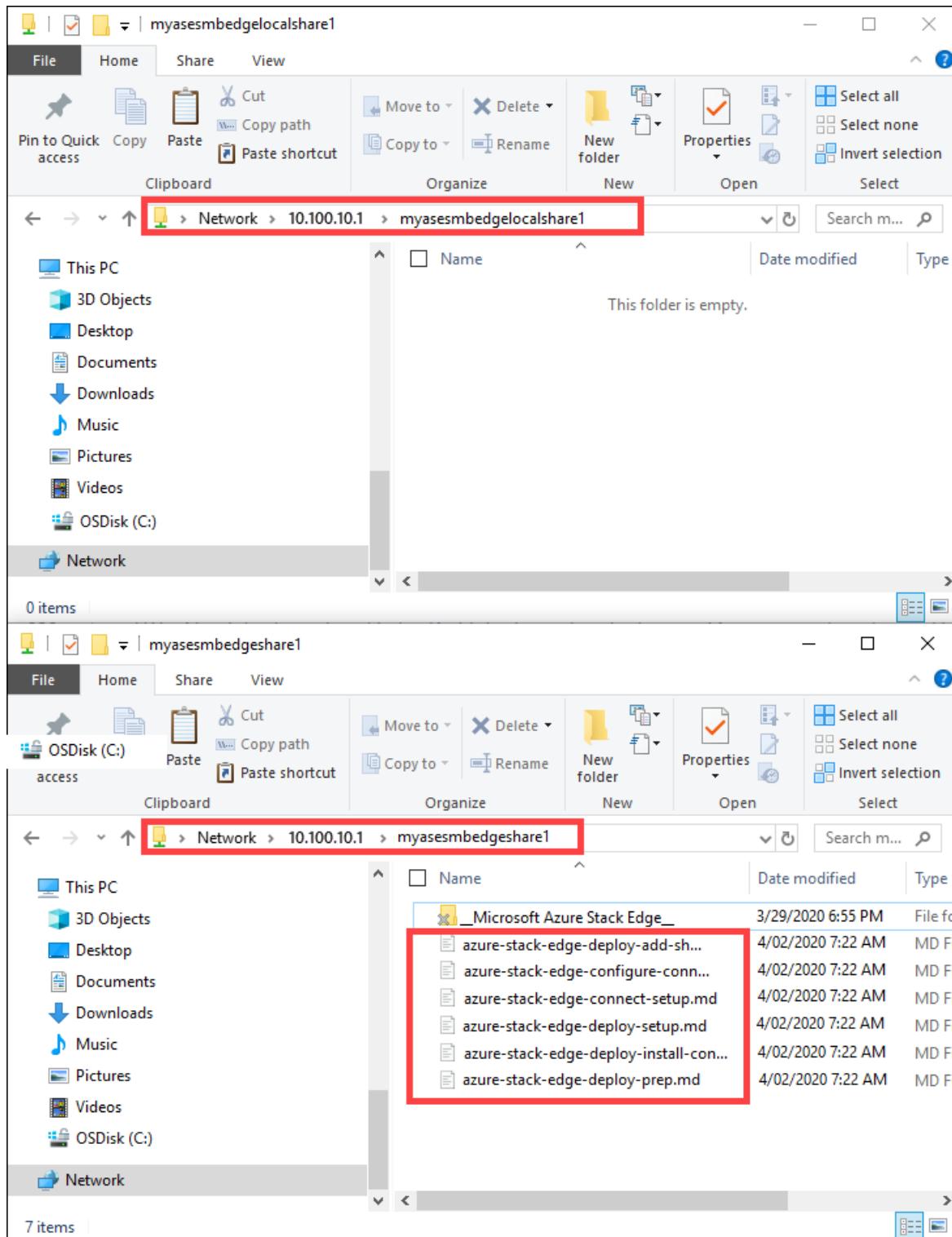
1. In File Explorer, connect to both the Edge local and Edge shares you created previously.



2. Add data to the local share.



The data gets moved to the cloud share.



The data is then pushed from the cloud share to the storage account. To view the data, go to your storage account and then select **Storage Explorer**. You can view the uploaded data in your storage account.

The screenshot shows the Azure Storage Explorer interface for the storage account "mytestsa1".

Left Panel: Shows navigation links including Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, and Storage Explorer (preview).

Right Panel: Shows the "myasesmbedgeshare1" file share under "FILE SHARES". The "myasesmbedgeshare1" folder contains several files, all of which are highlighted with a red box.

NAME	ACCESS TIER	ACCESS TIER LAST MODIFIED	LAST MODIFIED	BLOB TYPE	CONTENT TYPE	SIZE	STATUS	REMAIN
Microsoft Azure Stack Edge			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	7.4 KB	Active	
azure-stack-edge-deploy-add-shares.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	14.0 KB	Active	
azure-stack-edge-configure-compute-advanced.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	6.7 KB	Active	
azure-stack-edge-deploy-configure-compute.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	9.2 KB	Active	
azure-stack-edge-deploy-connect-setup-activate.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	9.2 KB	Active	
azure-stack-edge-deploy-install.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	11.0 KB	Active	
azure-stack-edge-deploy-prep.md			3/27/2020, 9:22:37 AM	Block Blob	application/octet-stream	9.2 KB	Active	

A message at the bottom of the right panel says: "Showing 1 to 7 of 7 cached items".

You have completed the validation process.

Next steps

In this tutorial, you learned how to:

- Configure compute
- Add shares
- Add a trigger
- Add a compute module
- Verify data transform and transfer

To learn how to administer your Azure Stack Edge Pro FPGA device, see:

[Use local web UI to administer a Azure Stack Edge Pro FPGA](#)

Azure Stack Edge Pro FPGA system requirements

9/21/2022 • 7 minutes to read • [Edit Online](#)

This article describes the important system requirements for your Microsoft Azure Stack Edge Pro FPGA solution and for the clients connecting to Azure Stack Edge Pro FPGA. We recommend that you review the information carefully before you deploy your Azure Stack Edge Pro FPGA. You can refer back to this information as necessary during the deployment and subsequent operation.

The system requirements for the Azure Stack Edge Pro FPGA include:

- **Software requirements for hosts** - describes the supported platforms, browsers for the local configuration UI, SMB clients, and any additional requirements for the clients that access the device.
- **Networking requirements for the device** - provides information about any networking requirements for the operation of the physical device.

Supported OS for clients connected to device

Here is a list of the supported operating systems for clients or hosts connected to your device. These operating system versions were tested in-house.

OPERATING SYSTEM/PLATFORM	VERSIONS
Windows Server	2012 R2 2016 2019
Windows	8, 10
SUSE Linux	Enterprise Server 12 (x86_64)
Ubuntu	16.04.3 LTS
CentOS	7.0
Mac OS	10.14.1

Supported protocols for clients accessing device

Here are the supported protocols for clients accessing your device.

PROTOCOL	VERSIONS	NOTES
SMB	2.X, 3.X	SMB 1 isn't supported.
NFS	3.0, 4.1	Mac OS is not supported with NFS v4.1.

Supported storage accounts

Here is a list of the supported storage accounts for your device.

STORAGE ACCOUNT	NOTES
Classic	Standard
General Purpose	Standard; both V1 and V2 are supported. Both hot and cool tiers are supported.

Supported storage types

Here is a list of the supported storage types for the device.

FILE FORMAT	NOTES
Azure block blob	
Azure page blob	
Azure Files	

Supported browsers for local web UI

Here is a list of the browsers supported for the local web UI for the virtual device.

BROWSER	VERSIONS	ADDITIONAL REQUIREMENTS/NOTES
Google Chrome	Latest version	
Microsoft Edge	Latest version	
Internet Explorer	Latest version	If Enhanced Security features are enabled, you may not be able to access local web UI pages. Disable enhanced security, and restart your browser.
FireFox	Latest version	

Networking port requirements

Port requirements for Azure Stack Edge Pro FPGA

The following table lists the ports that need to be opened in your firewall to allow for SMB, cloud, or management traffic. In this table, *in* or *inbound* refers to the direction from which incoming client requests access to your device. *Out* or *outbound* refers to the direction in which your Azure Stack Edge Pro FPGA device sends data externally, beyond the deployment, for example, outbound to the internet.

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	NOTES

Port No.	In or Out	Port Scope	Required	Notes
TCP 80 (HTTP)	Out	WAN	No	Outbound port is used for internet access to retrieve updates. The outbound web proxy is user configurable.
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound port is used for accessing data in the cloud. The outbound web proxy is user configurable.
UDP 123 (NTP)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based NTP server.
UDP 53 (DNS)	Out	WAN	In some cases See notes	This port is required only if you're using an internet-based DNS server. We recommend using a local DNS server.
TCP 5985 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTP.
TCP 5986 (WinRM)	Out/In	LAN	In some cases See notes	This port is required to connect to the device via remote PowerShell over HTTPS.
UDP 67 (DHCP)	Out	LAN	In some cases See notes	This port is required only if you're using a local DHCP server.
TCP 80 (HTTP)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management. Accessing the local UI over HTTP will automatically redirect to HTTPS.
TCP 443 (HTTPS)	Out/In	LAN	Yes	This port is the inbound port for local UI on the device for local management.

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	NOTES
TCP 445 (SMB)	In	LAN	In some cases See notes	This port is required only if you are connecting via SMB.
TCP 2049 (NFS)	In	LAN	In some cases See notes	This port is required only if you are connecting via NFS.

Port requirements for IoT Edge

Azure IoT Edge allows outbound communication from an on-premises Edge device to Azure cloud using supported IoT Hub protocols. Inbound communication is only required for specific scenarios where Azure IoT Hub needs to push down messages to the Azure IoT Edge device (for example, Cloud To Device messaging).

Use the following table for port configuration for the servers hosting Azure IoT Edge runtime:

PORT NO.	IN OR OUT	PORT SCOPE	REQUIRED	GUIDANCE
TCP 443 (HTTPS)	Out	WAN	Yes	Outbound open for IoT Edge provisioning. This configuration is required when using manual scripts or Azure IoT Device Provisioning Service (DPS).

For complete information, go to [Firewall and port configuration rules for IoT Edge deployment](#).

URL patterns for firewall rules

Network administrators can often configure advanced firewall rules based on the URL patterns to filter the inbound and the outbound traffic. Your Azure Stack Edge Pro FPGA device and the service depend on other Microsoft applications such as Azure Service Bus, Azure Active Directory Access Control, storage accounts, and Microsoft Update servers. The URL patterns associated with these applications can be used to configure firewall rules. It is important to understand that the URL patterns associated with these applications can change. These changes require the network administrator to monitor and update firewall rules for your Azure Stack Edge Pro FPGA as and when needed.

We recommend that you set your firewall rules for outbound traffic, based on Azure Stack Edge Pro FPGA fixed IP addresses, liberally in most cases. However, you can use the information below to set advanced firewall rules that are needed to create secure environments.

NOTE

- The device (source) IPs should always be set to all the cloud-enabled network interfaces.
- The destination IPs should be set to [Azure datacenter IP ranges](#).

URL patterns for gateway feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.com/* https://*.servicebus.windows.net/* https://login.windows.net	Azure Stack Edge / Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.com	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.windows.net/* https://*.data.microsoft.com http://*.msftncsi.com	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://go.microsoft.com http://dl.delivery.mp.microsoft.com https://dl.delivery.mp.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry
https://(vault-name).vault.azure.net:443	Key Vault

URL patterns for compute feature

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.mscl.io	
https://*.azuredcrio	Personal and third-party container registries (optional)
https://*.azure-devices.net	IoT Hub access (required)

URL patterns for gateway for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://*.databoxedge.azure.us/* https://*.servicebus.usgovcloudapi.net/* https://login.microsoftonline.us	Azure Stack Edge / Data Box Gateway service Azure Service Bus Authentication Service
http://*.backup.windowsazure.us	Device activation
http://crl.microsoft.com/pki/* http://www.microsoft.com/pki/*	Certificate revocation
https://*.core.usgovcloudapi.net/* https://*.data.microsoft.com http://*.msftncsi.com	Azure storage accounts and monitoring
http://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://*.ws.microsoft.com https://*.ws.microsoft.com http://*.mp.microsoft.com	Microsoft Update servers
http://*.deploy.akamaitechnologies.com	Akamai CDN
https://*.partners.extranet.microsoft.com/*	Support package
http://*.data.microsoft.com	Telemetry service in Windows, see the update for customer experience and diagnostic telemetry

URL patterns for compute for Azure Government

URL PATTERN	COMPONENT OR FUNCTIONALITY
https://mcr.microsoft.com	Microsoft container registry (required)
https://*.cdn.msccr.com	
https://*.azure-devices.us	IoT Hub access (required)
https://*.azuredcr.us	Personal and third-party container registries (optional)

Internet bandwidth

The devices are designed to continue to operate when your internet connection is slow or gets interrupted. In normal operating conditions, we recommend that you use:

- A minimum of 10-Mbps download bandwidth to ensure the device stays updated.
- A minimum of 20-Mbps dedicated upload and download bandwidth to transfer files.

Compute sizing considerations

Use your experience while developing and testing your solution to ensure there is enough capacity on your Azure Stack Edge Pro FPGA device and you get the optimal performance from your device.

Factors you should consider include:

- **Container specifics** - Think about the following.
 - How many containers are in your workload? You could have a lot of lightweight containers versus a few resource-intensive ones.
 - What are the resources allocated to these containers versus what are the resources they are consuming?
 - How many layers do your containers share?
 - Are there unused containers? A stopped container still takes up disk space.
 - In which language are your containers written?
- **Size of the data processed** - How much data will your containers be processing? Will this data consume disk space or the data will be processed in the memory?
- **Expected performance** - What are the desired performance characteristics of your solution?

To understand and refine the performance of your solution, you could use:

- The compute metrics available in the Azure portal. Go to your Azure Stack Edge resource and then go to **Monitoring > Metrics**. Look at the **Edge compute - Memory usage** and **Edge compute - Percentage CPU** to understand the available resources and how are the resources getting consumed.
- The monitoring commands available via the PowerShell interface of the device such as:
 - `dkr stats` to get a live stream of container(s) resource usage statistics. The command supports CPU, memory usage, memory limit, and network IO metrics.
 - `dkr system df` to get information regarding the amount of disk space used.
 - `dkr image [prune]` to clean up unused images and free up space.
 - `dkr ps --size` to view the approximate size of a running container.

For more information on the available commands, go to [Monitor and troubleshoot compute modules](#).

Finally, make sure that you validate your solution on your dataset and quantify the performance on Azure Stack Edge Pro FPGA before deploying in production.

Next step

- [Deploy your Azure Stack Edge Pro FPGA](#)

Azure Stack Edge limits

9/21/2022 • 3 minutes to read • [Edit Online](#)

Consider these limits as you deploy and operate your Microsoft Azure Stack Edge Pro GPU or Azure Stack Edge Pro FPGA solution.

Azure Stack Edge service limits

- The storage account should be physically closest to the region where the device is deployed (can be different from where the service is deployed).
- Moving a Data Box Gateway resource to a different subscription or resource group is not supported. For more details, go to [Move resources to new resource group or subscription](#).

Azure Stack Edge device limits

The following table describes the limits for the Azure Stack Edge device.

DESCRIPTION	VALUE
No. of files per device	100 million
No. of shares per container	1
Maximum no. of share endpoints and REST endpoints per device (GPU devices only)	24
Maximum no. of tiered storage accounts per device (GPU devices only)	24
Maximum file size written to a share	5 TB
Maximum number of resource groups per device	800

Azure storage limits

This section describes the limits for Azure Storage service, and the required naming conventions for Azure Files, Azure block blobs, and Azure page blobs, as applicable to the Azure Stack Edge / Data Box Gateway service. Review the storage limits carefully and follow all the recommendations.

For the latest information on Azure storage service limits and best practices for naming shares, containers, and files, go to:

- [Naming and referencing containers](#)
- [Naming and referencing shares](#)
- [Block blobs and page blob conventions](#)

IMPORTANT

If there are any files or directories that exceed the Azure Storage service limits, or do not conform to Azure Files/Blob naming conventions, then these files or directories are not ingested into the Azure Storage via the Azure Stack Edge / Data Box Gateway service.

Data upload caveats

Following caveats apply to data as it moves into Azure.

- We suggest that more than one device should not write to the same container.
- If you have an existing Azure object (such as a blob or a file) in the cloud with the same name as the object that is being copied, device will overwrite the file in the cloud.
- An empty directory hierarchy (without any files) created under share folders is not uploaded to the blob containers.
- You can copy the data using drag and drop with File Explorer or via command line. If the aggregate size of files being copied is greater than 10 GB, we recommend you use a bulk copy program such as Robocopy or rsync. The bulk copy tools retry the copy operation for intermittent errors and provide additional resiliency.
- If the share associated with the Azure storage container uploads blobs that do not match the type of blobs defined for the share at the time of creation, then such blobs are not updated. For example, you create a block blob share on the device. Associate the share with an existing cloud container that has page blobs. Refresh that share to download the files. Modify some of the refreshed files that are already stored as page blobs in the cloud. You will see upload failures.
- After a file is created in the shares, renaming of the file isn't supported.
- Deletion of a file from a share does not delete the entry in the storage account.
- If using rsync to copy data, then `rsync -a` option is not supported.

Azure storage account size and object size limits

Here are the limits on the size of the data that is copied into storage account. Make sure that the data you upload conforms to these limits. For the most up-to-date information on these limits, see [Scalability and performance targets for Blob storage](#) and [Azure Files scalability and performance targets](#).

SIZE OF DATA COPIED INTO AZURE STORAGE ACCOUNT	DEFAULT LIMIT
Block Blob and page blob	500 TB per storage account

Azure object size limits

Here are the sizes of the Azure objects that can be written. Make sure that all the files that are uploaded conform to these limits.

AZURE OBJECT TYPE	UPLOAD LIMIT
Block Blob	~ 4.75 TB
Page Blob	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

AZURE OBJECT TYPE	UPLOAD LIMIT
Azure Files	1 TB Every file uploaded in Page Blob format must be 512 bytes aligned (an integral multiple), else the upload fails. The VHD and VHDX are 512 bytes aligned.

IMPORTANT

Creation of files (irrespective of the storage type) is allowed up to 5 TB. However, if you create a file whose size is greater than the upload limit defined in the preceding table, the file does not get uploaded. You have to manually delete the file to reclaim the space.

Next steps

- [Prepare to deploy Azure Stack Edge Pro GPU](#)
- [Prepare to deploy Azure Stack Edge Pro FPGA](#)

Azure Stack Edge security and data protection

9/21/2022 • 6 minutes to read • [Edit Online](#)

Security is a major concern when you're adopting a new technology, especially if the technology is used with confidential or proprietary data. Azure Stack Edge helps you ensure that only authorized entities can view, modify, or delete your data.

This article describes the Azure Stack Edge security features that help protect each of the solution components and the data stored in them.

Azure Stack Edge consists of four main components that interact with each other:

- **Azure Stack Edge service, hosted in Azure.** The management resource that you use to create the device order, configure the device, and then track the order to completion.
- **Azure Stack Edge Pro FPGA device.** The transfer device that's shipped to you so you can import your on-premises data into Azure.
- **Clients/hosts connected to the device.** The clients in your infrastructure that connect to the Azure Stack Edge Pro FPGA device and contain data that needs to be protected.
- **Cloud storage.** The location in the Azure cloud platform where data is stored. This location is typically the storage account linked to the Azure Stack Edge resource that you create.

Azure Stack Edge service protection

The Azure Stack Edge service is a management service that's hosted in Azure. The service is used to configure and manage the device.

- To access the Azure Stack Edge service, your organization needs to have an Enterprise Agreement (EA) or Cloud Solution Provider (CSP) subscription. For more information, see [Sign up for an Azure subscription](#).
- Because this management service is hosted in Azure, it's protected by the Azure security features. For more information about the security features provided by Azure, go to the [Microsoft Azure Trust Center](#).
- For SDK management operations, you can get the encryption key for your resource in **Device properties**. You can view the encryption key only if you have permissions for the Resource Graph API.

Azure Stack Edge device protection

The Azure Stack Edge device is an on-premises device that helps transform your data by processing it locally and then sending it to Azure. Your device:

- Needs an activation key to access the Azure Stack Edge service.
- Is protected at all times by a device password.
- Is a locked-down device. The device BMC and BIOS are password-protected. The BIOS is protected by limited user-access.
- Has secure boot enabled.
- Runs Windows Defender Device Guard. Device Guard lets you run only trusted applications that you define in your code-integrity policies.

Protect the device via activation key

Only an authorized Azure Stack Edge device is allowed to join the Azure Stack Edge service that you create in your Azure subscription. To authorize a device, you need to use an activation key to activate the device with the Azure Stack Edge service.

The activation key that you use:

- Is an Azure Active Directory (Azure AD) based authentication key.
- Expires after three days.
- Isn't used after device activation.

After you activate a device, it uses tokens to communicate with Azure.

For more information, see [Get an activation key](#).

Protect the device via password

Passwords ensure that only authorized users can access your data. Azure Stack Edge devices boot up in a locked state.

You can:

- Connect to the local web UI of the device via a browser and then provide a password to sign in to the device.
- Remotely connect to the device PowerShell interface over HTTP. Remote management is turned on by default. You can then provide the device password to sign in to the device. For more information, see [Connect remotely to your Azure Stack Edge Pro FPGA device](#).

Keep these best practices in mind:

- We recommend that you store all passwords in a secure place so you don't have to reset a password if it's forgotten. The management service can't retrieve existing passwords. It can only reset them via the Azure portal. If you reset a password, be sure to notify all users before you reset it.
- You can access the Windows PowerShell interface of your device remotely over HTTP. As a security best practice, you should use HTTP only on trusted networks.
- Ensure that device passwords are strong and well protected. Follow the [password best practices](#).
- Use the local web UI to [change the password](#). If you change the password, be sure to notify all remote access users so they don't have problems signing in.

Protect your data

This section describes the Azure Stack Edge Pro FPGA security features that protect in-transit and stored data.

Protect data at rest

For data at rest:

- Access to data stored in shares is restricted.
 - SMB clients that access share data need user credentials associated with the share. These credentials are defined when the share is created.
 - The IP addresses of NFS clients that access a share need to be added when the share is created.
- BitLocker XTS-AES 256-bit encryption is used to protect local data.

Protect data in flight

For data in flight:

- Standard TLS 1.2 is used for data that travels between the device and Azure. There is no fallback to TLS 1.1 and earlier. Agent communication will be blocked if TLS 1.2 isn't supported. TLS 1.2 is also required for portal and SDK management.
- When clients access your device through the local web UI of a browser, standard TLS 1.2 is used as the default secure protocol.

- The best practice is to configure your browser to use TLS 1.2.
- If the browser doesn't support TLS 1.2, you can use TLS 1.1 or TLS 1.0.
- We recommend that you use SMB 3.0 with encryption to protect data when you copy it from your data servers.

Protect data via storage accounts

Your device is associated with a storage account that's used as a destination for your data in Azure. Access to the storage account is controlled by the subscription and two 512-bit storage access keys associated with that storage account.

One of the keys is used for authentication when the Azure Stack Edge device accesses the storage account. The other key is held in reserve, so you can rotate the keys periodically.

For security reasons, many datacenters require key rotation. We recommend that you follow these best practices for key rotation:

- Your storage account key is similar to the root password for your storage account. Carefully protect your account key. Don't distribute the password to other users, hard code it, or save it anywhere in plain text that's accessible to others.
- Regenerate your account key via the Azure portal if you think it could be compromised. For more information, see [Manage storage account access keys](#).
- Your Azure admin should periodically change or regenerate the primary or secondary key by using the Storage section of the Azure portal to access the storage account directly.
- Rotate and then [sync your storage account keys](#) regularly to help protect your storage account from unauthorized users.

Manage personal information

The Azure Stack Edge service collects personal information in the following scenarios:

- **Order details.** When an order is created, the shipping address, email address, and contact information of the user is stored in the Azure portal. The information saved includes:
 - Contact name
 - Phone number
 - Email address
 - Street address
 - City
 - ZIP Code/postal code
 - State
 - Country/province/region
 - Shipping tracking number

Order details are encrypted and stored in the service. The service retains the information until you explicitly delete the resource or order. The deletion of the resource and the corresponding order is blocked from the time the device is shipped until the device returns to Microsoft.

- **Shipping address.** After an order is placed, Data Box service provides the shipping address to third-party carriers like UPS.

- **Share users.** Users on your device can also access the data located on the shares. A list of users who can access the share data can be viewed. When the shares are deleted, this list is also deleted.

To view the list of users who can access or delete a share, follow the steps in [Manage shares on the Azure Stack Edge Pro FPGA](#).

For more information, review the Microsoft privacy policy on the [Trust Center](#).

Next steps

[Deploy your Azure Stack Edge Pro FPGA device](#)

Azure Stack Edge Pro FPGA technical specifications

9/21/2022 • 4 minutes to read • [Edit Online](#)

The hardware components of your Microsoft Azure Stack Edge Pro FPGA device adhere to the technical specifications and regulatory standards outlined in this article. The technical specifications describe the Power supply units (PSUs), storage capacity, enclosures, and environmental standards.

Compute, memory specifications

The Azure Stack Edge Pro FPGA device has the following specifications for compute and memory:

SPECIFICATION	VALUE
CPU type	Dual Intel Xeon Silver 4114 2.2 G
CPU: raw	20 total cores, 40 total vCPUs
CPU: usable	32 vCPUs
Memory type	8 x 16 GB RDIMM
Memory: raw	128 GB RAM (8 x 16 GB)
Memory: usable	102 GB RAM

FPGA specifications

A Field Programmable Gate Array (FPGA) is included on every Azure Stack Edge Pro FPGA device that enables Machine Learning (ML) scenarios.

SPECIFICATION	VALUE
FPGA	Intel Arria 10 Available Deep Neural Network (DNN) models are the same as those supported by cloud FPGA instances .

Power supply unit specifications

The Azure Stack Edge Pro FPGA device has two 100-240 V Power supply units (PSUs) with high-performance fans. The two PSUs provide a redundant power configuration. If a PSU fails, the device continues to operate normally on the other PSU until the failed module is replaced. The following table lists the technical specifications of the PSUs.

SPECIFICATION	750 W PSU
Maximum output power	750 W
Frequency	50/60 Hz

SPECIFICATION	750 W PSU
Voltage range selection	Auto ranging: 100-240 V AC
Hot pluggable	Yes

Azure Stack Edge Pro FPGA power cord specifications by region

Your Azure Stack Edge Pro FPGA device needs a power cord that varies depending on your Azure region. For technical specifications of all the supported power cords, see [Azure Stack Edge Pro FPGA power cord specifications by region](#).

Network interface specifications

Your Azure Stack Edge Pro FPGA device has 6 network interfaces, PORT1 - PORT6.

SPECIFICATION	DESCRIPTION
Network interfaces	2 X 1 GbE interfaces – 1 management, not user configurable, used for initial setup. The other interface is user configurable, can be used for data transfer, and is DHCP by default. 2 X 25 GbE interfaces – These can also operate as 10 GbE interfaces. These data interfaces can be configured by user as DHCP (default) or static. 2 X 25 GbE interfaces - These data interfaces can be configured by user as DHCP (default) or static.

The Network Adapters used are:

SPECIFICATION	DESCRIPTION
Network Daughter Card (rNDC)	QLogic FastLinQ 41264 Dual Port 25GbE SFP+, Dual Port 1GbE, rNDC
PCI Network Adapter	QLogic FastLinQ 41262 zwei Ports 25Gbit/s SFP28 Adapter

Please consult the Hardware Compatibility List from Intel QLogic for compatible Gigabit Interface Converter (GBIC). Gigabit Interface Converter (GBIC) are not included in the delivery of Azure Stack Edge.

Storage specifications

The Azure Stack Edge Pro FPGA devices have 9 X 2.5" NVMe SSDs, each with a capacity of 1.6 TB. Of these SSDs, 1 is an operating system disk, and the other 8 are data disks. The total usable capacity for the device is roughly 12.5 TB. The following table has the details for the storage capacity of the device.

SPECIFICATION	VALUE
Number of solid-state drives (SSDs)	8
Single SSD capacity	1.6 TB
Total capacity	12.8 TB
Total usable capacity*	~ 12.5 TB

*Some space is reserved for internal use.

Enclosure dimensions and weight specifications

The following tables list the various enclosure specifications for dimensions and weight.

Enclosure dimensions

The following table lists the dimensions of the enclosure in millimeters and inches.

ENCLOSURE	MILLIMETERS	INCHES
Height	44.45	1.75"
Width	434.1	17.09"
Length	740.4	29.15"

The following table lists the dimensions of the shipping package in millimeters and inches.

PACKAGE	MILLIMETERS	INCHES
Height	311.2	12.25"
Width	642.8	25.31"
Length	1,051.1	41.38"

Enclosure weight

The device package weighs 61 lbs. and requires two persons to handle it. The weight of the device depends on the configuration of the enclosure.

ENCLOSURE	WEIGHT
Total weight including the packaging	61 lbs.
Weight of the device	35 lbs.

Enclosure environment specifications

This section lists the specifications related to the enclosure environment such as temperature, humidity, and altitude.

Temperature and humidity

ENCLOSURE	AMBIENT TEMPERATURE RANGE	AMBIENT RELATIVE HUMIDITY	MAXIMUM DEW POINT
Operational	10°C - 35°C (50°F - 86°F)	10% - 80% non-condensing.	29°C (84°F)
Non-operational	-40°C to 65°C (-40°F - 149°F)	5% - 95% non-condensing.	33°C (91°F)

Airflow, altitude, shock, vibration, orientation, safety, and EMC

ENCLOSURE	OPERATIONAL SPECIFICATIONS
Airflow	System airflow is front to rear. System must be operated with a low-pressure, rear-exhaust installation.
Maximum altitude, operational	3048 meters (10,000 feet) with maximum operating temperature de-rated determined by Operating temperature de-rating specifications .
Maximum altitude, non-operational	12,000 meters (39,370 feet)
Shock, operational	6 G for 11 milliseconds in 6 orientations
Shock, non-operational	71 G for 2 milliseconds in 6 orientations
Vibration, operational	0.26 G _{RMS} 5 Hz to 350 Hz random
Vibration, non-operational	1.88 G _{RMS} 10 Hz to 500 Hz for 15 minutes (all six sides tested.)
Orientation and mounting	19" rack mount
Safety and approvals	EN 60950-1:2006 +A1:2010 +A2:2013 +A11:2009 +A12:2011/IEC 60950-1:2005 ed2 +A1:2009 +A2:2013 EN 62311:2008
EMC	FCC A, ICES-003 EN 55032:2012/CISPR 32:2012 EN 55032:2015/CISPR 32:2015 EN 55024:2010 +A1:2015/CISPR 24:2010 +A1:2015 EN 61000-3-2:2014/IEC 61000-3-2:2014 (Class D) EN 61000-3-3:2013/IEC 61000-3-3:2013
Energy	Commission Regulation (EU) No. 617/2013
RoHS	EN 50581:2012

Operating temperature de-rating specifications

OPERATING TEMPERATURE DE-RATING	AMBIENT TEMPERATURE RANGE
Up to 35°C (95°F)	Maximum temperature is reduced by 1°C/300 m (1°F/547 ft) above 950 m (3,117 ft).
35°C to 40°C (95°F to 104°F)	Maximum temperature is reduced by 1°C/175 m (1°F/319 ft) above 950 m (3,117 ft).
40°C to 45°C (104°F to 113°F)	Maximum temperature is reduced by 1°C/125 m (1°F/228 ft) above 950 m (3,117 ft).

Next steps

- Deploy your Azure Stack Edge Pro

Azure Stack Edge Pro FPGA power cord specifications

9/21/2022 • 6 minutes to read • [Edit Online](#)

Your Azure Stack Edge Pro FPGA device will need a power cord that will vary depending on your Azure region.

Supported power cords

You can use the following table to find the correct cord specifications for your region:

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Albania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Algeria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Angola	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Argentina	250	10	H05VV-F 3x1.00	IRAM 2073	C13	2500
Australia	250	10	H05VV-F 3x1.00	AS/NZS 3112	C13	2438
Austria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Azerbaijan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bahamas	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Bahrain	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Bangladesh	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Barbados	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Belarus	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Belgium	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bermuda	125	10	SVE 18/3	NEMA 5-15P	C13	1830

Country	Rated Voltage (V)	Rated Current (A)	Cord Standard	Input Connector	Output Connector	Length mm
Bolivia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Bosnia and Herzegovina	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Brazil	250	10	H05Z1Z1-F 3x.75	NBR 14136	C13	1914
Bulgaria	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Cambodia	250	10	H05VV-F 3X0.75	CEE 7/7	C13	1800
Canada	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Cayman Islands	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Chile	250	10	H05VV-F 3x0.75	CEI 23-50	C13	1800
China	250	10	RVV300/500 3X0.75	GB 2099.1	C13	2000
Colombia	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Costa Rica	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Côte D'Ivoire (Ivory Coast)	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Croatia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Cyprus	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Czech Republic	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Denmark	250	10	H05VV-F 3X0.75	SB107-2-DI	C13	1800
Dominican Republic	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Ecuador	125	10	SVE 18/3	NEMA 5-15P	C13	1830

Country	Rated Voltage (V)	Rated Current (A)	Cord Standard	Input Connector	Output Connector	Length mm
Egypt	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
El Salvador	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Estonia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ethiopia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Finland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
France	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Georgia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Germany	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ghana	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Guyana	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Greece	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Guatemala	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Honduras	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Hong Kong	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Hungary	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Iceland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
India	250	10	IS694 3x0.75	IS 1293	C13	1830
Indonesia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Ireland	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Israel	250	2.5	H05VV-F 3x1.00	SI 32	C13	2000
Italy	250	10	H05VV-F 3x0.75	CEI 23-50	C13	1800
Jamaica	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Japan	125	15	VCTF 3x2.00 Act on Product Safety of Electrical Appliances and Materials	JIS C 8303	C13	2300
Jordan	250	5	H05Z1Z1-F 3x0.75	BS 1363	C13	1830
Kazakhstan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Kenya	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Kuwait	250	5	H05VV-F 3x0.75	BS1363 SS145/A	C13	1800
Kyrgyzstan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Latvia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Lebanon	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Liechtenstein	250	10	H05VV-F 3x0.75	SEV 1011	C13	1800
Lithuania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Luxembourg	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Macau	2250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Macedonia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Malaysia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Malta	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Mauritius	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Mexico	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Moldova	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Monaco	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Mongolia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Montenegro	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Morocco	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Namibia	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
Nepal	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
Netherlands	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
New Zealand	250	10	H05VV-F 3x1.00	AS/NZS 3112	C13	2438
Nicaragua	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Nigeria	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Norway	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Oman	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Pakistan	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
Panama	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Paraguay	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Peru	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Philippines	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Poland	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Portugal	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Puerto Rico	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Qatar	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Romania	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Russia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Rwanda	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Saint Kitts and Nevis	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Samoa	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Saudi Arabia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Senegal	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Serbia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Singapore	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Slovakia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Slovenia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
South Africa	250	10	H05VV-F 3x0.75	SANS 164-1	C13	1830
South Korea	250	10	H05W-F 3x1.75	KS C 8305	C13	1830
Spain	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Sri Lanka	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Sweden	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Switzerland	250	10	H05VV-F 3x0.75	SEV 1011	C13	1800
Taiwan	125	10	VCTF 3x1.25	CNS10917	C13	2000
Tajikistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Tanzania	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Thailand	250	10	H05VV-F 3x0.75	TI16S3	C13	1829
Trinidad and Tobago	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Tunisia	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Turkey	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Turkmenistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Uganda	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Ukraine	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
United Arab Emirates	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
United Kingdom	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

COUNTRY	RATED VOLTAGE (V)	RATED CURRENT (A)	CORD STANDARD	INPUT CONNECTOR	OUTPUT CONNECTOR	LENGTH MM
United States	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Uruguay	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Uzbekistan	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Venezuela	125	10	SVE 18/3	NEMA 5-15P	C13	1830
Vietnam	250	10	H05Z1Z1 3x0.75	CEE 7	C13	1830
Yemen	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Zambia	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800
Zimbabwe	250	5	H05VV-F 3x0.75	BS 1363 / SS145/A	C13	1800

Next steps

[Azure Stack Edge Pro FPGA technical specifications](#)

Develop a C# IoT Edge module to move files with Azure Stack Edge Pro FPGA

9/21/2022 • 8 minutes to read • [Edit Online](#)

This article steps you through how to create an IoT Edge module for deployment with your Azure Stack Edge Pro FPGA device. Azure Stack Edge Pro FPGA is a storage solution that allows you to process data and send it over network to Azure.

You can use Azure IoT Edge modules with your Azure Stack Edge Pro FPGA to transform the data as it moved to Azure. The module used in this article implements the logic to copy a file from a local share to a cloud share on your Azure Stack Edge Pro FPGA device.

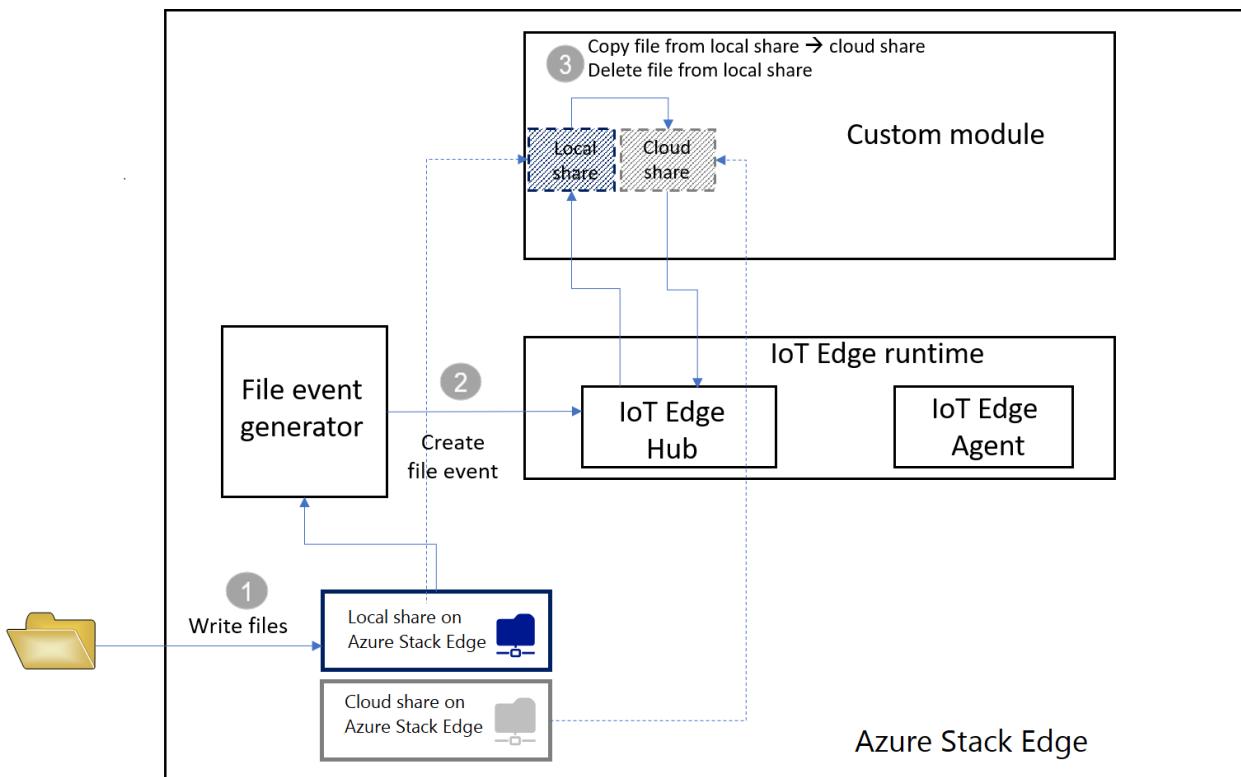
In this article, you learn how to:

- Create a container registry to store and manage your modules (Docker images).
- Create an IoT Edge module to deploy on your Azure Stack Edge Pro FPGA device.

About the IoT Edge module

Your Azure Stack Edge Pro FPGA device can deploy and run IoT Edge modules. Edge modules are essentially Docker containers that perform a specific task, such as ingest a message from a device, transform a message, or send a message to an IoT Hub. In this article, you will create a module that copies files from a local share to a cloud share on your Azure Stack Edge Pro FPGA device.

1. Files are written to the local share on your Azure Stack Edge Pro FPGA device.
2. The file event generator creates a file event for each file written to the local share. The file events are also generated when a file is modified. The file events are then sent to IoT Edge Hub (in IoT Edge runtime).
3. The IoT Edge custom module processes the file event to create a file event object that also contains a relative path for the file. The module generates an absolute path using the relative file path and copies the file from the local share to the cloud share. The module then deletes the file from the local share.



Once the file is in the cloud share, it automatically gets uploaded to your Azure Storage account.

Prerequisites

Before you begin, make sure you have:

- An Azure Stack Edge Pro FPGA device that is running.
 - The device also has an associated IoT Hub resource.
 - The device has Edge compute role configured. For more information, go to [Configure compute](#) for your Azure Stack Edge Pro FPGA.
- The following development resources:
 - [Visual Studio Code](#).
 - [C# for Visual Studio Code \(powered by OmniSharp\) extension](#).
 - [Azure IoT Edge extension for Visual Studio Code](#).
 - [.NET Core 2.1 SDK](#).
 - [Docker CE](#). You may have to create an account to download and install the software.

Create a container registry

An Azure container registry is a private Docker registry in Azure where you can store and manage your private Docker container images. The two popular Docker registry services available in the cloud are Azure Container Registry and Docker Hub. This article uses the Container Registry.

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. Select **Create a resource > Containers > Container Registry**. Click **Create**.
3. Provide:
 - a. A unique **Registry name** within Azure that contains 5 to 50 alphanumeric characters.
 - b. Choose a **Subscription**.

- c. Create new or choose an existing **Resource group**.
- d. Select a **Location**. We recommend that this location be the same as that is associated with the Azure Stack Edge resource.
- e. Toggle **Admin user** to **Enable**.
- f. Set the **SKU** to **Basic**.

The screenshot shows the 'Create container registry' wizard. The steps are as follows:

- Registry name:** mycontreg2 (with a green checkmark)
- Subscription:** Internal Consumption
- Resource group:** mycontregrg (with a 'Create new' link)
- Location:** West US
- Admin user:** Enable (selected)
- SKU:** Basic

At the bottom, there is a red **Create** button and a blue **Automation options** link.

- 4. Select **Create**.
- 5. After your container registry is created, browse to it, and select **Access keys**.

The screenshot shows the 'mycontreg2 - Access keys' page in the Azure portal. The left sidebar has a 'Search (Ctrl+ /)' bar and links for Overview, Activity log, Access control (IAM), Tags, Quick start, Events, Settings, Access keys (which is selected and highlighted with a red box), Locks, Automation script, Services, Repositories, Webhooks, and Replications. The main area shows the Registry name as 'mycontreg2', the Login server as 'mycontreg2.azurecr.io', and the Admin user status as 'Enable'. It also displays the Username 'mycontreg2' and two password entries: 'password' and 'password2', both containing '<Password>' and '<Password2>'. There are copy and refresh icons next to each entry.

6. Copy the values for **Login server**, **Username**, and **Password**. You use these values later to publish the Docker image to your registry and to add the registry credentials to the Azure IoT Edge runtime.

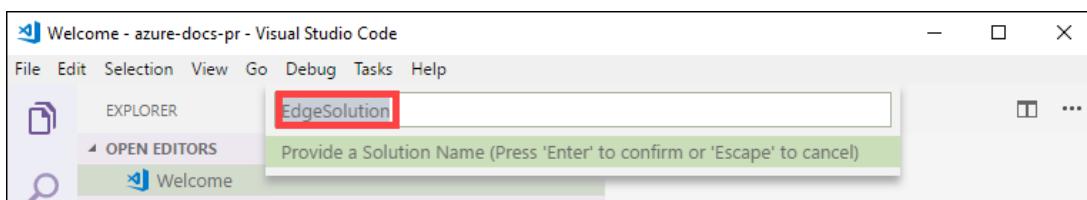
Create an IoT Edge module project

The following steps create an IoT Edge module project based on the .NET Core 2.1 SDK. The project uses Visual Studio Code and the Azure IoT Edge extension.

Create a new solution

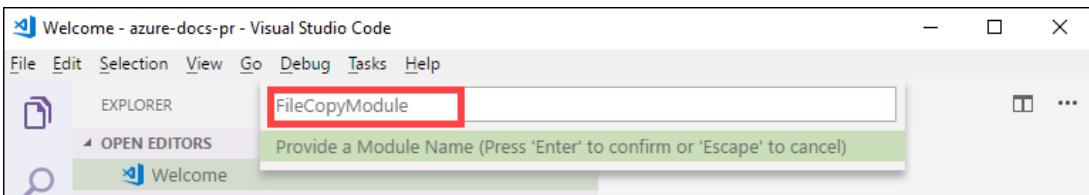
Create a C# solution template that you can customize with your own code.

1. In Visual Studio Code, select **View > Command Palette** to open the VS Code command palette.
2. In the command palette, enter and run the command **Azure: Sign in** and follow the instructions to sign in your Azure account. If you're already signed in, you can skip this step.
3. In the command palette, enter and run the command **Azure IoT Edge: New IoT Edge solution**. In the command palette, provide the following information to create your solution:
 - a. Select the folder where you want to create the solution.
 - b. Provide a name for your solution or accept the default **EdgeSolution**.



- c. Choose **C# Module** as the module template.
- d. Replace the default module name with the name you want to assign, in this case, it is

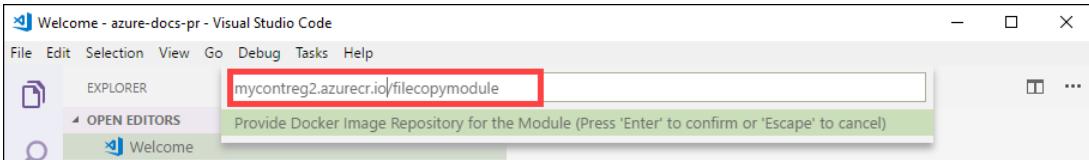
FileCopyModule.



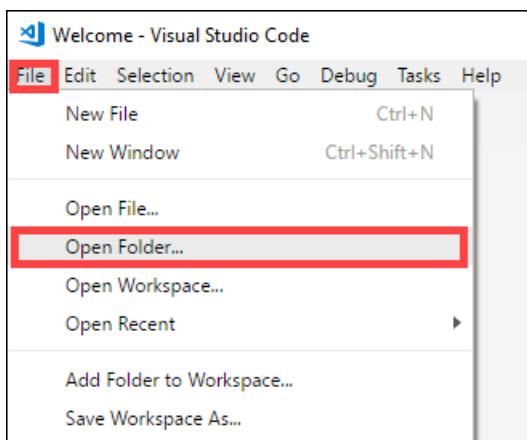
- e. Specify the container registry that you created in the previous section as the image repository for your first module. Replace **localhost:5000** with the login server value that you copied.

The final string looks like <Login server name>/<Module name>. In this example, the string is:

`mycontreg2.azurecr.io/filecopymodule`.

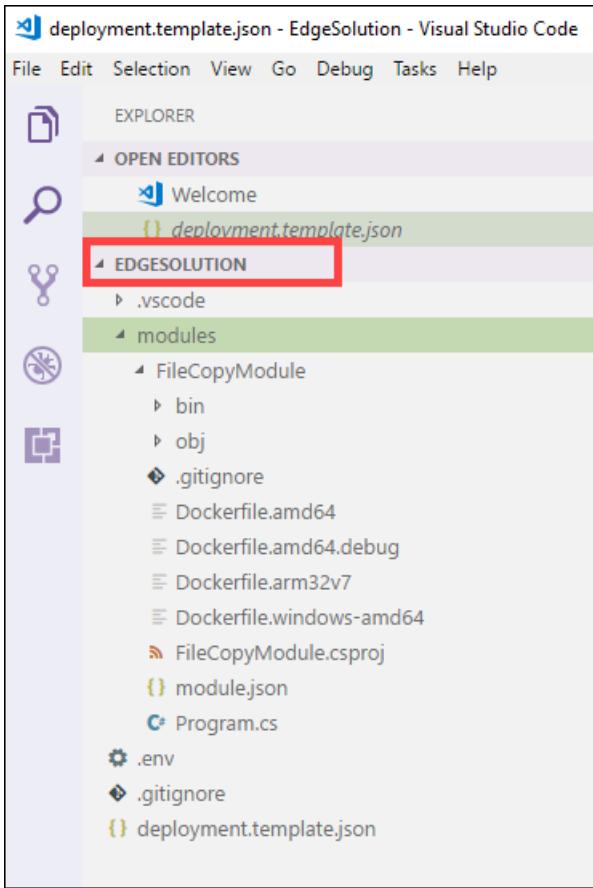


4. Go to **File > Open Folder**.



5. Browse and point to the **EdgeSolution** folder that you created earlier. The VS Code window loads your IoT Edge solution workspace with its five top-level components. You won't edit the **.vscode** folder, **.gitignore** file, **.env** file, and the **deployment.template.json** in this article.

The only component that you modify is the modules folder. This folder has the C# code for your module and Docker files to build your module as a container image.



Update the module with custom code

1. In the VS Code explorer, open **modules > FileCopyModule > Program.cs**.
2. At the top of the **FileCopyModule namespace**, add the following using statements for types that are used later. **Microsoft.Azure.Devices.Client.Transport.Mqtt** is a protocol to send messages to IoT Edge Hub.

```
namespace FileCopyModule
{
    using Microsoft.Azure.Devices.Client.Transport.Mqtt;
    using Newtonsoft.Json;
```

3. Add the **InputFolderPath** and **OutputFolderPath** variable to the Program class.

```
class Program
{
    static int counter;
    private const string InputFolderPath = "/home/input";
    private const string OutputFolderPath = "/home/output";
```

4. Immediately after the previous step, add the **FileEvent** class to define the message body.

```
/// <summary>
/// The FileEvent class defines the body of incoming messages.
/// </summary>
private class FileEvent
{
    public string ChangeType { get; set; }

    public string ShareRelativeFilePath { get; set; }

    public string ShareName { get; set; }
}
```

5. In the **Init** method, the code creates and configures a **ModuleClient** object. This object allows the module to connect to the local Azure IoT Edge runtime using MQTT protocol to send and receive messages. The connection string that's used in the **Init** method is supplied to the module by the IoT Edge runtime. The code registers a **FileCopy** callback to receive messages from an IoT Edge hub via the **input1** endpoint. Replace the **Init** method with the following code.

```
/// <summary>
/// Initializes the ModuleClient and sets up the callback to receive
/// messages containing file event information
/// </summary>
static async Task Init()
{
    MqttTransportSettings mqttSetting = new MqttTransportSettings(TransportType.Mqtt_Tcp_Only);
    ITransportSettings[] settings = { mqttSetting };

    // Open a connection to the IoT Edge runtime
    ModuleClient ioTHubModuleClient = await ModuleClient.CreateFromEnvironmentAsync(settings);
    await ioTHubModuleClient.OpenAsync();
    Console.WriteLine("IoT Hub module client initialized.");

    // Register callback to be called when a message is received by the module
    await ioTHubModuleClient.SetInputMessageHandlerAsync("input1", FileCopy, ioTHubModuleClient);
}
```

6. Remove the code for **PipeMessage** method and in its place, insert the code for **FileCopy**.

```

/// <summary>
/// This method is called whenever the module is sent a message from the IoT Edge Hub.
/// This method deserializes the file event, extracts the corresponding relative file path, and
creates the absolute input file path using the relative file path and the InputFolderPath.
/// This method also forms the absolute output file path using the relative file path and the
OutputFolderPath. It then copies the input file to output file and deletes the input file after the
copy is complete.
/// </summary>
static async Task<MessageResponse> FileCopy(Message message, object userContext)
{
    int counterValue = Interlocked.Increment(ref counter);

    try
    {
        byte[] messageBytes = message.GetBytes();
        string messageString = Encoding.UTF8.GetString(messageBytes);
        Console.WriteLine($"Received message: {counterValue}, Body: [{messageString}]");

        if (!string.IsNullOrEmpty(messageString))
        {
            var fileEvent = JsonConvert.DeserializeObject<FileEvent>(messageString);

            string relativeFileName = fileEvent.ShareRelativeFilePath.Replace("\\", "/");
            string inputFilePath = InputFolderPath + relativeFileName;
            string outputPath = OutputFolderPath + relativeFileName;

            if (File.Exists(inputFilePath))
            {
                Console.WriteLine($"Moving input file: {inputFilePath} to output file:
{outputPath}");
                var outputDir = Path.GetDirectoryName(outputPath);
                if (!Directory.Exists(outputDir))
                {
                    Directory.CreateDirectory(outputDir);
                }

                File.Copy(inputFilePath, outputPath, true);
                Console.WriteLine($"Copied input file: {inputFilePath} to output file:
{outputPath}");
                File.Delete(inputFilePath);
                Console.WriteLine($"Deleted input file: {inputFilePath}");
            }
            else
            {
                Console.WriteLine($"Skipping this event as input file doesn't exist:
{inputFilePath}");
            }
        }
        catch (Exception ex)
        {
            Console.WriteLine("Caught exception: {0}", ex.Message);
            Console.WriteLine(ex.StackTrace);
        }

        Console.WriteLine($"Processed event.");
        return MessageResponse.Completed;
    }
}

```

7. Save this file.

8. You can also [download an existing code sample](#) for this project. You can then validate the file that you saved against the `program.cs` file in this sample.

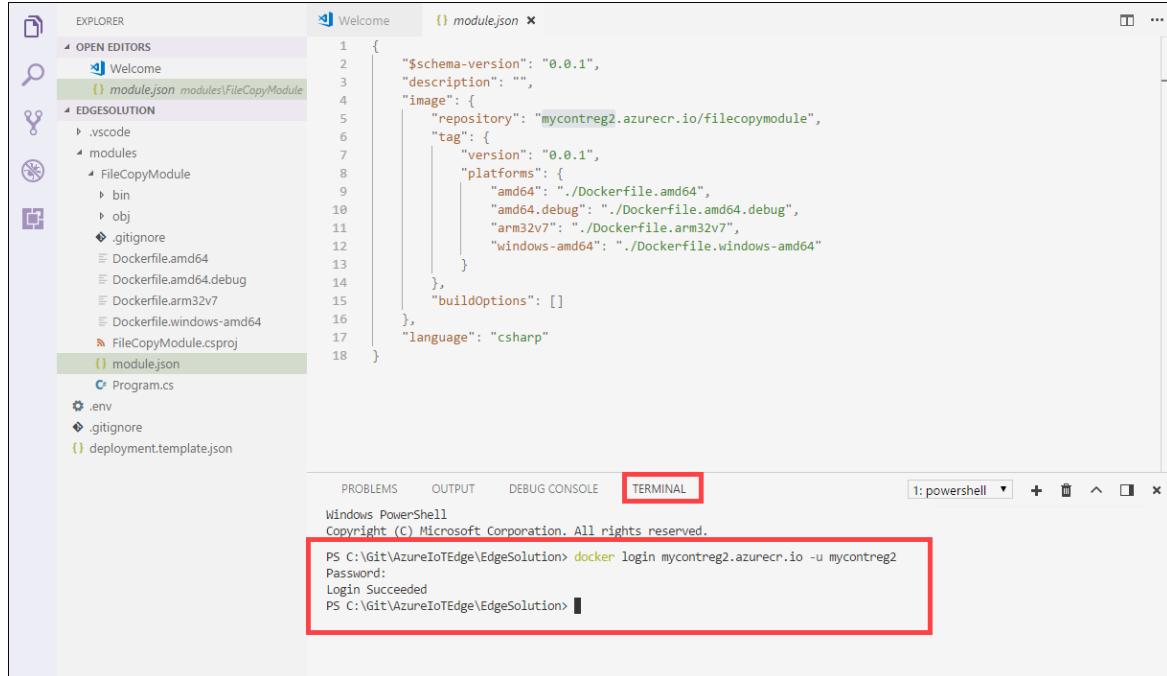
Build your IoT Edge solution

In the previous section, you created an IoT Edge solution and added code to the FileCopyModule to copy files from local share to the cloud share. Now you need to build the solution as a container image and push it to your container registry.

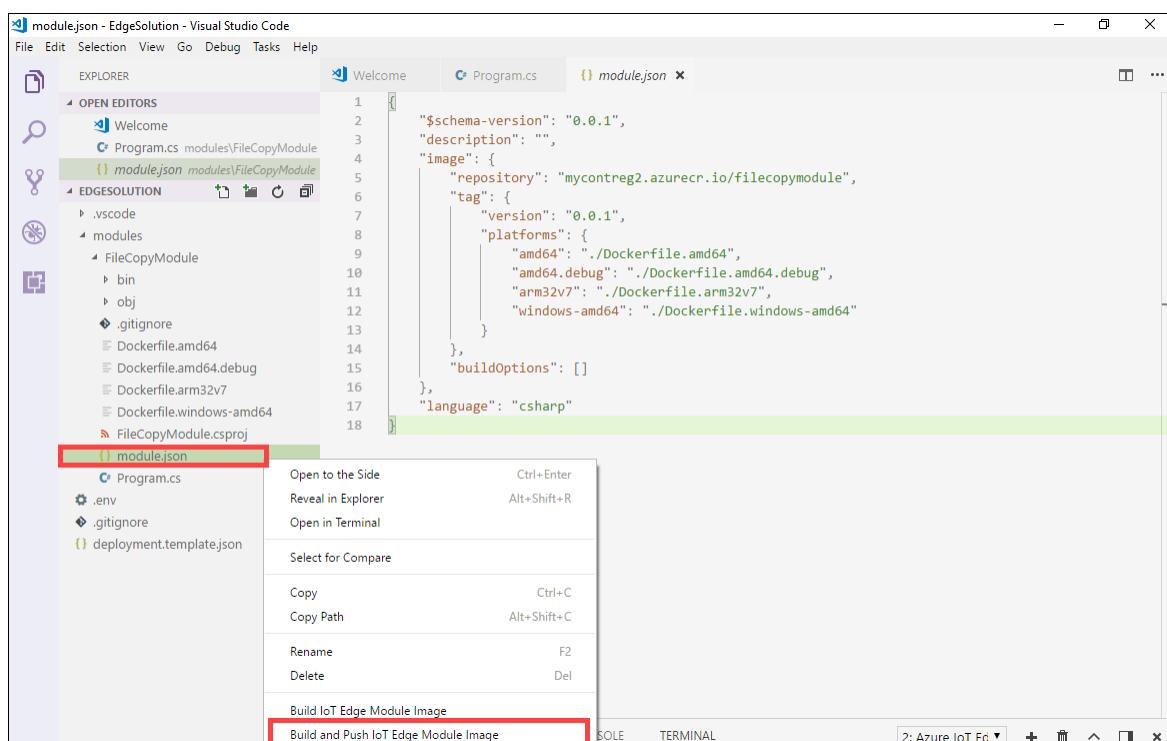
1. In VSCode, go to Terminal > New Terminal to open a new Visual Studio Code integrated terminal.
2. Sign in to Docker by entering the following command in the integrated terminal.

```
docker login <ACR login server> -u <ACR username>
```

Use the login server and username that you copied from your container registry.

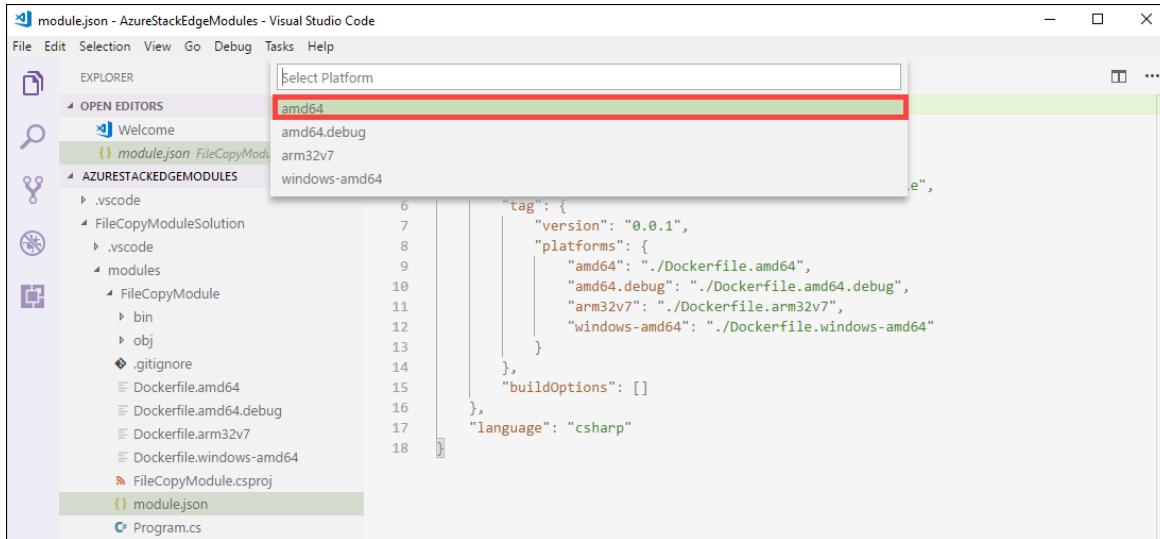


3. When prompted for password, supply the password. You can also retrieve the values for login server, username, and password from the **Access Keys** in your container registry in the Azure portal.
4. Once the credentials are supplied, you can push your module image to your Azure container registry. In the VS Code Explorer, right-click the **module.json** file and select **Build and Push IoT Edge solution**.



When you tell Visual Studio Code to build your solution, it runs two commands in the integrated terminal: docker build and docker push. These two commands build your code, containerize the CSharpModule.dll, and then push the code to the container registry that you specified when you initialized the solution.

You will be prompted to choose the module platform. Select *amd64* corresponding to Linux.



IMPORTANT

Only the Linux modules are supported.

You may see the following warning that you can ignore:

Program.cs(77,44): warning CS1998: This async method lacks 'await' operators and will run synchronously. Consider using the 'await' operator to await non-blocking API calls, or 'await Task.Run(...)' to do CPU-bound work on a background thread.

5. You can see the full container image address with tag in the VS Code integrated terminal. The image address is built from information that's in the module.json file with the format

<repository>:<version>-<platform>. For this article, it should look like
mycontreg2.azurecr.io/filecopymodule:0.0.1-amd64 .

Next steps

To deploy and run this module on Azure Stack Edge Pro FPGA, see the steps in [Add a module](#).

Manage compute on your Azure Stack Edge Pro FPGA

9/21/2022 • 4 minutes to read • [Edit Online](#)

This article describes how to manage compute on your Azure Stack Edge Pro FPGA. You can manage the compute via the Azure portal or via the local web UI. Use the Azure portal to manage modules, triggers, and compute configuration, and the local web UI to manage compute settings.

In this article, you learn how to:

- Manage triggers
- Manage compute configuration

Manage triggers

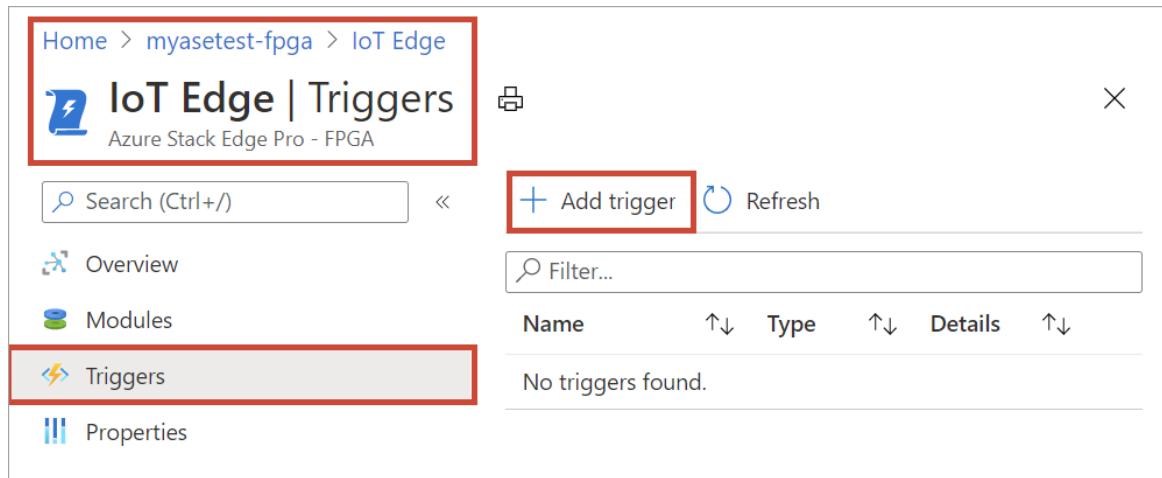
Events are things that happen within your cloud environment or on your device that you might want to take action on. For example, when a file is created in a share, it is an event. Triggers raise the events. For your Azure Stack Edge Pro FPGA, triggers can be in response to file events or a schedule.

- **File:** These triggers are in response to file events such as creation of a file, modification of a file.
- **Scheduled:** These triggers are in response to a schedule that you can define with a start date, start time, and the repeat interval.

Add a trigger

Take the following steps in the Azure portal to create a trigger.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge > Triggers**. Select **+ Add trigger** on the command bar.



2. In **Add trigger** blade, provide a unique name for your trigger.
3. Select a **Type** for the trigger. Choose **File** when the trigger is in response to a file event. Select **Scheduled** when you want the trigger to start at a defined time and run at a specified repeat interval. Depending on your selection, a different set of options is presented.
 - **File trigger** - Choose from the dropdown list a mounted share. When a file event is fired in this share, the trigger would invoke an Azure Function.

Add trigger

X

Triggers help invoke functions in a module. Triggers can be file event or scheduled. [Learn more](#)

Name *

mytrigger1



Type * ⓘ

File (When file is written to input share)



Input Edge local share * ⓘ

myasesmblocal



Add

- **Scheduled trigger** - Specify the start date/time, and the repeat interval in hours, minutes, or seconds. Also, enter the name for a topic. A topic will give you the flexibility to route the trigger to a module deployed on the device.

An example route string is:

```
"route3": "FROM /* WHERE topic = 'topicname' INTO  
BrokeredEndpoint(\"modules/modulename/inputs/input1\")"
```

Add trigger

X

Triggers help invoke functions in a module. Triggers can be file event or scheduled. [Learn more](#)

Name *

mytrigger2



Type * ⓘ

Scheduled (Run at repeat interval)



Start date & time * ⓘ

12/22/2020



10:22:44 AM

Repeat interval * ⓘ

12



Hour



Topic * ⓘ

topicname1



Add

4. Select **Add** to create the trigger. A notification shows that the trigger creation is in progress. After the trigger is created, the blade updates to reflect the new trigger.

Home > myasetest-fpga > IoT Edge

IoT Edge | Triggers

Azure Stack Edge Pro - FPGA

Search (Ctrl+ /) Add trigger Refresh

Overview Modules Triggers Properties

Filter... Name Type Details

Name	Type	Details
mytrigger1	File	Associated share: myasesmblocal
mytrigger2	Scheduled	Scheduled start: 12/22/2020, 23:52:44, Repeat interval: Every 12 hours

Delete a trigger

Take the following steps in the Azure portal to delete a trigger.

- From the list of triggers, select the trigger that you want to delete.

Home > myasetest-fpga > IoT Edge

IoT Edge | Triggers

Azure Stack Edge Pro - FPGA

Search (Ctrl+ /) Add trigger Refresh

Overview Modules Triggers Properties

Filter... Name Type Details

Name	Type	Details
mytrigger1	File	Associated share: myasesmblocal
mytrigger2	Scheduled	Scheduled start: 12/22/2020, 23:52:44, Repeat interval: Every 12 hours

- Right-click and then select **Delete**.

Home > myasetest-fpga > IoT Edge

IoT Edge | Triggers

Azure Stack Edge Pro - FPGA

Search (Ctrl+ /) Add trigger Refresh

Overview Modules Triggers Properties

Filter... Name Type Details

Name	Type	Details
mytrigger1	File	Associated share: myasesmblocal
mytrigger2	Scheduled	Scheduled start: 12/22/2020, 23:52:44, Repeat interval: Every 12 hours

- When prompted for confirmation, click **Yes**.

Do you want to delete this trigger?

You are about to delete the trigger 'mytrigger1'. Modules using this trigger will not be able to emit events. Are you sure you want to delete this trigger?

OK Cancel

The list of triggers updates to reflect the deletion.

Manage compute configuration

Use the Azure portal to view the compute configuration, remove an existing compute configuration, or to refresh the compute configuration to sync up access keys for the IoT device and IoT Edge device for your Azure Stack Edge Pro FPGA.

View compute configuration

Take the following steps in the Azure portal to view the compute configuration for your device.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge > Overview**.

IoT Edge | Overview

IoT Edge service is running fine!

Modules
Total 1 No
mymodule1
[View all modules](#)

Triggers
Total 1 No
mytrigger1
[View all triggers](#)

Edge Shares
For container to store or transfer files and folders to Azure Storage account (other than temp data), create a share.
[Configure Shares](#)

Edge Storage account
For container to transfer unstructured data like binary, audio, or video streaming data to Azure Storage account, create a storage account.
[Configure Storage account](#)

Network bandwidth usage
If containers uploads data to cloud using shares configure network bandwidth usage across multiple time-of-day schedules.
[Configure Bandwidth schedule](#)

- Go to **Properties** page. Make a note of the compute configuration on your device. When you configured compute, you created an IoT Hub resource. Under that IoT Hub resource, an IoT device and an IoT Edge device are configured. Only the Linux modules are supported to run on the IoT Edge device.

IoT Edge | Properties

IoT Hub	myasetest-iothub1
IoT Edge device	myasetest-fpga-edge
IoT device for storage gateway	myasetest-fpga-storagegateway
Platform	Linux

Remove compute configuration

Take the following steps in the Azure portal to remove the existing Edge compute configuration for your device.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge > Overview**. Select **Remove** on the command bar.

IoT Edge | Overview

IoT Edge service is running fine!

Modules

Triggers

Remove

- If you remove the compute configuration, you will need to reconfigure your device in case you need to use compute again. When prompted for confirmation, select **Yes**.

Remove IoT Edge Service

⚠ This operation cannot be undone. The following entities will be removed from your device.

Triggers

Modules

OK

Cancel

Sync up IoT device and IoT Edge device access keys

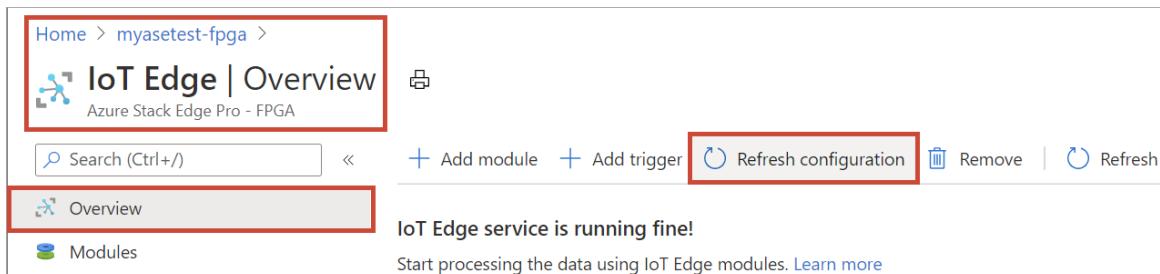
When you configure compute on your Azure Stack Edge Pro FPGA, an IoT device and an IoT Edge device are created. These devices are automatically assigned symmetric access keys. As a security best practice, these keys are rotated regularly via the IoT Hub service.

To rotate these keys, you can go to the IoT Hub service that you created and select the IoT device or the IoT Edge device. Each device has a primary access key and a secondary access keys. Assign the primary access key to the secondary access key and then regenerate the primary access key.

If your IoT device and IoT Edge device keys have been rotated, then you need to refresh the configuration on your Azure Stack Edge Pro FPGA to get the latest access keys. The sync helps the device get the latest keys for your IoT device and IoT Edge device. Azure Stack Edge Pro FPGA uses only the primary access keys.

Take the following steps in the Azure portal to sync the access keys for your device.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **IoT Edge > Overview**. Select **Refresh configuration** on the command bar.



2. Select **Yes** when prompted for confirmation.

Refresh configuration

Refresh configuration will get the latest connection credentials for the IoT Edge components and synchronize with on-premises device.

Yes

No

3. Exit out of the dialog once the sync is complete.

Next steps

- Learn how to [Manage Edge compute network via Azure portal](#).

Enable compute network on your Azure Stack Edge Pro

9/21/2022 • 2 minutes to read • [Edit Online](#)

This article describes how the modules running on your Azure Stack Edge Pro can access the compute network enabled on the device.

To configure the network, you'll take the following steps:

- Enable a network interface on your Azure Stack Edge Pro device for compute
- Add a module to access compute network on your Azure Stack Edge Pro
- Verify the module can access the enabled network interface

In this tutorial, you'll use a webserver app module to demonstrate the scenario.

Prerequisites

Before you begin, you'll need:

- An Azure Stack Edge Pro device with device setup completed.
- You've completed **Configure compute** step as per the [Tutorial: Transform data with Azure Stack Edge Pro](#) on your device. Your device should have an associated IoT Hub resource, an IoT device, and an IoT Edge device.

Enable network interface for compute

To access the modules running on your device via an external network, you'll need to assign an IP address to a network interface on your device. You can manage these compute settings from your local web UI.

Take the following steps on your local web UI to configure compute settings.

1. In the local web UI, go to **Configuration > Compute settings**.
2. **Enable** the network interface that you want to use to connect to a compute module that you'll run on the device.
 - If using static IP addresses, enter an IP address for the network interface.
 - If using DHCP, the IP addresses are automatically assigned. This example uses DHCP.

The screenshot shows the 'Compute settings' page for an Azure Stack Edge device named 'MyAzureStackEdge1'. The left sidebar lists various configuration options: Dashboard, Configuration (Device name, Network settings, Web proxy settings, Time settings, Storage settings, Cloud settings), Maintenance (Power settings, Hardware status, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The 'Compute settings' option is selected and highlighted with a red box. The main content area displays network configuration for five ports:

- Port 2 (F4-E9-D4-69-E1-F2) (1 Gbps)**: 'Enable for compute' is set to Yes (highlighted with a red box). Network: 10.128.24.0 (DHCP). IP address: ...
- Port 3 (F4-E9-D4-69-E1-F1) (25 Gbps)**: 'Enable for compute' is set to No. Network: 10.128.24.0 (DHCP). IP address: ...
- Port 4 (F4-E9-D4-69-E1-F0) (25 Gbps)**: 'Enable for compute' is set to Yes. Network: 5.5.0.0 (DHCP). IP address: ...
- Port 5 (F4-E9-D4-65-EA-5F) (25 Gbps)**: 'Enable for compute' is set to No.

- Select **Apply** to apply the settings. Make a note of the IP address assigned to the network interface if using DHCP.

The screenshot shows the 'Compute settings' page for an Azure Stack Edge device. The left sidebar and main content area are identical to the previous screenshot, except for the network configuration for Port 2:

- Port 2 (00-15-5D-69-E1-F2) (1 Gbps)**: 'Enable for compute' is set to Yes. Network: 10.128.44.0 (DHCP). The 'IP address' field (10.128.47.78) is highlighted with a red box.
- Port 3 (F4-E9-D4-69-E1-F1) (25 Gbps)**: 'Enable for compute' is set to No.

Add webserver app module

Take the following steps to add a webserver app module on your Azure Stack Edge Pro device.

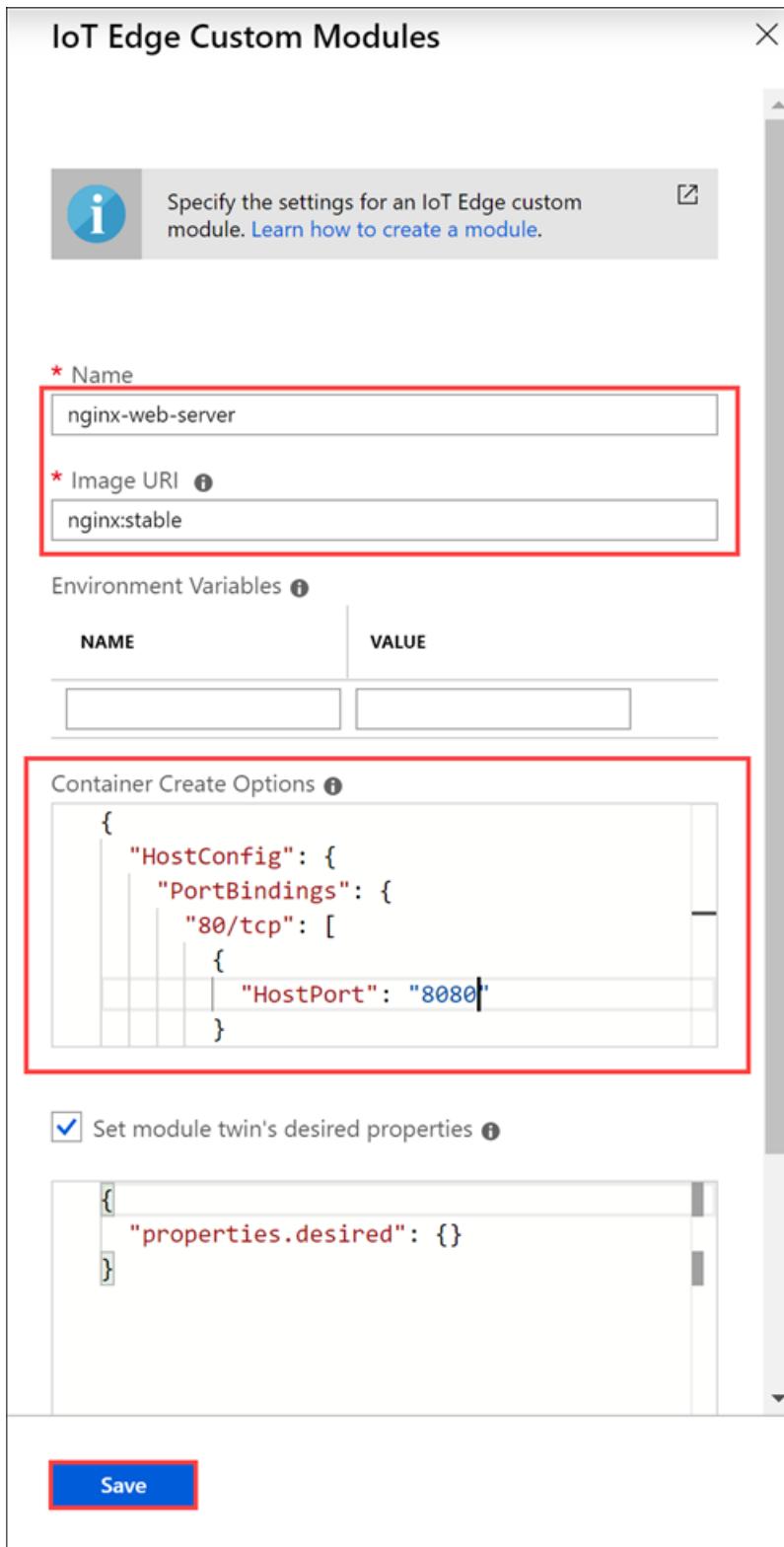
- Go to the IoT Hub resource associated with your Azure Stack Edge Pro device and then select **IoT Edge device**.
- Select the IoT Edge device associated with your Azure Stack Edge Pro device. On the **Device details**, select **Set modules**. On **Add modules**, select **+ Add** and then select **IoT Edge Module**.
- In the **IoT Edge custom modules** blade:
 - Specify a **Name** for your webserver app module that you want to deploy.

b. Provide an **Image URI** for your module image. A module matching the provided name and tags is retrieved. In this case, `mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine` will pull an nginx image (tagged as `1.15.5-alpine`) from the public `mcr.microsoft.com` registry.

c. In the **Container Create Options**, paste the following sample code:

```
{  
    "HostConfig": {  
        "PortBindings": {  
            "80/tcp": [  
                {  
                    "HostPort": "8080"  
                }  
            ]  
        }  
    }  
}
```

This configuration lets you access the module using the compute network IP over *http* on TCP port 8080 (with the default webserver port being 80).



d. Select Save.

Verify module access

1. Verify the module is successfully deployed and is running. On the **Device Details** page, on the **Modules** tab, the runtime status of the module should be **running**.
2. Connect to the web server app module. Open a browser window and type:

```
http://<compute-network-IP-address>:8080
```

You should see that the webserver app is running.



Next steps

- Learn how to [Manage users via Azure portal](#).

Use the Azure portal to manage shares on Azure Stack Edge Pro FPGA

9/21/2022 • 8 minutes to read • [Edit Online](#)

This article describes how to manage shares on your Azure Stack Edge Pro FPGA device. You can manage the Azure Stack Edge Pro FPGA device via the Azure portal or via the local web UI. Use the Azure portal to add, delete, refresh shares, or sync storage key for storage account associated with the shares.

About shares

To transfer data to Azure, you need to create shares on your Azure Stack Edge Pro FPGA. The shares that you add on the Azure Stack Edge Pro FPGA device can be local shares or shares that push data to cloud.

- **Local shares:** Use these shares when you want the data to be processed locally on the device.
- **Shares:** Use these shares when you want the device data to be automatically pushed to your storage account in the cloud. All the cloud functions such as **Refresh** and **Sync storage keys** apply to the shares.

In this article, you learn how to:

- Add a share
- Delete a share
- Refresh shares
- Sync storage key

Add a share

Do the following steps in the Azure portal to create a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway**. Go to **Shares** and then select **+ Add share** on the command bar.

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

2. In **Add Share**, specify the share settings. Provide a unique name for your share.

Share names can only contain numbers, lowercase letters, and hyphens. The share name must be between 3 and 63 characters long and begin with a letter or a number. Each hyphen must be preceded and followed by a non-hyphen character.

3. Select a **Type** for the share. The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients. Depending upon whether you choose SMB or NFS shares, options presented are slightly different.

- Provide a **Storage account** where the share lives. A container is created in the storage account with the share name if the container already does not exist. If the container already exists, then the existing container is used.
- From the dropdown list, choose the **Storage service** from block blob, page blob, or files. The type of the service chosen depends on which format you want the data to reside in Azure. For example, in this instance, we want the data to reside as block blobs in Azure, hence we select **Block Blob**. If choosing **Page Blob**, you must ensure that your data is 512 bytes aligned. Use **Page blob** for VHDs or VHDX that are always 512 bytes aligned.

IMPORTANT

Make sure that the Azure Storage account that you use does not have immutability policies set on it if you are using it with a Azure Stack Edge or Data Box Gateway device. For more information, see [Set and manage immutability policies for blob storage](#).

- This step depends on whether you are creating an SMB or an NFS share.

- If creating an **SMB share** - In the **All privilege local user** field, choose from **Create new** or **Use existing**. If creating a new local user, provide the **username**, **password**, and then confirm password. This assigns the permissions to the local user. After you have assigned the permissions here, you can then use File Explorer to modify these permissions.

Add share

myasetest

Share details

Name ***** myasesmb1 ✓

Type ***** SMB NFS

Use the share with Edge compute ✓
(i)

Configure as Edge local share

Storage account ***** (i) ▼

Storage service (i) ▼

User details

Allow only read operations

All privilege local user ✓ Create new Use existing

User name ***** Admin1 ✓

Password ***** ✓

Confirm password ***** ✓

Create

If you check allow only read operations for this share data, you can specify read-only users.

- If creating an NFS share - You need to supply the IP addresses of the allowed clients that can access the share.

Add share

myasetest

Share details

Name * mynfsshare

Type * SMB NFS

Use the share with Edge compute

Configure as Edge local share

Storage account * mystorageaccount02

Storage service * Block Blob

Select blob container * Create new Use existing mynfsshare

User details

Allow only read operations

Allowed client IP addresses

10.100.100.10

Enter an IP address.

7. To easily access the shares from Edge compute modules, use the local mount point. Select **Use the share with Edge compute** so that the share is automatically mounted after it is created. When this option is selected, the Edge module can also use the compute with the local mount point.
8. Click **Create** to create the share. You are notified that the share creation is in progress. After the share is created with the specified settings, the **Shares** blade updates to reflect the new share.

Add a local share

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. Select **+ Add share** on the command bar.

The screenshot shows the 'Cloud storage gateway | Shares' page. On the left, there's a sidebar with links: 'Overview' (highlighted with a red box), 'Shares' (highlighted with a red box), 'Storage accounts', 'Users', and 'Bandwidth'. At the top right is a close button ('X'). Below the sidebar is a search bar ('Search (Ctrl+/)') and a 'Refresh' button. A large 'Add share' button with a plus sign is prominently displayed. The main area is a table with columns: Name, Status, Type, Used for compute, Storage account, Storage service, and three dots. Two rows are listed: 'mysmb-cloudshare' (Status: OK, Type: SMB, Used for compute: Disabled, Storage account: mynewsa1, Storage service: Block Blob) and 'mysmb-localshare' (Status: OK, Type: SMB, Used for compute: Disabled, Storage account: -, Storage service: -). The 'Shares' link in the sidebar and the 'Add share' button are both highlighted with red boxes.

2. In **Add Share**, specify the share settings. Provide a unique name for your share.

Share names can only contain numbers, lowercase letters, and hyphens. The share name must be between 3 and 63 characters long and begin with a letter or a number. Each hyphen must be preceded and followed by a non-hyphen character.

3. Select a **Type** for the share. The type can be **SMB** or **NFS**, with SMB being the default. SMB is the standard for Windows clients, and NFS is used for Linux clients. Depending upon whether you choose SMB or NFS shares, options presented are slightly different.
4. To easily access the shares from Edge compute modules, use the local mount point. Select **Use the share with Edge compute** so that the Edge module can use the compute with the local mount point.
5. Select **Configure as Edge local shares**. The data in local shares will stay locally on the device. You can process this data locally.
6. In the **All privilege local user** field, choose from **Create new** or **Use existing**.
7. Select **Create**.

Add share

X

myasetest

Share details

Name *

mysharelocal1



Type * ⓘ

SMB

NFS

Use the share with Edge compute



Configure as Edge local share ⓘ



Use an Edge local share to process data prior to upload to the cloud. Data in local shares stays on the device.

User details

All privilege local user ⓘ

Create new

Use existing

Admin



Create

You see a notification that the share creation is in progress. After the share is created with the specified settings, the **Shares** blade updates to reflect the new share.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares

myasetest

Search (Ctrl+ /) Add share Refresh

Overview

Shares

Storage accounts

Users

Bandwidth

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Disabled	mynewsal1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

Mount a share

If you created a share before you configured compute on your Azure Stack Edge device, you will need to mount the share. Take the following steps to mount a share.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. From the list of the shares, select the share you want to mount. The **Used for compute** column will show the status as **Disabled** for the selected share.

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

2. Select **Mount**.

Status	OK
Type	SMB
Mounted (Used for compute)	Disabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Select users	Admin

3. When prompted for confirmation, select **Yes**. This will mount the share.

Mount share

Are you sure you want to go ahead with the mount operation?

Yes **No**

4. After the share is mounted, go to the list of shares. You'll see that the **Used for compute** column shows the share status as **Enabled**.

Name	Status	Type	Used for compute	Storage account	Storage service
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

5. Select the share again to view the local mountpoint for the share. Edge compute module uses this local mountpoint for the share.

mysmb-cloudshare

myasetest

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Local mount point for Edge compute modules	/home/databox-edge/hostgatewayshares/mysmb-cloudshare
Select users	Admin

Unmount a share

Do the following steps in the Azure portal to unmount a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares

myasetest

Search (Ctrl+ /) Add share Refresh

Overview Shares Storage accounts Users Bandwidth

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

2. From the list of the shares, select the share that you want to unmount. You want to make sure that the share you unmount is not used by any modules. If the share is used by a module, then you will see issues with the corresponding module. Select **Unmount**.

mysmb-cloudshare

myasetest

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mynewsa1
Storage account container	mysmb-cloudshare
Last updated time	-
Last update error logs	-
Local mount point for Edge compute modules	/home/databox-edge/hostgatewayshares/mysmb-cloudshare
Select users	Admin

3. When prompted for confirmation, select **Yes**. This will unmount the share.

mysmb-cloudshare

myasetest

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Unmount share

Ensure that the share isn't used by a module. If the share is in use, you will see issues with the module. Are you sure you want to unmount the share?

Yes **No**

4. After the share is unmounted, go to the list of shares. You'll see that **Used for compute** column shows the share status as **Disabled**.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares

myasetest

Search (Ctrl+ /) Add share Refresh

Name	Status	Type	Used for compute	Storage account	Storage service	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Disabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

Delete a share

Do the following steps in the Azure portal to delete a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. From the list of shares, select and click the share that you want to delete.

Name	Status	Type	Used for compute	Storage account	Storage service
myasesmblocal2	OK	SMB	Enabled	-	-
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

2. Select **Delete**.

This share stores data locally and won't be pushing data to cloud. Some cloud functionalities are disabled. Ensure you delete the data post processing to avoid running out of capacity.

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Local mount point for Edge compute modules	/home/hcsshares/myasesmblocal2
Select users	Admin1

3. When prompted for confirmation, click **Yes**.

Delete share

Ensure that the share isn't being used by any modules. If the share is in-use, you will see issues with the module. This does not remove the data residing in your storage account. Delete this data from your storage account to avoid charges. Are you sure you want to delete the share?

Yes No

The list of shares updates to reflect the deletion.

Refresh shares

The refresh feature allows you to refresh the contents of a share. When you refresh a share, a search is initiated to find all the Azure objects including blobs and files that were added to the cloud since the last refresh. These additional files are then downloaded to refresh the contents of the share on the device.

IMPORTANT

- You can't refresh local shares.
- Permissions and access control lists (ACLs) are not preserved across a refresh operation.

Do the following steps in the Azure portal to refresh a share.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. Select and click the share that you want to refresh.

Name	Status	Type	Used for compute	Storage account	Storage service
myasesmb1	OK	SMB	Enabled	mytests1	Block Blob
myasesmblocal2	OK	SMB	Enabled	-	-
mysharelocal1	OK	SMB	Enabled	-	-
mysmb-cloudshare	OK	SMB	Enabled	mynews1	Block Blob
mysmb-localshare	OK	SMB	Disabled	-	-

2. Select **Refresh data**.

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mytests1
Storage account container name	myasesmb1
Last refresh time	-
Last refresh error logs	-
Local mount point for Edge compute modules	/home/hcssshares/myasesmb1
Select users	Admin1

3. When prompted for confirmation, select **Yes**. A job starts to refresh the contents of the on-premises share.

Refresh Edge share
This action finds objects in Azure storage that were last added, modified, and removed from the on-premises share. The metadata for these objects is refreshed. Are you sure you want to refresh the share metadata?

Yes **No**

4. While the refresh is in progress, the refresh option is grayed out in the context menu. Click the job notification to view the refresh job status.
5. The time to refresh depends on the number of files in the Azure container as well as the files on the device. Once the refresh has successfully completed, the share timestamp is updated. Even if the refresh has partial failures, the operation is considered successful and the timestamp is updated. The refresh error logs are also updated.

myasesmb1
MyAzureStackEdge1

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Status	OK
Type	SMB
Mounted (Used for compute)	Enabled
Storage account	mytestsa1
Storage account container name	myasesmb1
Last refresh time	3/12/2019, 09:01:06
Last refresh error logs	mytestsa1\myasesmb1__Microsoft Azure Stack Edge__Refresh
Local mount point for Edge compute modules	/home/hcsshares/myasesmb1
Select users	Admin1

If there is a failure, an alert is raised. The alert details the cause and the recommendation to fix the issue. The alert also links to a file that has the complete summary of the failures including the files that failed to update or delete.

Sync storage keys

If your storage account keys have been rotated, then you need to sync the storage access keys. The sync helps the device get the latest keys for your storage account.

Do the following steps in the Azure portal to sync your storage access key.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Cloud storage gateway > Shares**. From the list of shares, choose and click a share associated with the storage account that you need to sync.

Home > myasetest > Cloud storage gateway

Cloud storage gateway | Shares

myasetest

Search (Ctrl+ /) Add share Refresh

Overview

Shares

Storage accounts

Users

Bandwidth

Name	Status	Type	Used for compute	Storage account	Storage service	...
myasesmb1	OK	SMB	Enabled	mytestsa1	Block Blob	...
myasesmblocal2	OK	SMB	Enabled	-	-	...
mysharelocal1	OK	SMB	Enabled	-	-	...
mysmb-cloudshare	OK	SMB	Enabled	mynewsa1	Block Blob	...
mysmb-localshare	OK	SMB	Disabled	-	-	...

2. Click **Sync storage key**. Click **Yes** when prompted for confirmation.

myasesmb1
MyAzureStackEdge1

Save Discard Refresh data Sync storage keys Mount Unmount Delete

Synchronize storage account keys

This action updates the storage account access keys for the storage account attached to your device. Are you sure you want to synchronize the keys?

Yes No

3. Exit out of the dialog once the sync is complete.

NOTE

You only have to do this once for a given storage account. You don't need to repeat this action for all the shares associated with the same storage account.

Next steps

- Learn how to [Manage users via Azure portal](#).

Use the Azure portal to manage users on your Azure Stack Edge Pro FPGA

9/21/2022 • 2 minutes to read • [Edit Online](#)

This article describes how to manage users on your Azure Stack Edge Pro FPGA device. You can manage the Azure Stack Edge Pro FPGA via the Azure portal or via the local web UI. Use the Azure portal to add, modify, or delete users.

In this article, you learn how to:

- Add a user
- Modify user
- Delete a user

About users

Users can be read-only or full privilege. As the names indicate, the read-only users can only view the share data. The full privilege users can read share data, write to these shares, and modify or delete the share data.

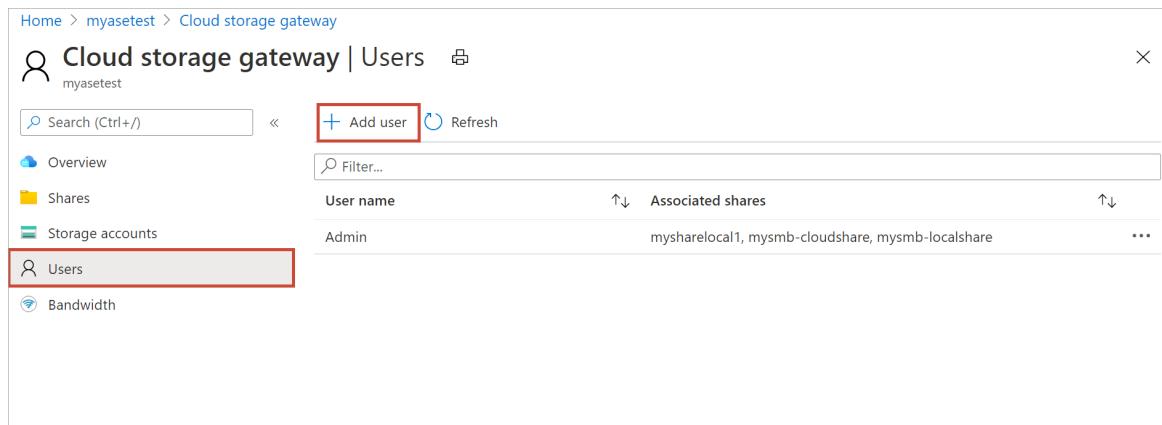
- **Full privilege user** - A local user with full access.
- **Read-only user** - A local user with read-only access. These users are associated with shares that allow read-only operations.

The user permissions are first defined when the user is created during share creation. Modification of share-level permissions is currently not supported.

Add a user

Do the following steps in the Azure portal to add a user.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Users**. Select **+ Add user** on the command bar.



The screenshot shows the Azure portal interface for managing users in a Cloud storage gateway. The top navigation bar includes 'Home > myasetest > Cloud storage gateway'. On the left, there's a sidebar with links: Overview, Shares, Storage accounts, **Users** (which is selected and highlighted with a red box), and Bandwidth. The main content area has a search bar ('Search (Ctrl+ /)') and a 'Filter...' button. At the top right, there are 'Add user' (highlighted with a red box), 'Refresh', and 'X' buttons. Below these are two columns: 'User name' and 'Associated shares'. A single row is listed: 'Admin' with 'mysharelocal1, mysmb-cloudshare, mysmb-localshare' under 'Associated shares'. There are also 'Up/Down' arrows and a 'More' (three dots) button.

2. Specify the username and password for the user you want to add. Confirm the password and select **Add**.

Add user

MyAzureStackEdge1

* User name	Admin2	✓
* Password	✓
* Confirm password	✓

Add

IMPORTANT

These users are reserved by the system and should not be used: Administrator, EdgeUser, EdgeSupport, HcsSetupUser, WDAGUtilityAccount, CLIUSR, DefaultAccount, Guest.

3. A notification is shown when the user creation starts and is completed. After the user is created, from the command bar, select **Refresh** to view the updated list of users.

Modify user

You can change the password associated with a user once the user is created. Select from the list of users. Enter and confirm the new password. Save the changes.

Modify user

MyAzureStackEdge1

Save **Discard** **Delete**

User name	Admin1
Associated shares	myasesmblocalcomp1 myasesmb1 myasesmbcomp1
Password
Confirm password

Delete a user

Do the following steps in the Azure portal to delete a user.

1. In the Azure portal, go to your Azure Stack Edge resource and then go to **Users**.

Home > myasetest > Cloud storage gateway

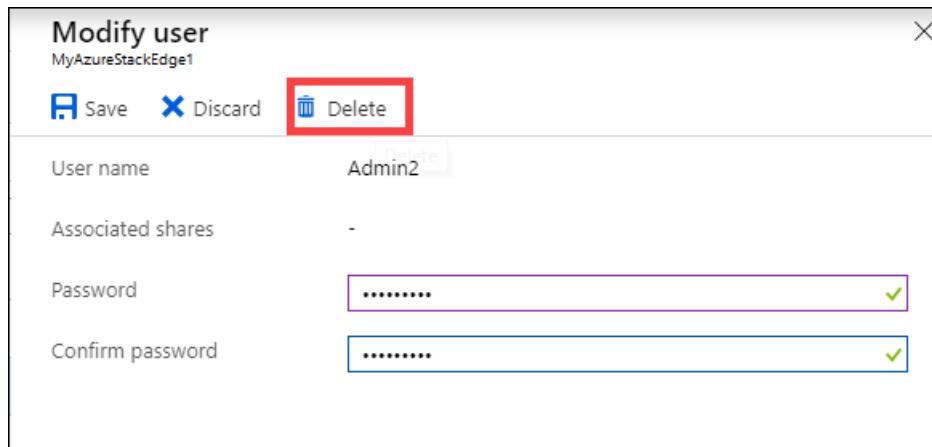
Cloud storage gateway | Users

Search (Ctrl+ /)	Add user	Refresh
Overview		
Shares		
Storage accounts		
Users		
Bandwidth		

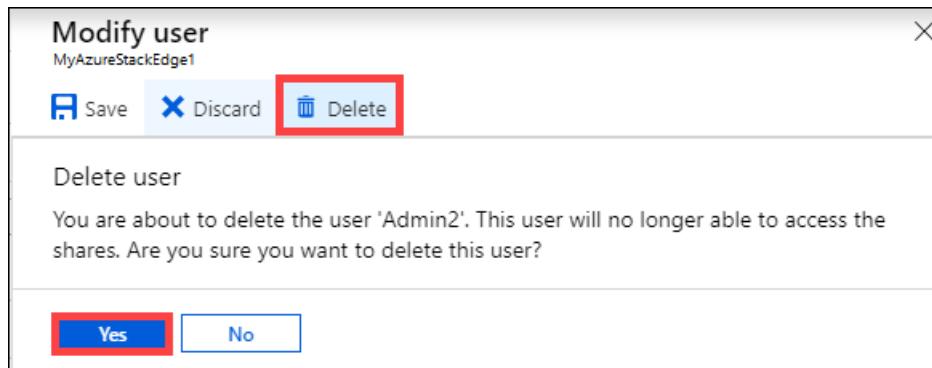
User name Associated shares

Admin	mysharelocal1, myasesmb1, mysmb-cloudshare, mysmb-localshare	...
Admin2	-	...
user01	myasesmblocal2	...

2. Select a user from the list of users and then select **Delete**.



- When prompted, confirm the deletion.



The list of users is updated to reflect the deleted user.

The screenshot shows the 'Cloud storage gateway | Users' page. On the left, there is a sidebar with 'Overview', 'Shares', 'Storage accounts', and 'Users' (which is highlighted with a red box). The main area displays a table of users:

User name	Associated shares	Actions
Admin	mysharelocal1, myasesmb1, mysmb-cloudshare, mysmb-localshare	...
user01	myasesmblocal2	...

Next steps

- Learn how to [Manage bandwidth](#).

Use the Azure portal to manage bandwidth schedules on your Azure Stack Edge Pro FPGA

9/21/2022 • 2 minutes to read • [Edit Online](#)

This article describes how to manage users on your Azure Stack Edge Pro FPGA. Bandwidth schedules allow you to configure network bandwidth usage across multiple time-of-day schedules. These schedules can be applied to the upload and download operations from your device to the cloud.

You can add, modify, or delete the bandwidth schedules for your Azure Stack Edge Pro FPGA via the Azure portal.

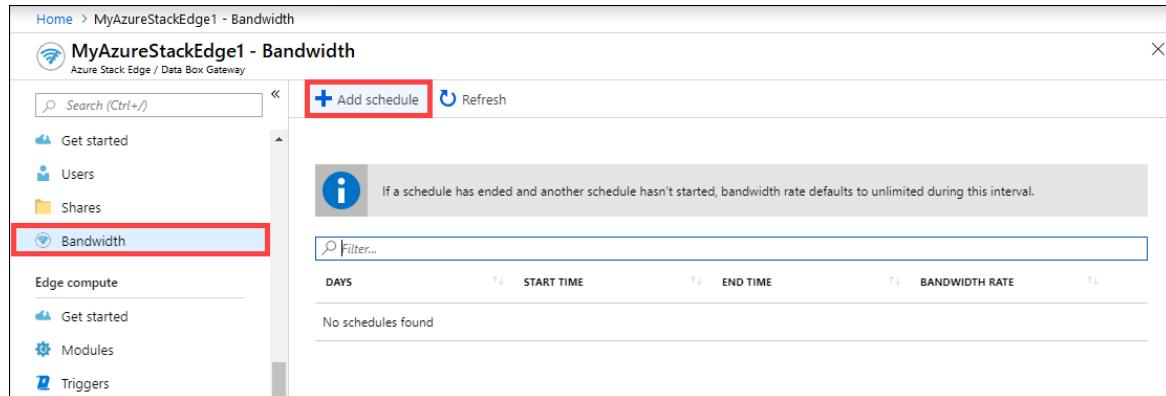
In this article, you learn how to:

- Add a schedule
- Modify schedule
- Delete a schedule

Add a schedule

Do the following steps in the Azure portal to add a schedule.

1. In the Azure portal for your Azure Stack Edge resource, go to **Bandwidth**.
2. In the right-pane, select **+ Add schedule**.



3. In the **Add schedule**:
 - a. Provide the **Start day**, **End day**, **Start time**, and **End time** of the schedule.
 - b. Check the **All day** option if this schedule should run all day.
 - c. **Bandwidth rate** is the bandwidth in Megabits per second (Mbps) used by your device in operations involving the cloud (both uploads and downloads). Supply a number between 20 and 1,000,000,007 for this field.
 - d. Check **Unlimited** bandwidth if you do not want to throttle the date upload and download.
 - e. Select **Add**.

Add schedule

MyAzureStackEdge1

* Start day	Monday
* End day	Friday
All day	<input type="checkbox"/>
* Start time	8:00 AM
* End time	6:00 PM
Unlimited bandwidth <small>(i)</small>	<input type="checkbox"/>
Bandwidth rate (Mbps) <small>(i)</small>	35 <small>(✓)</small>

Add

- A schedule is created with the specified parameters. This schedule is then displayed in the list of bandwidth schedules in the portal.

Home > MyAzureStackEdge1 - Bandwidth

MyAzureStackEdge1 - Bandwidth
Azure Stack Edge / Data Box Gateway

+ Add schedule Refresh

If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Days	Start Time	End Time	Bandwidth Rate	...
Monday, Tuesday, Wednesday, ...	08:00:00	18:00:00	35 (Mbps)	...

Edit schedule

Do the following steps to edit a bandwidth schedule.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **Bandwidth**.
- From the list of bandwidth schedules, select and select a schedule that you want to modify.

Home > MyAzureStackEdge1 - Bandwidth

MyAzureStackEdge1 - Bandwidth
Azure Stack Edge / Data Box Gateway

+ Add schedule Refresh

If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Days	Start Time	End Time	Bandwidth Rate	...
Monday, Tuesday, Wednesday, ...	08:00:00	18:00:00	35 (Mbps)	...

- Make the desired changes and save the changes.

Edit schedule

MyAzureStackEdge1

Save **Discard** **Delete**

* Start day	Monday
* End day	Friday
All day	<input type="checkbox"/>
* Start time	8:00 AM
* End time	5:00 PM
Unlimited bandwidth <small>(i)</small>	<input type="checkbox"/>
Bandwidth rate (Mbps) <small>(i)</small>	50

- After the schedule is modified, the list of schedules is updated to reflect the modified schedule.

Home > MyAzureStackEdge1 - Bandwidth

MyAzureStackEdge1 - Bandwidth

Azure Stack Edge / Data Box Gateway

Add schedule **Refresh**

Bandwidth

If a schedule has ended and another schedule hasn't started, bandwidth rate defaults to unlimited during this interval.

Filter...

DAYS	START TIME	END TIME	BANDWIDTH RATE	...
Monday, Tuesday, Wednesday, ...	08:00:00	17:00:00	50 (Mbps)	...

Delete a schedule

Do the following steps to delete a bandwidth schedule associated with your Azure Stack Edge Pro FPGA device.

- In the Azure portal, go to your Azure Stack Edge resource and then go to **Bandwidth**.
- From the list of bandwidth schedules, select a schedule that you want to delete. In the **Edit schedule**, select **Delete**. When prompted for confirmation, select **Yes**.

Edit schedule

MyAzureStackEdge1

Save **Discard** **Delete**

Delete schedule

Do you want to delete this schedule?

Yes **No**

- After the schedule is deleted, the list of schedules is updated.

Next steps

- Learn how to [Manage shares](#).

Manage access, power, and connectivity mode for your Azure Stack Edge Pro FPGA

9/21/2022 • 5 minutes to read • [Edit Online](#)

This article describes how to manage the access, power, and connectivity mode for your Azure Stack Edge Pro FPGA. These operations are performed via the local web UI or the Azure portal.

In this article, you learn how to:

- Manage device access
- Manage connectivity mode
- Manage power

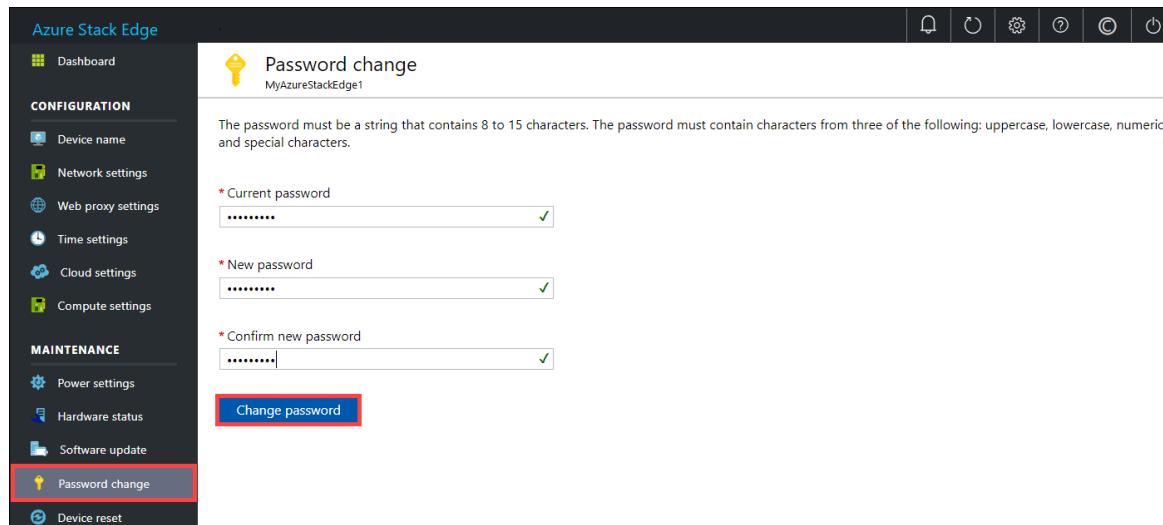
Manage device access

The access to your Azure Stack Edge Pro FPGA device is controlled by the use of a device password. You can change the password via the local web UI. You can also reset the device password in the Azure portal.

Change device password

Follow these steps in the local UI to change the device password.

1. In the local web UI, go to **Maintenance > Password change**.
2. Enter the current password and then the new password. The supplied password must be between 8 and 16 characters. The password must have 3 of the following characters: uppercase, lowercase, numeric, and special characters. Confirm the new password.



3. Select **Change password**.

Reset device password

The reset workflow does not require the user to recall the old password and is useful when the password is lost. This workflow is performed in the Azure portal.

1. In the Azure portal, go to **Overview > Reset admin password**.

The screenshot shows the Azure Stack Edge / Data Box Gateway management interface. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, and Properties. The 'Overview' tab is currently selected. At the top right, there are buttons for Add share, Update device, Reset device password (which is highlighted with a red box), Feedback, Refresh, and Delete. Below these buttons, there are two main sections: 'Device' and 'Shares'. The 'Device' section displays Device status: Online, Capacity: 11.89 TB, and Software version: Azure Stack Edge 1903. The 'Shares' section shows 3 shares, all of which are OK.

2. Enter the new password and then confirm it. The supplied password must be between 8 and 16 characters. The password must have 3 of the following characters: uppercase, lowercase, numeric, and special characters. Select **Reset**.

The screenshot shows a 'Reset device password' dialog box. It has two input fields: 'New password' and 'Confirm password', both containing masked text. A red box highlights the 'Reset' button at the bottom.

Manage resource access

To create your Azure Stack Edge / Data Box Gateway, IoT Hub, and Azure Storage resource, you need permissions as a contributor or higher at a resource group level. You also need the corresponding resource providers to be registered. For any operations that involve activation key and credentials, permissions to the Microsoft Graph API are also required. These are described in the following sections.

Manage Microsoft Graph API permissions

When generating the activation key for the Azure Stack Edge Pro FPGA device, or performing any operations that require credentials, you need permissions to Azure Active Directory Graph API. The operations that need credentials could be:

- Creating a share with an associated storage account.
- Creating a user who can access the shares on the device.

You should have a **User** access on Active Directory tenant as you need to be able to

Read all directory objects. You can't be a Guest user as they don't have permissions to

Read all directory objects. If you're a guest, then the operations such as generation of an activation key, creation of a share on your Azure Stack Edge Pro FPGA device, creation of a user, configuration of Edge compute role, reset device password will all fail.

For more information on how to provide access to users to Microsoft Graph API, see [Microsoft Graph permissions reference](#).

Register resource providers

To provision a resource in Azure (in the Azure Resource Manager model), you need a resource provider that supports the creation of that resource. For example, to provision a virtual machine, you should have a

'Microsoft.Compute' resource provider available in the subscription.

Resource providers are registered on the level of the subscription. By default, any new Azure subscription is pre-registered with a list of commonly used resource providers. The resource provider for 'Microsoft.DataBoxEdge' is not included in this list.

You don't need to grant access permissions to the subscription level for users to be able to create resources like 'Microsoft.DataBoxEdge' within their resource groups that they have owner rights on, as long as the resource providers for these resources is already registered.

Before you attempt to create any resource, make sure that the resource provider is registered in the subscription. If the resource provider is not registered, you'll need to make sure that the user creating the new resource has enough rights to register the required resource provider on the subscription level. If you haven't done this as well, then you'll see the following error:

The subscription <Subscription name> doesn't have permissions to register the resource provider(s): Microsoft.DataBoxEdge.

To get a list of registered resource providers in the current subscription, run the following command:

```
Get-AzResourceProvider -ListAvailable |where {$_.Registrationstate -eq "Registered"}
```

For Azure Stack Edge Pro FPGA device, `Microsoft.DataBoxEdge` should be registered. To register `Microsoft.DataBoxEdge`, subscription admin should run the following command:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.DataBoxEdge
```

For more information on how to register a resource provider, see [Resolve errors for resource provider registration](#).

Manage connectivity mode

Apart from the default fully connected mode, your device can also run in partially connected, or fully disconnected mode. Each of these modes is described as below:

- **Fully connected** - This is the normal default mode in which the device operates. Both the cloud upload and download of data is enabled in this mode. You can use the Azure portal or the local web UI to manage the device.
- **Partially connected** – In this mode, the device cannot upload or download any share data however can be managed via the Azure portal.

This mode is typically used when on a metered satellite network and the goal is to minimize network bandwidth consumption. Minimal network consumption may still occur for device monitoring operations.

- **Disconnected** – In this mode, the device is fully disconnected from the cloud and both the cloud uploads and downloads are disabled. The device can only be managed via the local web UI.

This mode is typically used when you want to take your device offline.

To change device mode, follow these steps:

1. In the local web UI of your device, go to **Configuration > Cloud settings**.
2. From the dropdown list, select the mode that you want to operate the device in. You can select from **Fully connected**, **Partially connected**, and **Fully disconnected**. To run the device in partially disconnected mode, enable **Azure portal management**.

The screenshot shows the Azure Stack Edge local web interface. On the left, a sidebar menu includes options like Dashboard, Configuration (Device name, Network settings, Web proxy settings, Time settings, Cloud settings), Maintenance (Power settings, Hardware status, Software update, Password change, Device reset), and Help. The 'Cloud settings' option is highlighted with a red box. The main content area is titled 'Cloud settings' for 'MyAzureStackEdge1'. It has sections for Activation (with a note about secret keys) and Connectivity mode. Under Connectivity mode, it says 'Configure the mode to control the cloud data transfer and Azure portal management. Learn more'. It lists three modes: Fully connected, Partially connected (selected and highlighted with a red box), and Fully disconnected. Below is a dropdown menu set to 'Partially connected'. At the bottom is a blue 'Apply settings' button.

Manage power

You can shut down or restart your physical device using the local web UI. We recommend that before you restart, take the shares offline on the data server and then the device. This action minimizes any possibility of data corruption.

1. In the local web UI, go to **Maintenance > Power settings**.
2. Select **Shutdown** or **Restart** depending on what you intend to do.

The screenshot shows the Azure Stack Edge local web interface. The sidebar menu highlights 'Power settings'. The main content area is titled 'Power settings' for 'MyAzureStackEdge1'. It contains two sections: 'Shut down' (described as shutting down the device) and 'Restart' (described as restarting the device). Both buttons are highlighted with red boxes.

3. When prompted for confirmation, select **Yes** to proceed.

NOTE

If you shut down the physical device, you will need to push the power button on the device to turn it on.

Next steps

- Learn how to [Manage shares](#).

Manage an Azure Stack Edge Pro FPGA device via Windows PowerShell

9/21/2022 • 13 minutes to read • [Edit Online](#)

Azure Stack Edge Pro FPGA solution lets you process data and send it over the network to Azure. This article describes some of the configuration and management tasks for your Azure Stack Edge Pro FPGA device. You can use the Azure portal, local web UI, or the Windows PowerShell interface to manage your device.

This article focuses on the tasks you do using the PowerShell interface.

This article includes the following procedures:

- Connect to the PowerShell interface
- Create a support package
- Upload certificate
- Reset the device
- View device information
- Get compute logs
- Monitor and troubleshoot compute modules

Connect to the PowerShell interface

Depending on the operating system of client, the procedures to remotely connect to the device are different.

Remotely connect from a Windows client

Before you begin, make sure that your Windows client is running Windows PowerShell 5.0 or later.

Follow these steps to remotely connect from a Windows client.

1. Run a Windows PowerShell session as an administrator.
2. Make sure that the Windows Remote Management service is running on your client. At the command prompt, type:

```
winrm quickconfig
```

For more information, see [Installation and configuration for Windows Remote Management](#).

3. Assign a variable to the device IP address.

```
$ip = "<device_ip>"
```

Replace `<device_ip>` with the IP address of your device.

4. To add the IP address of your device to the client's trusted hosts list, type the following command:

```
Set-Item WSMAN:\localhost\Client\TrustedHosts $ip -Concatenate -Force
```

5. Start a Windows PowerShell session on the device:

```
Enter-PSSession -ComputerName $ip -Credential $ip\EdgeUser -ConfigurationName Minishell
```

6. Provide the password when prompted. Use the same password that is used to sign into the local web UI. The default local web UI password is *Password1*. When you successfully connect to the device using

remote PowerShell, you see the following sample output:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> winrm quickconfig
WinRM service is already running on this machine.
PS C:\WINDOWS\system32> $ip = "10.100.10.10"
PS C:\WINDOWS\system32> Set-Item WSMan:\localhost\Client\TrustedHosts $ip -Concatenate -Force
PS C:\WINDOWS\system32> Enter-PSSession -ComputerName $ip -Credential $ip\EdgeUser -ConfigurationName
Minishell

WARNING: The Windows PowerShell interface of your device is intended to be used only for the initial
network configuration. Please engage Microsoft Support if you need to access this interface to
troubleshoot any potential issues you may be experiencing. Changes made through this interface
without involving Microsoft Support could result in an unsupported configuration.

[10.100.10.10]: PS>
```

Remotely connect from a Linux client

On the Linux client that you'll use to connect:

- [Install the latest PowerShell Core for Linux](#) from GitHub to get the SSH remoting feature.
- [Install only the `gss-ntlmssp` package from the NTLM module](#). For Ubuntu clients, use the following command:
 - `sudo apt-get install gss-ntlmssp`

For more information, go to [PowerShell remoting over SSH](#).

Follow these steps to remotely connect from an NFS client.

1. To open PowerShell session, type:

```
pwsh
```

2. For connecting using the remote client, type:

```
Enter-PSSession -ComputerName $ip -Authentication Negotiate -ConfigurationName Minishell -Credential
~\EdgeUser
```

When prompted, provide the password used to sign into your device.

NOTE

This procedure does not work on Mac OS.

Create a support package

If you experience any device issues, you can create a support package from the system logs. Microsoft Support uses this package to troubleshoot the issues. Follow these steps to create a support package:

1. [Connect to the PowerShell interface of your device](#).
2. Use the `Get-HcsNodeSupportPackage` command to create a support package. The usage of the cmdlet is as follows:

```

Get-HcsNodeSupportPackage [-Path] <string> [-Zip] [-ZipFileName <string>] [-Include {None | RegistryKeys | EtwLogs | PeriodicEtwLogs | LogFiles | DumpLog | Platform | FullDumps | MiniDumps | ClusterManagementLog | ClusterLog | UpdateLogs | CbsLogs | StorageCmdlets | ClusterCmdlets | ConfigurationCmdlets | KernelDump | RollbackLogs | Symbols | NetworkCmdlets | NetworkCmds | Fltmc | ClusterStorageLogs | UTElement | UTFlag | SmbWmiProvider | TimeCmds | LocalUILogs | ClusterHealthLogs | BcdeditCommand | BitLockerCommand | DirStats | ComputeRolesLogs | ComputeCmdlets | DeviceGuard | Manifests | MeasuredBootLogs | Stats | PeriodicStatLogs | MigrationLogs | RollbackSupportPackage | ArchivedLogs | Default}] [-MinimumTimestamp <datetime>] [-MaximumTimestamp <datetime>] [-IncludeArchived] [-IncludePeriodicStats] [-Credential <pscredential>] [<CommonParameters>]

```

The cmdlet collects logs from your device and copies those logs to a specified network or local share.

The parameters used are as follows:

- `-Path` - Specify the network or the local path to copy support package to. (required)
- `-Credential` - Specify the credentials to access the protected path.
- `-Zip` - Specify to generate a zip file.
- `-Include` - Specify to include the components to be included in the support package. If not specified, `Default` is assumed.
- `-IncludeArchived` - Specify to include archived logs in the support package.
- `-IncludePeriodicStats` - Specify to include periodic stat logs in the support package.

Upload certificate

A proper SSL certificate ensures that you're sending encrypted information to the right server. Besides encryption, the certificate also allows for authentication. You can upload your own trusted SSL certificate via the PowerShell interface of the device.

1. [Connect to the PowerShell interface](#).
2. Use the `Set-HcsCertificate` cmdlet to upload the certificate. When prompted, provide the following parameters:
 - `CertificateFilePath` - Path to the share that contains the certificate file in `.pfx` format.
 - `CertificatePassword` - A password used to protect the certificate.
 - `Credentials` - Username to access the share that contains the certificate. Provide the password to the network share when prompted.

The following example shows the usage of this cmdlet:

```

Set-HcsCertificate -Scope LocalWebUI -CertificateFilePath
  "\\\myfileshare\certificates\mycert.pfx" -CertificatePassword "mypassword" -Credential
  "Username"

```

You can also upload IoT Edge certificates to enable a secure connection between your IoT Edge device and the downstream devices that may connect to it. There are three files (`.pem` format) that you need to install:

- Root CA certificate or the owner CA
- Device CA certificate

- Device private key

The following example shows the usage of this cmdlet to install IoT Edge certificates:

```
Set-HcsCertificate -Scope IoTEdge -RootCACertificateFilePath "\\\hcfs\root-ca-cert.pem" -
DeviceCertificateFilePath "\\\hcfs\device-ca-cert.pem\" -DeviceKeyFilePath "\\\hcfs\device-private-key.pem" -
Credential "username"
```

When you run this cmdlet, you will be prompted to provide the password for the network share.

For more information on certificates, go to [Azure IoT Edge certificates](#) or [Install certificates on a gateway](#).

View device information

1. [Connect to the PowerShell interface](#).
2. Use the `Get-HcsApplianceInfo` to get the information for your device.

The following example shows the usage of this cmdlet:

```
[10.100.10.10]: PS>Get-HcsApplianceInfo

Id : b2044bdb-56fd-4561-a90b-407b2a67bdfe
FriendlyName : DBE-NBSVFQR94S6
Name : DBE-NBSVFQR94S6
SerialNumber : HCS-NBSVFQR94S6
DeviceId : 40d7288d-cd28-481d-a1ea-87ba9e71ca6b
Model : Virtual
FriendlySoftwareVersion : Data Box Gateway 1902
HcsVersion : 1.4.771.324
IsClustered : False
IsVirtual : True
LocalCapacityInMb : 1964992
SystemState : Initialized
SystemStatus : Normal
Type : DataBoxGateway
CloudReadRateBytesPerSec : 0
CloudWriteRateBytesPerSec : 0
IsInitialPasswordSet : True
FriendlySoftwareVersionNumber : 1902
UploadPolicy : All
DataDiskResiliencySettingName : Simple
ApplianceTypeFriendlyName : Data Box Gateway
IsRegistered : False
```

Here is a table summarizing some of the important device information:

PARAMETER	DESCRIPTION
FriendlyName	The friendly name of the device as configured through the local web UI during device deployment. The default friendly name is the device serial number.
SerialNumber	The device serial number is a unique number assigned at the factory.
Model	The model for your Azure Stack Edge or Data Box Gateway device. The model is physical for Azure Stack Edge and virtual for Data Box Gateway.

PARAMETER	DESCRIPTION
FriendlySoftwareVersion	The friendly string that corresponds to the device software version. For a system running preview, the friendly software version would be Data Box Edge 1902.
HcsVersion	The HCS software version running on your device. For instance, the HCS software version corresponding to Data Box Edge 1902 is 1.4.771.324.
LocalCapacityInMb	The total local capacity of the device in Megabits.
IsRegistered	This value indicates if your device is activated with the service.

Reset your device

To reset your device, you need to securely wipe out all the data on the data disk and the boot disk of your device.

Use the `Reset-HcsAppliance` cmdlet to wipe out both the data disks and the boot disk or just the data disks. The `SecureWipeBootDisk` and `SecureWipeDataDisks` switches allow you to wipe the boot disk and the data disks respectively.

The `SecureWipeBootDisk` switch wipes the boot disk and makes the device unusable. It should be used only when the device needs to be returned to Microsoft. For more information, see [Return the device to Microsoft](#).

If you use the device reset in the local web UI, only the data disks are securely wiped but the boot disk is kept intact. The boot disk contains the device configuration.

1. [Connect to the PowerShell interface](#).

2. At the command prompt, type:

```
Reset-HcsAppliance -SecureWipeBootDisk -SecureWipeDataDisks
```

The following example shows how to use this cmdlet:

```
[10.128.24.33]: PS>Reset-HcsAppliance -SecureWipeBootDisk -SecureWipeDataDisks

Confirm
Are you sure you want to perform this action?
Performing the operation "Reset-HcsAppliance" on target "ShouldProcess appliance".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): N
```

Get compute logs

If the compute role is configured on your device, you can also get the compute logs via the PowerShell interface.

1. [Connect to the PowerShell interface](#).

2. Use the `Get-AzureDataBoxEdgeComputeRoleLogs` to get the compute logs for your device.

The following example shows the usage of this cmdlet:

```
Get-AzureDataBoxEdgeComputeRoleLogs -Path "\\\hcsfs\logs\myacct" -Credential "username" -
FullLogCollection
```

Here is a description of the parameters used for the cmdlet:

- `Path` : Provide a network path to the share where you want to create the compute log package.
- `Credential` : Provide the username for the network share. When you run this cmdlet, you will need to provide the share password.
- `FullLogCollection` : This parameter ensures that the log package will contain all the compute logs. By default, the log package contains only a subset of logs.

Monitor and troubleshoot compute modules

On an Azure Stack Edge device that has the compute role configured, you can troubleshoot or monitor the device using two different set of commands.

- Using `iotedge` commands. These commands are available for basic operations for your device.
- Using `dkrdbe` commands. These commands are available for an extensive set of operations for your device.

To execute either of the above set of commands, you need to [Connect to the PowerShell interface](#).

Use `iotedge` commands

To see a list of available commands, [connect to the PowerShell interface](#) and use the `iotedge` function.

```
[10.100.10.10]: PS>iotedge -?  
Usage: iotedge COMMAND  
  
Commands:  
  check  
  list  
  logs  
  restart  
  
[10.100.10.10]: PS>
```

The following table has a brief description of the commands available for `iotedge` :

COMMAND	DESCRIPTION
<code>check</code>	Perform automated checks for common configuration and connectivity issues
<code>list</code>	List modules
<code>logs</code>	Fetch the logs of a module
<code>restart</code>	Stop and restart a module

Use `dkrdbe` commands

To see a list of available commands, [connect to the PowerShell interface](#) and use the `dkrdbe` function.

```
[10.100.10.10]: PS>dkrdbe -?
```

```
Usage: dkrdbe COMMAND
```

Commands:

```
image [prune]
images
inspect
login
logout
logs
port
ps
pull
start
stats
stop
system [df]
top
```

```
[10.100.10.10]: PS>
```

The following table has a brief description of the commands available for `dkrdbe`:

COMMAND	DESCRIPTION
<code>image</code>	Manage images. To remove unused images, use: <code>dkrdbe image prune -a -f</code>
<code>images</code>	List images
<code>inspect</code>	Return low-level information on Docker objects
<code>login</code>	Sign in to a Docker registry
<code>logout</code>	Sign out from a Docker registry
<code>logs</code>	Fetch the logs of a container
<code>port</code>	List port mappings or a specific mapping for the container
<code>ps</code>	List containers
<code>pull</code>	Pull an image or a repository from a registry
<code>start</code>	Start one or more stopped containers
<code>stats</code>	Display a live stream of container(s) resource usage statistics
<code>stop</code>	Stop one or more running containers
<code>system</code>	Manage Docker
<code>top</code>	Display the running processes of a container

To get help for any available command, use `dkrdbe <command-name> --help`.

For example, to understand the usage of the `port` command, type:

```
[10.100.10.10]: P> dkrdbe port --help

Usage: dkrdbe port CONTAINER [PRIVATE_PORT[/PROTO]]

List port mappings or a specific mapping for the container
[10.100.10.10]: P> dkrdbe login --help

Usage: docker login [OPTIONS] [SERVER]

Log in to a Docker registry.
If no server is specified, the default is defined by the daemon.

Options:
  -p, --password string    Password
  --password-stdin         Take the password from stdin
  -u, --username string   Username
[10.100.10.10]: PS>
```

The available commands for the `dkrdbe` function use the same parameters as the ones used for the normal docker commands. For the options and parameters used with the docker command, go to [Use the Docker commandline](#).

To check if the module deployed successfully

Compute modules are containers that have a business logic implemented. To check if a compute module is deployed successfully, run the `ps` command and check if the container (corresponding to the compute module) is running.

To get the list of all the containers (including the ones that are paused), run the `ps -a` command.

```
[10.100.10.10]: P> dkrdbe ps -a
CONTAINER ID        IMAGE                               COMMAND                  CREATED             NAMES
STATUS              PORTS
d99e2f91d9a8        edgecompute.azurecr.io/filemovemode... "dotnet FileMoveModu ;"   2 days ago      Up 2 days   movefile
0a06f6d605e9        edgecompute.azurecr.io/filemovemode... "dotnet FileMoveModu ;"   2 days ago      Up 2 days   filermove
2f8a36e629db        mcr.microsoft.com/azureiotedge-hub:1.0 "/bin/sh -c 'echo \"$ ;"  2 days ago      Up 2 days   edgeHub
acce59f70d60        mcr.microsoft.com/azureiotedge-agent:1.0 "/bin/sh -c 'echo \"$ ;"  2 days ago      Up 2 days   edgeAgent
[10.100.10.10]: PS>
```

If there was an error in creation of the container image or while pulling the image, run `logs edgeAgent`.

`EdgeAgent` is the IoT Edge runtime container that is responsible for provisioning other containers.

Because `logs edgeAgent` dumps all the logs, a good way to see the recent errors is to use the option `--tail 20`.

```
[10.100.10.10]: PS>dkrdbe logs edgeAgent --tail 20
2019-02-28 23:38:23.464 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Util.Uds.HttpUdsMessageHandler] -
Connected socket /var/run/iotedge/mgmt.sock
2019-02-28 23:38:23.464 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Util.Uds.HttpUdsMessageHandler] - Sending
request http://mgmt.sock/modules?api-version=2018-06-28
2019-02-28 23:38:23.464 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Agent.Core.Agent] - Getting edge agent
config...
2019-02-28 23:38:23.464 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Agent.Core.Agent] - Obtained edge agent
config
2019-02-28 23:38:23.469 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Agent.Edgelet.ModuleManagementHttpClient]
- Received a valid Http response from unix:///var/run/iotedge/mgmt.sock
k for List modules
-----CUT-----
-----CUT-----
08:28.1007774+00:00", "restartCount":0, "lastRestartTimeUtc":"2019-02-
26T20:08:28.1007774+00:00", "runTimeStatus":"running", "version":"1.0", "status":"running", "restartPolicy":"alw
ays
", "type":"docker", "settings": {"image": "edgecompute.azurecr.io/filemovemode2:0.0.1-
amd64", "imageHash": "sha256:47778bbe0602fb077d7bc2aaae9b0760fbfc7c058bf4df192f207ad6cbb96f7cc", "c
reateOptions": {"HostConfig": {"Binds": ["\\home\hcsshares\share4-
d1460:\\home\input\\", "\\home\hcsshares\share4-iot:\\home\output\\"]}, "env": {}}}
2019-02-28 23:38:28.480 +00:00 [DBG] [Microsoft.Azure.Devices.Edge.Agent.Core.Planners.HealthRestartPlanner]
- HealthRestartPlanner created Plan, with 0 command(s).
```

To get container logs

To get logs for a specific container, first list the container and then get the logs for the container that you're interested in.

1. Connect to the PowerShell interface.
2. To get the list of running containers, run the `ps` command.

CONTAINER ID	IMAGE	COMMAND
CREATED	STATUS	POR
NAMES		
d99e2f91d9a8	edgecompute.azurecr.io/filemovemode2:0.0.1-amd64	"dotnet FileMoveModu�;"
2 days ago	Up 2 days	
movefile		
0a06f6d605e9	edgecompute.azurecr.io/filemovemode2:0.0.1-amd64	"dotnet FileMoveModu�;"
2 days ago	Up 2 days	
filmove		
2f8a36e629db	mcr.microsoft.com/azureiotedge-hub:1.0	"/bin/sh -c 'echo \"\$�;"
2 days ago	Up 2 days	0.0.0.0:443->443/tcp, 0.0.0.0:5671->5671/tcp, 0.0.0.0:8883- >8883/tcp
edgeHub		
acce59f70d60	mcr.microsoft.com/azureiotedge-agent:1.0	"/bin/sh -c 'echo \"\$�;"
2 days ago	Up 2 days	
edgeAgent		

3. Make a note of the container ID for the container that you need the logs for.
4. To get the logs for a specific container, run the `logs` command providing the container ID.

```
[10.100.10.10]: PS>dkrdbe logs d99e2f91d9a8
02/26/2019 18:21:45: Info: Opening module client connection.
02/26/2019 18:21:46: Info: Initializing with input: /home/input, output: /home/output.
02/26/2019 18:21:46: Info: IoT Hub module client initialized.
02/26/2019 18:22:24: Info: Received message: 1, SequenceNumber: 0 CorrelationId: , MessageId: 081886a07e694c4c8f245a80b96a252a Body: [{"ChangeType": "Created", "ShareRelativeFilePath": "\_\_Microsoft Data Box Edge\_\_Upload\Errors.xml", "ShareName": "share4-d1460"}]
02/26/2019 18:22:24: Info: Moving input file: /home/input/\_\_Microsoft Data Box Edge\_\_Upload/Errors.xml to /home/output/\_\_Microsoft Data Box Edge\_\_Upload/Errors.xml
02/26/2019 18:22:24: Info: Processed event.
02/26/2019 18:23:38: Info: Received message: 2, SequenceNumber: 0 CorrelationId: , MessageId: 30714d005eb048e7a4e7e3c22048cf20 Body: [{"ChangeType": "Created", "ShareRelativeFilePath": "\f [10]", "ShareName": "share4-d1460"}]
02/26/2019 18:23:38: Info: Moving input file: /home/input/f [10] to /home/output/f [10]
02/26/2019 18:23:38: Info: Processed event.
```

To monitor the usage statistics of the device

To monitor the memory, CPU usage, and IO on the device, use the `stats` command.

1. Connect to the PowerShell interface.
2. Run the `stats` command so as to disable the live stream and pull only the first result.

```
dkrdbe stats --no-stream
```

The following example shows the usage of this cmdlet:

```
[10.100.10.10]: P> dkrdbe stats --no-stream
CONTAINER ID      NAME          CPU %     MEM USAGE / LIMIT      MEM %      NET I/O
BLOCK I/O          PIDS
d99e2f91d9a8      movefile      0.0       24.4MiB / 62.89GiB    0.04%      751kB / 497kB
299kB / 0B          14           0.00%    24.11MiB / 62.89GiB   0.04%      679kB / 481kB
0a06f6d605e9      filermove     0.18%    173.8MiB / 62.89GiB   0.27%      4.58MB / 5.49MB
49.5MB / 0B          14           0.00%    35.55MiB / 62.89GiB   0.06%      2.23MB / 2.31MB
2f8a36e629db      edgeHub       0.00%    25.7MB / 2.19MB        0.00%      0.00MB / 0.00MB
55.7MB / 332kB      241          0.00%    25.7MB / 2.19MB        0.00%      0.00MB / 0.00MB
[10.100.10.10]: PS>
```

Exit the remote session

To exit the remote PowerShell session, close the PowerShell window.

Next steps

- Deploy [Azure Stack Edge Pro FPGA](#) in Azure portal.

Troubleshoot your Azure Stack Edge Pro FPGA issues

9/21/2022 • 4 minutes to read • [Edit Online](#)

This article describes how to troubleshoot issues on your Azure Stack Edge Pro FPGA.

In this article, you learn how to:

- Run diagnostics
- Collect Support package
- Use logs to troubleshoot
- Troubleshoot IoT Edge errors

Run diagnostics

To diagnose and troubleshoot any device errors, you can run the diagnostics tests. Do the following steps in the local web UI of your device to run diagnostic tests.

1. In the local web UI, go to **Troubleshooting > Diagnostic tests**. Select the test you want to run and select **Run test**. This runs the tests to diagnose any possible issues with your network, device, web proxy, time, or cloud settings. You're notified that the device is running tests.

The screenshot shows the Azure Stack Edge local web interface. On the left, there's a navigation sidebar with sections: Configuration (Device name, Network settings, Web proxy settings, Time settings, Cloud settings, Compute settings), Maintenance (Power settings, Hardware status, Software update, Password change, Device reset), and Troubleshooting (Diagnostic tests, Support). The 'Diagnostic tests' link is highlighted with a red box. The main content area has a title 'Diagnostic tests' with a subtitle 'MyAzureStackEdge1'. It contains a sub-instruction 'Run diagnostic tests to troubleshoot issues.' Below this is a table with columns: TEST, CATEGORY, STATUS, and RECOMMENDED ACTIONS. The table lists 17 items, all of which are checked and marked as 'Healthy'. At the bottom of the table is a large red 'Run test' button.

TEST	CATEGORY	STATUS	RECOMMENDED ACTIONS
Azure portal connectivity	Azure connectivity	Healthy	-
Azure storage account credentials	Azure connectivity	-	-
Azure container read/write	Azure connectivity	-	-
Azure Edge compute runtime	Edge compute	-	-
Disks	Hardware	Healthy	-
Network interfaces	Hardware	Healthy	-
CPUs	Hardware	Healthy	-
Network settings	Networking	Healthy	-
Name resolution	Networking	Healthy	-
Internet connectivity	Networking	Healthy	-
System software	Software	Healthy	-
Time sync	Time	Healthy	-
Software update settings	Update	Healthy	-

2. After the tests have completed, the results are displayed.

TEST	CATEGORY	STATUS	RECOMMENDED ACTIONS
Azure portal connectivity	Azure connectivity	Healthy	-
Azure storage account credentials	Azure connectivity	Healthy	-
Azure container read/write	Azure connectivity	Healthy	-
Azure Edge compute runtime	Edge compute	Healthy	-
Disks	Hardware	Healthy	-
Network interfaces	Hardware	Warning	1 recommended action(s)
CPUs	Hardware	Healthy	-
Network settings	Networking	Healthy	-
Name resolution	Networking	Healthy	-
Internet connectivity	Networking	Healthy	-
System software	Software	Healthy	-
Time sync	Time	Healthy	-
Software update settings	Update	Healthy	-

If a test fails, then a URL for recommended action is presented. Select the URL to view the recommended action.

Recommended actions

To resolve the issue(s), complete the following:

- RDMA performance is slower than expected. Examine your network adapters.

OK

Collect Support package

A log package is composed of all the relevant logs that can help Microsoft Support troubleshoot any device issues. You can generate a log package via the local web UI.

Do the following steps to collect a Support package.

- In the local web UI, go to **Troubleshooting > Support**. Select **Create support package**. The system starts collecting support package. The package collection may take several minutes.

The screenshot shows the Azure Stack Edge portal interface. On the left, there is a navigation sidebar with the following sections and items:

- CONFIGURATION**: Device name, Network settings, Web proxy settings, Time settings, Cloud settings.
- MAINTENANCE**: Power settings, Hardware status, Software update, Password change, Device reset.
- TROUBLESHOOTING**: Diagnostic tests, Support.

The "Support" item under Troubleshooting is highlighted with a red box. The main content area is titled "Support" and shows the device name "MyAzureStackEdge1". It contains two sections: "Contact" and "Support package".

Contact: If you are experiencing issues with your device, file a service request with Microsoft Support. A link "Contact Microsoft Support" is provided.

Support package: Create and download a package of all the system logs if you are experiencing any issues with your device. A blue button "Create Support package" is visible, and another one "Download Support package" is highlighted with a red box.

- After the Support package is created, select **Download Support package**. A zipped package is downloaded on the path you chose. You can unzip the package and view the system log files.

This screenshot shows the same portal interface as the previous one, but it includes a download history at the bottom. The "Support" item in the sidebar is highlighted with a red box.

The main content area shows the "Support package" section with the following details:

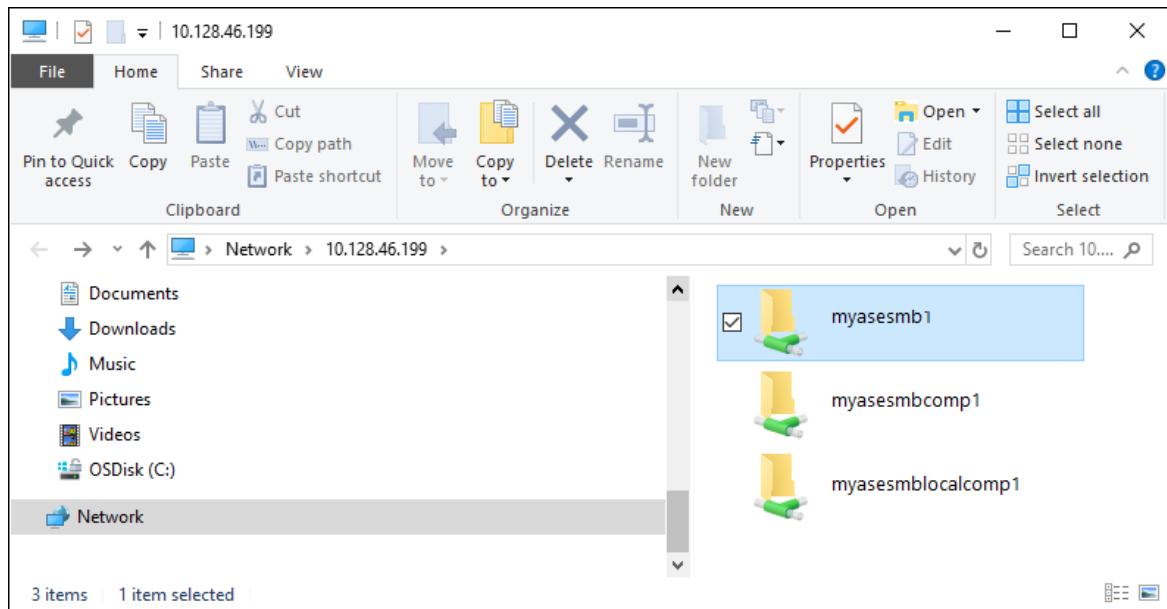
- Create and download a package of all the system logs if you are experiencing any issues with your device.
- Support package last created on: 4/7/2020 9:20:22 AM
- A blue button "Create Support package" and a red-highlighted blue button "Download Support package" are present.

At the bottom, a download history entry is shown: "SupportPackage.zip" with a download icon, followed by a red box. To the right, there are "Show all" and "X" buttons.

Use logs to troubleshoot

Any errors experienced during the upload and refresh processes are included in the respective error files.

- To view the error files, go to your share and select it to view the contents.



2. Select the *Microsoft Azure Stack Edge folder*. This folder has two subfolders:

- Upload folder that has log files for upload errors.
- Refresh folder for errors during refresh.

Here is a sample log file for refresh.

```
<root container="test1" machine="VM15BS020663" timestamp="03/18/2019 00:11:10" />
<file item="test.txt" local="False" remote="True" error="16001" />
<summary runtime="00:00:00.0945320" errors="1" creates="2" deletes="0" insync="3" replaces="0"
pending="9" />
```

3. When you see an error in this file (highlighted in the sample), note down the error code, in this case it's 16001. Look up the description of this error code against the following error reference.

ERROR CODE	ERROR DESCRIPTION
100	The container or share name must be between 3 and 63 characters.
101	The container or share name must consist of only letters, numbers, or hyphens.
102	The container or share name must consist of only letters, numbers, or hyphens.
103	The blob or file name contains unsupported control characters.
104	The blob or file name contains illegal characters.
105	Blob or file name contains too many segments (each segment is separated by a slash -/).
106	The blob or file name is too long.
107	One of the segments in the blob or file name is too long.

ERROR CODE	ERROR DESCRIPTION
108	The file size exceeds the maximum file size for upload.
109	The blob or file is incorrectly aligned.
110	The Unicode encoded file name or blob is not valid.
111	The name or the prefix of the file or blob is a reserved name that isn't supported (for example, COM1).
2000	An etag mismatch indicates that there is a conflict between a block blob in the cloud and on the device. To resolve this conflict, delete one of those files – either the version in the cloud or the version on the device.
2001	An unexpected problem occurred while processing a file after the file was uploaded. If you see this error, and the error persists for more than 24 hours, contact support.
2002	The file is already open in another process and can't be uploaded until the handle is closed.
2003	Couldn't open the file for upload. If you see this error, contact Microsoft Support.
2004	Couldn't connect to the container to upload data to it.
2005	Couldn't connect to the container because the account permissions are either wrong or out of date. Check your access.
2006	Couldn't upload data to the account as the account or share is disabled.
2007	Couldn't connect to the container because the account permissions are either wrong or out of date. Check your access.
2008	Couldn't add new data as the container is full. Check the Azure specifications for supported container sizes based on type. For example, Azure File only supports a maximum file size of 5 TB.
2009	Couldn't upload data because the container associated with the share doesn't exist.
2997	An unexpected error occurred. This is a transient error that will resolve itself.
2998	An unexpected error occurred. The error may resolve itself but if it persists for more than 24 hours, contact Microsoft Support.
16000	Couldn't bring down this file.

ERROR CODE	ERROR DESCRIPTION
16001	Couldn't bring down this file since it already exists on your local system.
16002	Couldn't refresh this file since it isn't fully uploaded.

Troubleshoot IoT Edge errors

Use the IoT Edge agent runtime responses to troubleshoot compute-related errors. Here is a list of possible responses:

- 200 - OK
- 400 - The deployment configuration is malformed or invalid.
- 417 - The device doesn't have a deployment configuration set.
- 412 - The schema version in the deployment configuration is invalid.
- 406 - The IoT Edge device is offline or not sending status reports.
- 500 - An error occurred in the IoT Edge runtime.

For more information, see [IoT Edge Agent](#).

Next steps

- Learn more about the [known issues in this release](#).

Troubleshoot your Azure Stack Edge ordering issues

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro 2 ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R

This article describes how to troubleshoot Azure Stack Edge ordering issues.

Unsupported subscription or region

Error Description: In Azure portal, if you get the error:

Selected subscription or region is not supported. Choose a different subscription or region.

The screenshot shows a form with two dropdown menus. The first dropdown is labeled "1. Select a subscription * ⓘ" and contains "Azure subscription 1". The second dropdown is labeled "2. Select ship to country * ⓘ" and contains "In your hypervisor". Below the dropdowns, a red box highlights the error message: "Selected subscription or region is not supported. Choose a different subscription or region."

Suggested solution: Make sure that you used a supported subscription such as [Microsoft Enterprise Agreement \(EA\)](#), [Cloud Solution Provider \(CSP\)](#), or [Microsoft Azure Sponsorship](#). Pay-as-you-go subscriptions aren't supported. For more information, see [Azure Stack Edge resource prerequisites](#).

There's the possibility that Microsoft may allow a subscription type upgrade on a case-by-case basis. Contact [Microsoft support](#) so that they can understand your needs and adjust these limits appropriately.

Selected subscription type not supported

Error: You have an EA, CSP, or sponsored subscription and you get the following error:

*The selected subscription type is not supported. Make sure that you use a supported subscription. [Learn more](#). If using a supported subscription type, make sure:

- That the `Microsoft.DataBoxEdge` provider is registered, when placing orders via the classic portal.
- That the `Microsoft.EdgeOrder` provider is registered, when placing orders via the Azure Edge Hardware Center (Preview).

For information on how to register, see [Register resource provider*](#).

Suggested solution: Follow these steps to register your Azure Stack Edge resource provider:

1. In Azure portal, go to **Home > Subscriptions**.
2. Select the subscription that you'll use to order your device.
3. Select **Resource providers** and then search for **Microsoft.DataBoxEdge**.

Provider	Status
microsoft.batch	Registered
Microsoft.Cdn	Registered
Microsoft.ClassicCompute	Registered
Microsoft.ClassicNetwork	Registered
Microsoft.ClassicStorage	Registered
Microsoft.ClassicInfrastructureMigrate	Registered
Microsoft.CognitiveServices	Registered
Microsoft.Commerce	Registered
Microsoft.HybridData	Registered
Microsoft.DataBox	Registered
Microsoft.DataBoxEdge	Registered
Microsoft.Databricks	Registered
Microsoft.Devices	Registered
Microsoft.DocumentDB	Registered

If you don't have owner or contributor access to register the resource provider, you see the following error: *The subscription <subscription name> doesn't have permissions to register the resource provider(s): Microsoft.DataBoxEdge.*

For more information, see [Register resource providers](#).

Resource provider not registered for subscription

Error: In Azure portal, you select a subscription to use for Azure Stack Edge or Data Box Gateway and get one of the following error:

Resource provider(s): Microsoft.DataBoxEdge are not registered for subscription <subscription name> and you don't have permissions to register a resource provider for subscription <subscription name>.

Resource provider(s): Microsoft.EdgeOrder are not registered for subscription <subscription name> and you don't have permissions to register a resource provider for subscription <subscription name>.

Suggested solution: Elevate your subscription access or find someone with owner or contributor access to register the resource provider.

Resource disallowed by policy

Error: In Azure portal, you attempt to register a resource provider and get the following error:

Resource <resource name> was disallowed by policy. (Code: RequestDisallowedByPolicy). Initiative: Deny generally unwanted Resource Types. Policy: Not allowed resource types.

Suggested solution: This error occurs due to an existing Azure Policy assignment that blocks the resource creation. Azure Policy definitions and assignments are set by an organization's system administrator to ensure compliance while using or creating Azure resources. If any such policy assignment is blocking Azure Stack Edge resource creation, contact your system administrator to edit your Azure Policy definition.

Next steps

- Learn more about how to [Troubleshoot your Azure Stack Edge issues](#).

Troubleshoot IoT Edge issues on your Azure Stack Edge FPGA device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to troubleshoot compute-related errors on an Azure Stack Edge FPGA device by reviewing IoT Edge agent runtime responses.

IoT Edge runtime responses

Use the IoT Edge agent runtime responses to troubleshoot compute-related errors. Here is a list of possible responses:

- 200 - OK
- 400 - The deployment configuration is malformed or invalid.
- 417 - The device doesn't have a deployment configuration set.
- 412 - The schema version in the deployment configuration is invalid.
- 406 - The IoT Edge device is offline or not sending status reports.
- 500 - An error occurred in the IoT Edge runtime.

For more information, see [IoT Edge Agent](#).

Next steps

- [Debug Kubernetes issues related to IoT Edge](#).
- [Troubleshoot device issues](#).

Open a support ticket for Azure Stack Edge and Azure Data Box Gateway

9/21/2022 • 3 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro R Azure Stack Edge Mini R Azure Stack Edge FPGA Azure Data Box Gateway

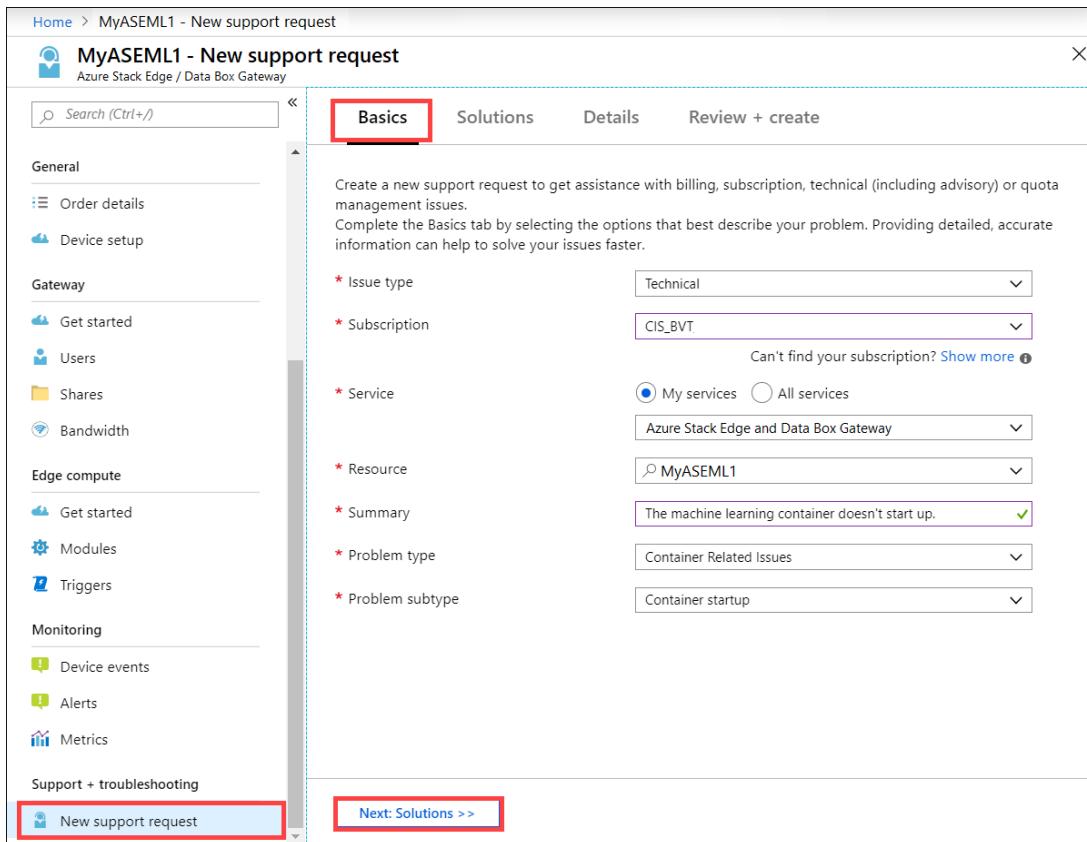
This article applies to Azure Stack Edge and Azure Data Box Gateway both of which are managed by the Azure Stack Edge / Azure Data Box Gateway service. If you encounter any issues with your service, you can create a service request for technical support. This article walks you through:

- How to create a support request.
- How to manage a support request lifecycle from within the portal.

Create a support request

Do the following steps to create a support request:

1. Go to your Azure Stack Edge or Data Box Gateway order. Navigate to **Support + troubleshooting** section and then select **New support request**.
2. In **New support request**, on the **Basics** tab, take the following steps:
 - a. From the **Issue type** dropdown list, select **Technical**.
 - b. Choose your **Subscription**.
 - c. Under **Service**, check **My Services**. From the dropdown list, select **Azure Stack Edge and Data Box Gateway**.
 - d. Select your **Resource**. This corresponds to the name of your order.
 - e. Give a brief **Summary** of the issue you are experiencing.
 - f. Select your **Problem type**.
 - g. Based on the problem type you selected, choose a corresponding **Problem subtype**.
 - h. Select **Next: Solutions >>**.



3. On the **Details** tab, take the following steps:

- a. Provide the start date and time for the problem.
- b. Supply a **Description** for your problem.
- c. In the **File upload**, select the folder icon to browse any other files you want to upload.
- d. Check **Share diagnostic information**.
- e. Based on your subscription, a **Support plan** is automatically populated.
- f. From the dropdown list, select the **Severity**.
- g. Specify a **Preferred contact method**.
- h. The **Response hours** are automatically selected based on your subscription plan.
- i. Provide the language you prefer for Support.
- j. In the **Contact information**, provide your name, email, phone, optional contact, country/region. Microsoft Support uses this information to reach out to you for further information, diagnosis, and resolution.
- k. Select **Next: Review + Create >>**.

Home > MyASEML1 - New support request

MyASEML1 - New support request

Azure Stack Edge / Data Box Gateway

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Properties

General

Order details

Device setup

Gateway

Get started

Users

Shares

Bandwidth

Edge compute

Get started

Modules

Triggers

Monitoring

Device events

Alerts

Metrics

Support + troubleshooting

New support request

Basics Solutions Details Review + create

PROBLEM DETAILS

When did the problem start? 2019-07-10 12:00 AM

* Description
The machine learning container that I deployed on Azure Stack Edge does not start up.

File upload Choose file to upload

Consent Share diagnostic information

SUPPORT METHOD

Support plan Azure Support Plan - Internal

* Severity B - Moderate impact

* Preferred contact method

Contact me later Email

Call me later Phone

* Response hours Business Hours

* Support language English

CONTACT INFO Edit

Contact name John Contoso

Email john@contoso.com

Additional email for notification --

<< Previous: Basics Next: Review + create >>

The screenshot shows the 'New support request' interface in the Azure Stack Edge portal. The 'Details' tab is active. In the 'PROBLEM DETAILS' section, the 'Description' field contains a note about a machine learning container not starting. The 'SUPPORT METHOD' section shows the support plan as 'Azure Support Plan - Internal' and the severity as 'B - Moderate impact'. Under 'Preferred contact method', both 'Contact me later' (Email) and 'Call me later' (Phone) are listed. The 'CONTACT INFO' section shows the contact name as 'John Contoso' and the email as 'john@contoso.com'. Navigation buttons at the bottom allow switching between 'Basics' and 'Review + create'.

4. On the **Review + Create** tab, review the information related to Support ticket. Select **Create**.

Home > MyASEML1 - New support request

MyASEML1 - New support request

Azure Stack Edge / Data Box Gateway

Search (Ctrl+I)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Properties

General

Order details

Device setup

Gateway

Get started

Users

Shares

Bandwidth

Edge compute

Get started

Modules

Triggers

Monitoring

Device events

Alerts

Metrics

Support + troubleshooting

New support request

Basics Solutions Details Review + create

BASICS

Issue type	Technical
Subscription	CIS_BVT
Service	Azure Stack Edge and Data Box Gateway
Resource	MyASEML1
Problem type	Container Related Issues
Problem subtype	Container startup
Summary	The machine learning container doesn't start up.

TERMS, CONDITIONS AND PRIVACY POLICY

By clicking "Create" you accept the [terms and conditions](#).

View our [privacy policy](#).

DETAILS

When did the problem start?	Wed, Jul 10, 2019, 12:00 AM PDT
Description	The machine learning container that I deployed on Azure Stack Edge does not start up.
Consent	Share diagnostic information

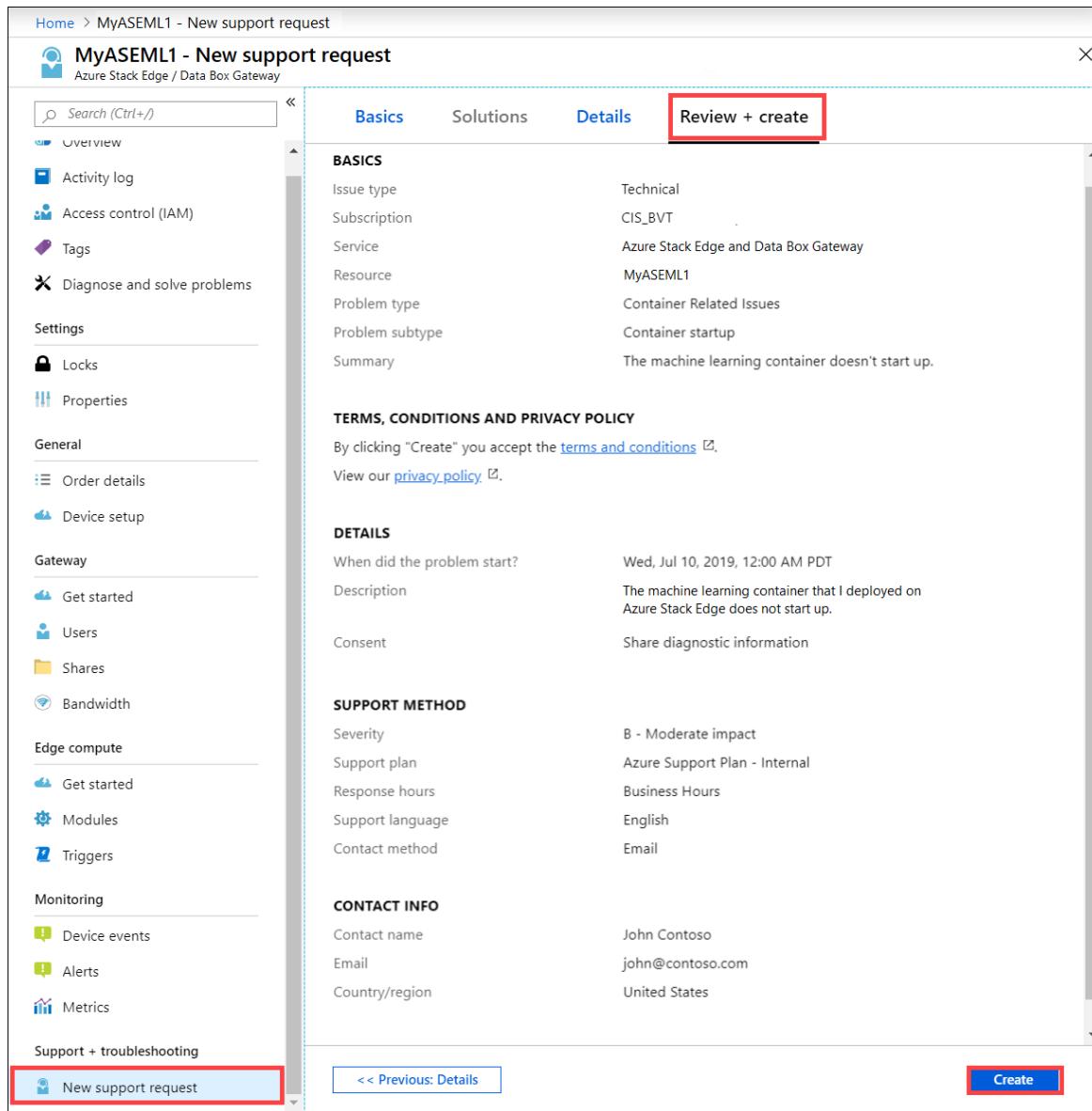
SUPPORT METHOD

Severity	B - Moderate impact
Support plan	Azure Support Plan - Internal
Response hours	Business Hours
Support language	English
Contact method	Email

CONTACT INFO

Contact name	John Contoso
Email	john@contoso.com
Country/region	United States

<< Previous: Details Create



After you create the Support ticket, a Support engineer will contact you as soon as possible to proceed with your request.

Get hardware support

This information only applies to Azure Stack device. The process to report hardware issues is as follows:

1. Open a Support ticket from the Azure portal for a hardware issue. Under **Problem type**, select **Azure Stack Hardware**. Choose the **Problem subtype** as **Hardware failure**.

The screenshot shows the 'MyASEML1 - New support request' page in the Azure Stack Edge / Data Box Gateway portal. The left sidebar includes sections for Gateway (Get started, Users, Shares, Bandwidth), Edge compute (Get started, Modules, Triggers), Monitoring (Device events, Alerts, Metrics), and Support + troubleshooting (New support request). The main area has tabs for Basics, Solutions, Details, and Review + create. The Basics tab is active. It contains fields for Issue type (Technical), Subscription (CIS_BVT.), Service (My services selected, Azure Stack Edge and Data Box Gateway), Resource (MyASEML1), Summary (My power supply unit LED indicates that there is a problem...), Problem type (Azure Stack Edge Hardware selected), and Problem subtype (Hardware failure selected). A red box highlights the Problem type and Problem subtype fields.

After you have created the Support ticket, a Support engineer will contact you as soon as possible to proceed with your request.

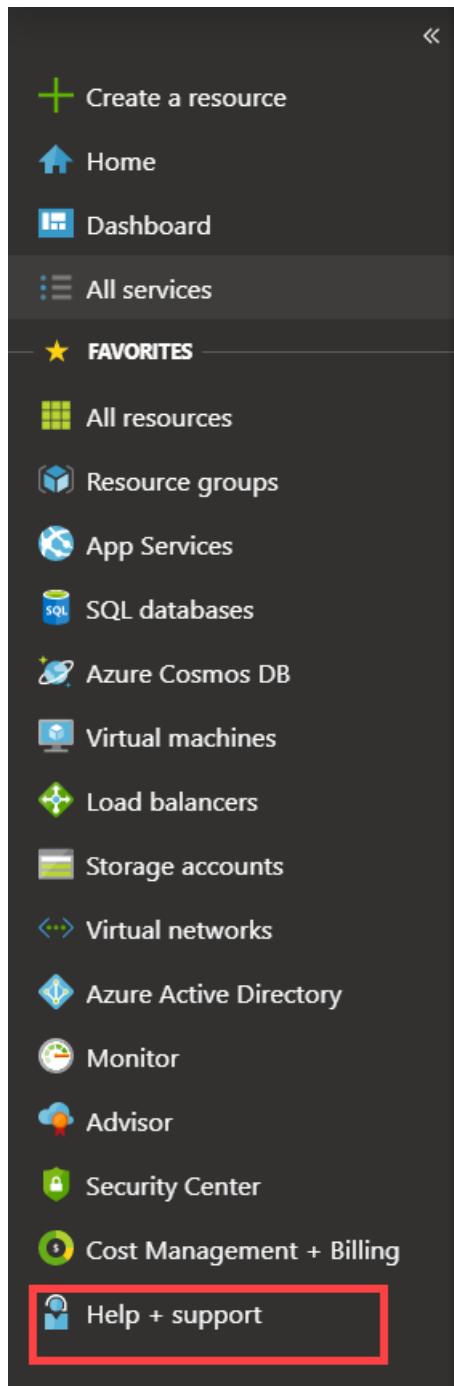
2. If Microsoft Support determines that this is a hardware issue, then one of the following actions occurs:
 - A Field Replacement Unit (FRU) for the failed hardware part is sent. Currently, power supply units and solid-state drives are the only supported FRUs.
 - Only FRUs are replaced within the next business day, everything else requires a full system replacement (FSR) to be shipped.
3. If it is determined that a FRU replacement is needed by 1 PM local time (Monday to Friday), an onsite technician is dispatched the next business day to your location to perform a FRU replacement. A full system replacement typically will take much longer because the parts are shipped from our factory and could be subject to transportation and customs delays.

Manage a support request

After creating a support ticket, you can manage the lifecycle of the ticket from within the portal.

To manage your support requests

1. To get to the help and support page, navigate to **Browse > Help + support**.



2. A tabular listing of **Recent support requests** is displayed in **Help + support**.
3. Select and click a support request. You can view the status and the details for this request. Click **+ New message** if you want to follow up on this request.

Next steps

- [Troubleshoot issues related to Azure Stack Edge FPGA](#).
- [Troubleshoot device issues for Azure Stack Edge Pro GPU](#).
- [Troubleshoot issues related to Data Box Gateway](#).

Monitor your Azure Stack Edge device

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R ✓ Azure Stack Edge Pro - FPGA

This article describes how to monitor your Azure Stack Edge device. To monitor your device, you can use the Azure portal or the local web UI. Use the Azure portal to view metrics, view device events, and configure and manage alerts. Use the local web UI on your physical device to view the hardware status of the various device components.

In this article, you learn how to:

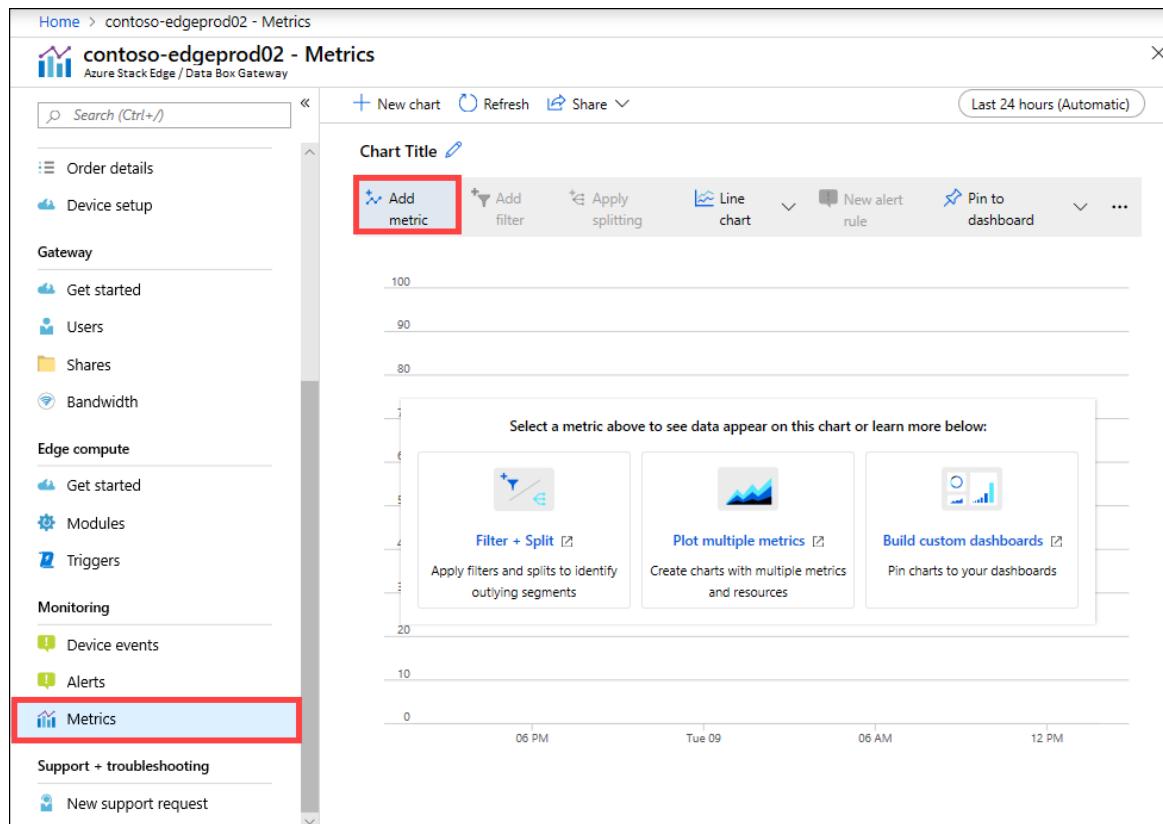
- View capacity and transaction metrics for your device
- View hardware status of device components

View metrics

You can also view the metrics to monitor the performance of the device and in some instances for troubleshooting device issues.

Take the following steps in the Azure portal to create a chart for selected device metrics.

1. For your resource in the Azure portal, go to **Monitoring > Metrics** and select **Add metric**.



The screenshot shows the Azure portal Metrics blade for the resource 'contoso-edgeprod02'. The left sidebar contains navigation links for Order details, Device setup, Gateway (Get started, Users, Shares, Bandwidth), Edge compute (Get started, Modules, Triggers), Monitoring (Device events, Alerts), and Support + troubleshooting (New support request). The main area displays a line chart for the last 24 hours. At the top right, there are buttons for 'New chart', 'Refresh', 'Share', and a time range selector set to 'Last 24 hours (Automatic)'. Below the chart, there's a 'Chart Title' input field and a 'Line chart' selection. A 'Select a metric above to see data appear on this chart or learn more below:' section is present, showing three options: 'Filter + Split' (Apply filters and splits to identify outlying segments), 'Plot multiple metrics' (Create charts with multiple metrics and resources), and 'Build custom dashboards' (Pin charts to your dashboards). The chart itself has a y-axis from 0 to 100 and an x-axis from 06 PM to 12 PM, with a single data series plotted.

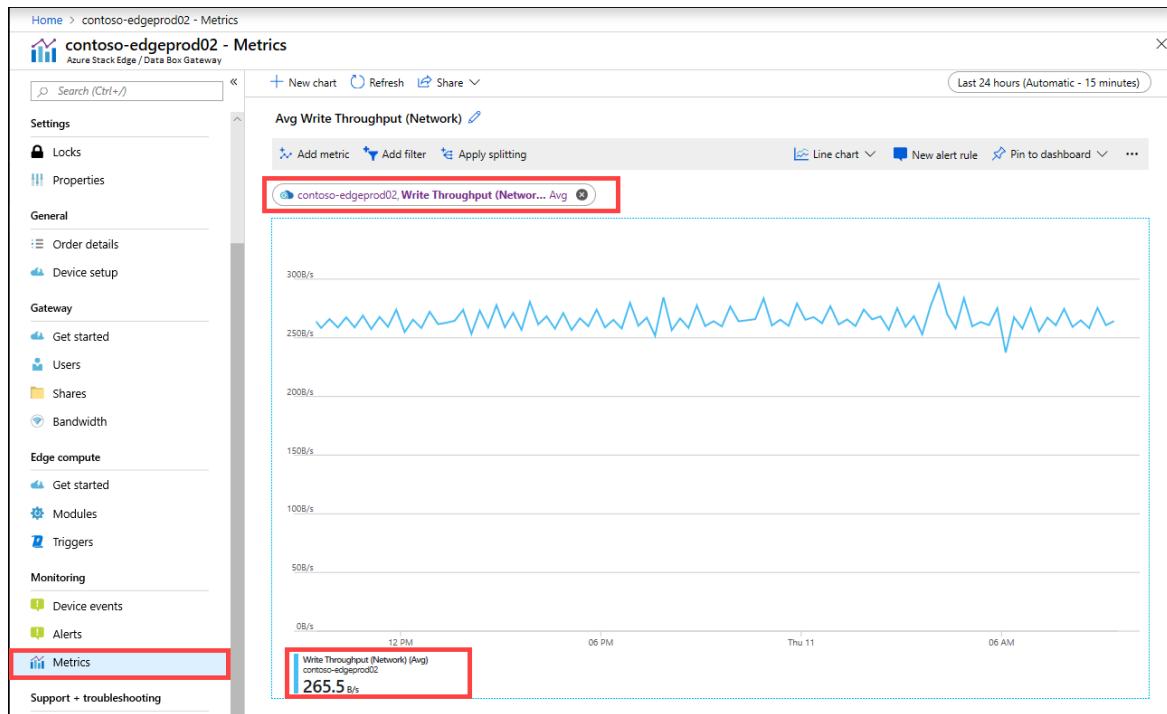
2. The resource is automatically populated.

The screenshot shows the 'contoso-edgeprod02 - Metrics' blade. On the left, a navigation menu includes 'Metrics' (which is highlighted with a red box). In the main area, there's a search bar and a chart title section. Below that is a row of filters: 'Add metric', 'Add filter', 'Apply splitting', 'Line chart' (selected), 'New alert rule', 'Pin to dashboard', and '...'. A red box highlights the 'RESOURCE' dropdown, which is set to 'contoso-edgeprod02'. To the right of it are 'METRIC NAMESPACE' (set to 'Standard metrics'), 'METRIC' (set to 'Select metric'), and 'AGGREGATION' (set to 'Select aggregation'). Below these controls is a line chart showing data from 10 to 100. At the bottom of the chart area, there are three cards: 'Filter + Split', 'Plot multiple metrics', and 'Build custom dashboards'. The 'Metrics' link in the left sidebar is also highlighted with a red box.

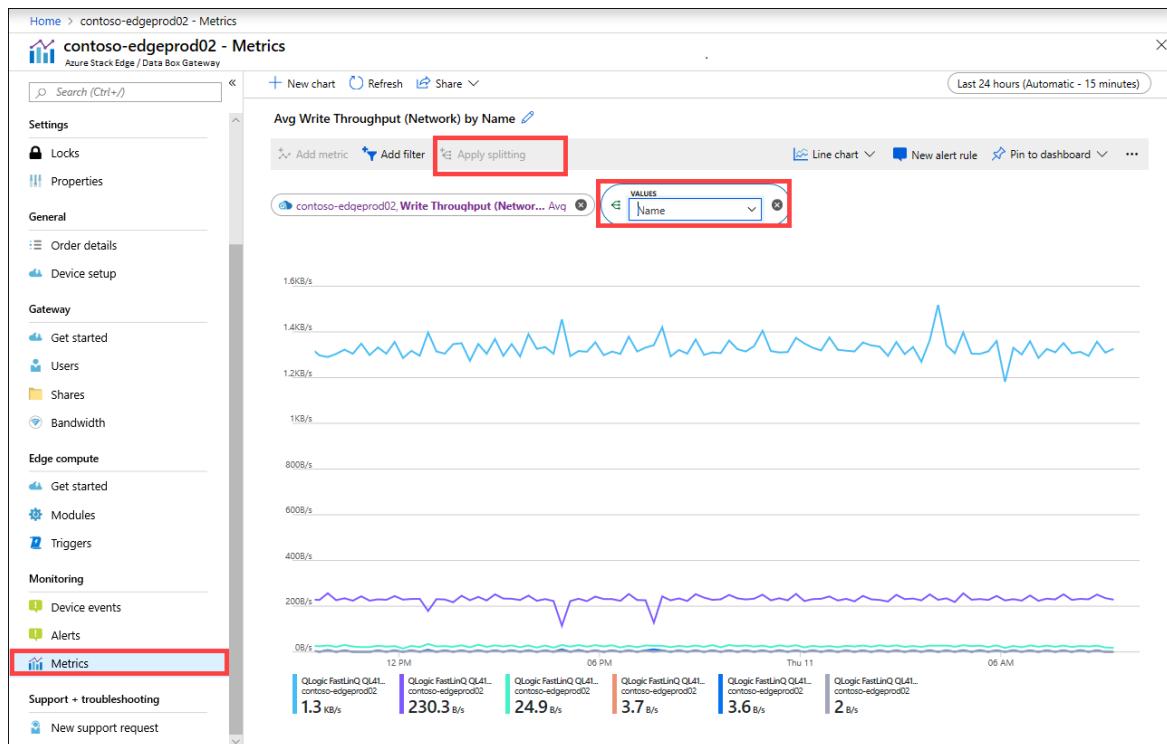
To specify another resource, select the resource. On **Select a resource** blade, select the subscription, resource group, resource type, and the specific resource for which you want to show the metrics and select **Apply**.

The screenshot shows the 'Select a resource' blade. It has tabs for 'Browse' and 'Recent'. Under 'Subscriptions', it says 'All 16 selected – Don't see a subscription? Open Directory + Subscription settings'. It shows dropdowns for 'Subscription' (set to 'All subscriptions'), 'Resource group' (set to '2 resource groups'), and 'Resource type' (set to 'Azure Stack Edge / Data Box Gateway'). A red box highlights the 'RESOURCE' dropdown in the main metrics blade. In the 'Select a resource' blade, a red box highlights the 'Subscription' dropdown set to 'All subscriptions'. Below it, a table lists resources: contoso-edgeprod01 (ContosoRG), contoso-edgeprod02 (ContosoRG), contoso-edgeprod03 (ContosoRG), contoso-gw-prod01 (ContosoRG), and Test-edgeContoso-2 (ContosoRG). The 'contoso-edgeprod01' row is highlighted with a red box. At the bottom are 'Apply' and 'Cancel' buttons, with 'Apply' being highlighted with a red box.

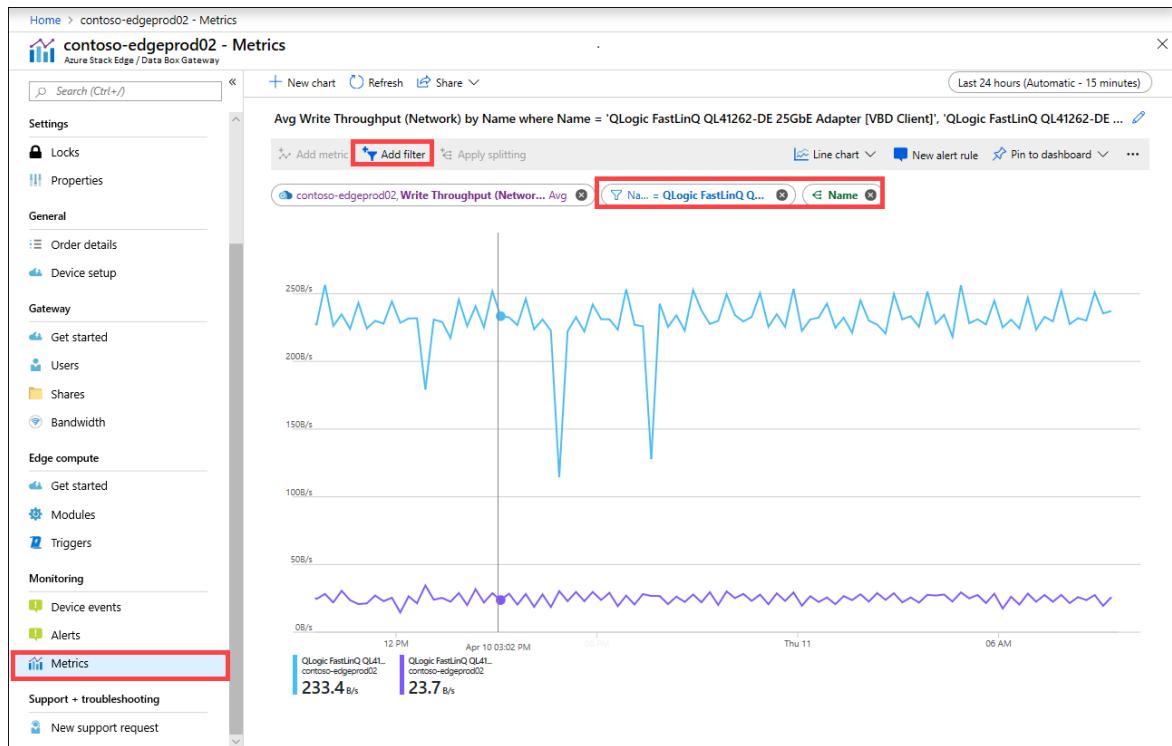
3. From the dropdown list, select a metric to monitor your device. For a full list of these metrics, see [Metrics on your device](#).
4. When a metric is selected from the dropdown list, aggregation can also be defined. Aggregation refers to the actual value aggregated over a specified span of time. The aggregated values can be average, minimum, or the maximum value. Select the Aggregation from Avg, Max, or Min.



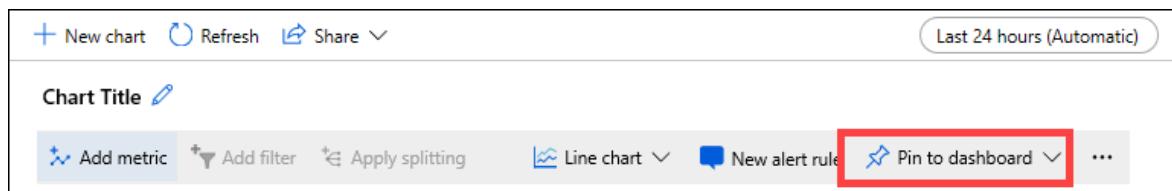
- If the metric you selected has multiple instances, then the splitting option is available. Select **Apply splitting** and then select the value by which you want to see the breakdown.



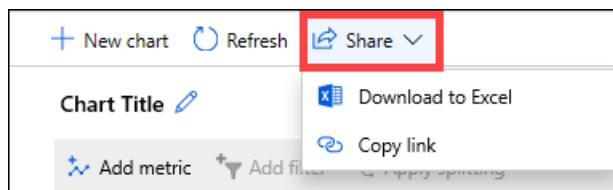
- If you now want to see the breakdown only for a few instances, you can filter the data. For example, in this case, if you want to see the network throughput only for the two connected network interfaces on your device, you could filter those interfaces. Select **Add filter** and specify the network interface name for filtering.



7. You could also pin the chart to dashboard for easy access.



8. To export chart data to an Excel spreadsheet or get a link to the chart that you can share, select the share option from the command bar.



Metrics on your device

This section describes the monitoring metrics on your device. The metrics can be:

- Capacity metrics. The capacity metrics are related to the capacity of the device.
- Transaction metrics. The transaction metrics are related to the read and write operations to Azure Storage.
- Edge compute metrics. The Edge compute metrics are related to the usage of the Edge compute on your device.

A full list of the metrics is shown in the following table:

CAPACITY METRICS	DESCRIPTION
------------------	-------------

CAPACITY METRICS	DESCRIPTION
Available capacity	<p>Refers to the size of the data that can be written to the device. In other words, this metric is the capacity that can be made available on the device.</p> <p>You can free up the device capacity by deleting the local copy of files that have a copy on both the device and the cloud.</p>
Total capacity	<p>Refers to the total bytes on the device to write data to, which is also referred to as the total size of the local cache.</p> <p>You can now increase the capacity of an existing virtual device by adding a data disk. Add a data disk through the hypervisor management for the VM and then restart your VM. The local storage pool of the Gateway device will expand to accommodate the newly added data disk.</p> <p>For more information, go to Add a hard drive for Hyper-V virtual machine.</p>
TRANSACTION METRICS	DESCRIPTION
Cloud bytes uploaded (device)	Sum of all the bytes uploaded across all the shares on your device
Cloud bytes uploaded (share)	<p>Bytes uploaded per share. This metric can be:</p> <p>Avg, which is the (Sum of all the bytes uploaded per share / Number of shares),</p> <p>Max, which is the maximum number of bytes uploaded from a share</p> <p>Min, which is the minimum number of bytes uploaded from a share</p>
Cloud download throughput (share)	<p>Bytes downloaded per share. This metric can be:</p> <p>Avg, which is the (Sum of all bytes read or downloaded to a share / Number of shares)</p> <p>Max, which is the maximum number of bytes downloaded from a share</p> <p>and Min, which is the minimum number of bytes downloaded from a share</p>
Cloud read throughput	Sum of all the bytes read from the cloud across all the shares on your device
Cloud upload throughput	Sum of all the bytes written to the cloud across all the shares on your device
Cloud upload throughput (share)	Sum of all bytes written to the cloud from a share / # of shares is average, max, and min per share

TRANSACTION METRICS	DESCRIPTION
Read throughput (network)	<p>Includes the system network throughput for all the bytes read from the cloud. This view can include data that is not restricted to shares.</p> <p>Splitting will show the traffic over all the network adapters on the device, including adapters that are not connected or enabled.</p>
Write throughput (network)	<p>Includes the system network throughput for all the bytes written to the cloud. This view can include data that is not restricted to shares.</p> <p>Splitting will show the traffic over all the network adapters on the device, including adapters that are not connected or enabled.</p>
EDGE COMPUTE METRICS	DESCRIPTION
Edge compute - memory usage	
Edge compute - percentage CPU	

View device events

Take the following steps in the Azure portal to view a device event.

1. In the Azure portal, go to your Azure Stack Edge / Data Box Gateway resource and then go to **Monitoring > Device events**.
2. Select an event and view the alert details. Take appropriate action to resolve the alert condition.

The screenshot shows the Azure portal interface for a device named 'MyDataBoxGW1'. On the left, the 'Device events' section is selected under the 'Monitoring' category. A specific event titled 'Lost heartbeat from your device.' is highlighted with a red box. To the right, a detailed 'Alert details' modal is open, also with a red box around its content area. The modal displays the message 'Lost heartbeat from your device.', a recommendation about internet connectivity, and a 'Severity' of 'Critical'. Below the main content, there's an 'Additional information' section with an 'Occurrences' count of 1.

View hardware status

Take the following steps in the local web UI to view the hardware status of your device components.

1. Connect to the local web UI of your device.
2. Go to **Maintenance > Hardware status**. You can view the health of the various device components.

The screenshot shows the Azure Stack Edge management interface. On the left, there's a navigation sidebar with sections for Configuration (Device name, Network settings, Web proxy settings, Time settings, Cloud settings, Compute settings) and Maintenance (Power settings, Hardware status, Software update, Password change). The 'Hardware status' option is selected and highlighted with a red box. The main content area is titled 'Hardware status' and displays a table of device components and their statuses. All components listed are marked as 'Healthy'.

COMPONENT	STATUS
Power Supply 1	Healthy
Power Supply 2	Healthy
Processor 0	Healthy
Processor 1	Healthy
Physical Memory 1	Healthy
Physical Memory 2	Healthy
Physical Memory 13	Healthy
Physical Memory 14	Healthy
Disk 2	Healthy
Disk 3	Healthy

Next steps

- Learn how to [Manage bandwidth](#).
- Learn how to [Manage alert notifications](#).

Return your Azure Stack Edge device

9/21/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO: ✓ Azure Stack Edge Pro - GPU ✓ Azure Stack Edge Pro R ✓ Azure Stack Edge Mini R ✓ Azure Stack Edge Pro - FPGA

This article describes how to wipe the data and then return your Azure Stack Edge device. After you've returned the device, you can also delete the resource associated with the device.

In this article, you learn how to:

- Wipe the data off the data disks on the device
- Initiate device return in Azure portal
- Pack up the device and schedule a pickup
- Delete the resource in Azure portal

Erase data from the device

To wipe the data off the data disks of your device, you need to reset your device.

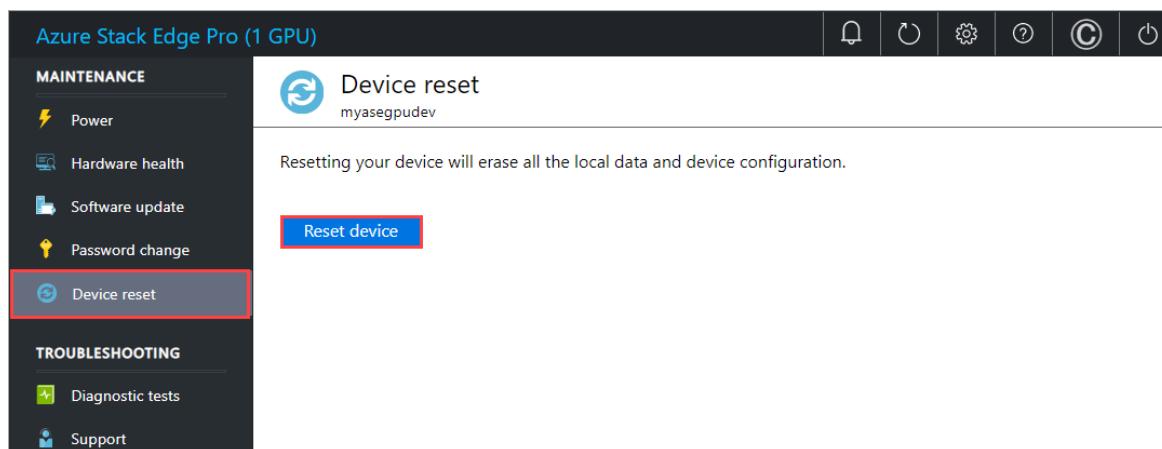
Before you reset, create a copy of the local data on the device if needed. You can copy the data from the device to an Azure Storage container.

You can initiate the device return even before the device is reset.

You can reset your device in the local web UI or in PowerShell. For PowerShell instructions, see [Reset your device](#).

To reset your device using the local web UI, take the following steps.

1. In the local web UI, go to **Maintenance > Device reset**.
2. Select **Reset device**.



3. When prompted for confirmation, review the warning. Type **Yes** and then select **Yes** to continue.

Confirm device reset

Are you sure you want to reset your device to factory settings? This action deletes all the local data on the device. To confirm, enter 'Yes' and click Yes.

* Enter 'Yes'



The reset erases the data off the device data disks. Depending on the amount of data on your device, this process takes about 30-40 minutes.

NOTE

- If you're exchanging or upgrading to a new device, we recommend that you reset your device only after you've received the new device.
- The device reset only deletes all the local data off the device. The data that is in the cloud isn't deleted and collects charges. This data needs to be deleted separately using a cloud storage management tool like [Azure Storage Explorer](#).

Initiate device return

To begin the return process, take the following steps.

- [Azure Edge Hardware Center \(Preview\)](#)
- [Portal \(Classic\)](#)

If you used the Azure Edge Hardware Center to order your device, follow these steps to return the device:

1. In the Azure portal, go to your Azure Edge Hardware Center order item resource. In the **Overview**, go to the top command bar in the right pane and select **Return**. The return option is only enabled after you have received a device.

The screenshot shows the Azure Edge Hardware Center Overview blade for an order item named 'DemoOrderAS3contoso-re-03'. The top navigation bar includes 'Home >', the order name, and a 'PREVIEW' link. Below the navigation is a search bar and a set of top-level navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Locks, Automation, Tasks (preview), Support + troubleshooting, and New Support Request. On the right side, there's a summary section with details like Resource group, Location, Subscription, and Tags. Below this is a status section showing a flow from 'Confirmed' to 'Shipped' to 'Delivered'. A message states 'Order item delivered' and 'Your order item was delivered to your address.' At the bottom, there's a call-to-action to 'Configure and activate your hardware by creating an Azure Stack Edge management resource.'

2. In the **Return hardware** blade, provide the following information:

Return hardware

PREVIEW

Reset your hardware unit and initiate return by providing the information below.

Reason for returning *

Business need is met

Hardware details

Serial number *

DemoOrderAS3contoso-re-03

Service tag

 Shipping box required to return the hardware unit

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

 I have reviewed the provided information. I agree to the privacy terms.

Pickup details

Contact person

Address

Gus Poland
4255555555
gusp@contoso.com
Contoso LE

One Microsoft Way
Building 52
Redmond
WA 98152 United States

[Add a new address](#) [Select a different address](#)
[Initiate Return](#)
[Cancel](#)

a. From the dropdown list, select a **Reason for returning**.

b. Provide the serial number of the device. To get the device serial number, go to the local web UI of the device and then go to **Overview**.

System		Device	
Health status : Healthy	Device serial no. : HW9C1T2	Software version : 2.1.1272.1632	Node serial no. : HW9C1T2
Software version : 2.1.1272.1632	Total capacity : 4.19 TB	Total capacity : 4.19 TB	State : Not activated
Total capacity : 4.19 TB	Available capacity : 4.15 TB	Available capacity : 4.15 TB	

c. (Optional) Enter the **Service tag** number. The service tag number is an identifier with five or more characters, which is unique to your device. The service tag is located on the bottom-right corner of the device (as you face the device). Pull out the information tag (it is a slide-out label panel). This panel contains system information such as service tag, NIC, MAC address, and so on.



- d. To request a return shipping box, check the **Shipping box required to return the hardware unit**. You can request it. Answer **Yes** to the question **Need an empty box to return**.
- e. Review the **Privacy terms**, and select the checkbox by the note that you have reviewed and agree to the privacy terms.
- f. Verify the **Pickup details**. By default, these are set to your shipping address. You can add a new address or select a different one from the saved addresses for the return pickup.

Return hardware

Reason for returning: Business need is met

Hardware details:

- Serial number: DemoOrderAS3contoso-re-03
- Service tag: ASE-service-tag-number-1234

Shipping box required to return the hardware unit

Privacy terms

Your privacy is important to us. Microsoft uses the personal data you provide on this form as necessary to complete any transaction as part of the service. If you need to provide personal data in order to complete your registration or an order, you agree that we may share such data with your consent with select third party companies working on our behalf to help provide the service you have requested. If you would like to make changes to, or request deletion of the personal data provided to the third party companies, please contact the third party company directly.

For more information about Microsoft's privacy practices, see <https://aka.ms/privacy>

I have reviewed the provided information. I agree to the privacy terms.

Pickup details

Contact person	Address
Gus Poland 4255555555 gusp@contoso.com Contoso LE	One Microsoft Way Building 52 Redmond WA 98152 United States

[Add a new address](#) [Select a different address](#)

Select address(es)

Showing addresses from address book with selected ship to country/region | PREVIEW

Maximum of 20 addresses can be added to an order

Contact person	Address
Noopur 9112312312 test@test.com Microsoft	RedmondOffice One Microsoft Way Redmond WA 233435 United States
Bldg42Office One microsoft way, building 42 Redmond WA 233434 United States	TestReturnAddress 9112312312 test@test.com
AddressAlias Line1 City	

Initiate Return **Select** **Cancel**

g. Select **Initiate return**.

- Once the return request is submitted, the order item resource starts reflecting the status of your return shipment. The status progresses from **Return initiated** to **Picked up** to **Return completed**. Use the portal to check the return status of your resource at any time.

DemoOrderAS3contoso-re-03

Resource group (change) : testRG

Location (change) : East US

Subscription (change) : Azure Data Box testing

Subscription ID : <Subscription ID>

Tags (change) : test : test

Return initiated → Picked-up → Return completed

Return initiated

Return request for your hardware is in progress. We will reach out to you with more details via email.

Azure Stack Edge Pro - 1 GPU : 40 vCPU Usable compute, 102 GB Usable memory, 4.2 TB Usable storage

Device serial number: DemoOrderAS3contoso-re-03

Order name : DemoOrderAS3

Requested on : 9/16/2021

Pickup address : 1020 Enterprise Way, Sunnyvale CA 94089 US

Contact information : Gus Poland 4085555555, gus.poland@contoso.com

[View Updates](#)

- Once the request is initiated, the Azure Stack Edge operations team reaches out to you to help schedule the device pickup.

The next step is to package the device.

Pack the device

To pack the device, take the following steps.

- Shut down the device. In the local web UI, go to **Maintenance > Power settings**.
- Select **Shut down**. When prompted for confirmation, click **Yes** to continue. For more information, see [Manage power](#).

3. Unplug the power cables and remove all the network cables from the device.
4. Carefully prepare the shipment package as per the following instructions and as shown in the following diagram:



- a. Use the shipping box you requested from Azure or the original shipping box with its foam packaging.
- b. Place the bottom foam piece in the box.
- c. Lay the device on top of the foam taking care that it sits snugly in the foam.
- d. Place the top foam piece in the package.
- e. Place the power cords in the accessory tray and the rails on the top foam piece.
- f. Seal the box and affix the shipping label that you received from Azure on the package.

IMPORTANT

If proper guidelines to prepare the return shipment aren't observed, the device could be damaged and damaged device fee may apply. Review the [Product Terms of service](#) and the [FAQ on lost or damaged device](#).

Schedule a pickup

To schedule a pickup, take the following steps.

1. Schedule a pickup with your regional carrier. If returning the device in US, your carrier could be UPS or FedEx. To schedule a pickup with UPS:

- a. Call the local UPS (country/region-specific toll free number).
 - b. In your call, quote the reverse shipment tracking number as shown on your printed label.
 - c. If the tracking number isn't quoted, UPS will require you to pay an extra charge during pickup.
- Instead of scheduling the pickup, you can also drop off the Azure Stack Edge at the nearest drop-off location.

Complete return

In this section, you can verify when the return is complete and then choose to delete the order.

-
- [Azure Edge Hardware Center \(Preview\)](#)
 - [Portal \(Classic\)](#)

When you initiate the return, the billing is paused. After the device is received at the Azure datacenter, the device is inspected for damage or any signs of tampering.

- If the device arrives intact and is in good shape, Azure Stack Edge operations team will contact you to confirm that the device was returned. You can choose to delete the resource associated with the device in the Azure portal.
- If the device arrives significantly damaged, charges may apply. For details, see the [FAQ on lost or damaged device](#) and [Product Terms of Service](#).

Next steps

- Learn how to [Get a replacement Azure Stack Edge device](#).

Replace your Azure Stack Edge device

9/21/2022 • 2 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article describes how to replace your Azure Stack Edge device. A replacement device is needed when the existing device has a hardware failure or needs an upgrade.

In this article, you learn how to:

- Open a Support ticket for hardware issue
- Create a new order for a replacement device in the Azure portal
- Install, activate the replacement device
- Return the original device

Open a Support ticket

If your existing device has a hardware failure, open a Support ticket by following these steps:

1. Open a Support ticket with Microsoft Support indicating that you wish to return the device. Select the **Azure Stack Edge Hardware** problem type, and choose the **Hardware issues** subtype.

The screenshot shows the 'contoso-edgeprod01 - New support request' page in the Azure portal. The 'Basics' tab is selected. On the left sidebar, 'New support request' is highlighted with a red box. The main form fields include:

- * Issue type: Technical
- * Subscription: MyAzureStack-test-subscription
- * Service: My services (selected)
- Azure Stack Edge and Data Box Gateway
- * Resource: contoso-edgeprod01
- * Problem type: Azure Stack Edge Hardware
- * Problem subtype: Hardware issues
- * Subject: I need to return the Azure Stack Edge device.

2. A Microsoft Support engineer will get in touch with you to determine if a Field Replacement Unit (FRU) can fix the problem and is available for this instance. If a FRU is not available or the device needs a hardware upgrade, Support will guide you to place a new order and return your old device.

Create a new order

Create a new resource for the activation of your replacement device by following the steps in [Create a new resource](#).

NOTE

Activation of a replacement device against an existing resource is not supported. The new resource is considered a new order. You will start getting billed 14 days after the device is shipped to you.

Install and activate the replacement device

Follow these steps to install and activate the replacement device:

1. [Install your device](#).
2. [Activate your device](#) against the new resource that you created earlier.

Return your existing device

Follow all the steps to return the original device:

1. [Erase the data on the device](#).
2. [Initiate device return](#) for the original device.
3. [Schedule a pickup](#).
4. Once the device is received at Microsoft, you can [Delete the resource](#) associated with the returned device.

Next steps

- Learn how to [Return an Azure Stack Edge device](#).

Migrate workloads from an Azure Stack Edge Pro FPGA to an Azure Stack Edge Pro GPU

9/21/2022 • 9 minutes to read • [Edit Online](#)

This article describes how to migrate workloads and data from an Azure Stack Edge Pro FPGA device to an Azure Stack Edge Pro GPU device. The migration process begins with a comparison of the two devices, a migration plan, and a review of migration considerations. The migration procedure gives detailed steps ending with verification and device cleanup.

IMPORTANT

Azure Stack Edge Pro FPGA devices will reach end-of-life in February 2024. If you are considering new deployments, we recommend that you explore [Azure Stack Edge Pro GPU](#) devices for your workloads.

About migration

Migration is the process of moving workloads and application data from one storage location to another. This entails making an exact copy of an organization's current data from one storage device to another storage device - preferably without disrupting or disabling active applications - and then redirecting all input/output (I/O) activity to the new device.

This migration guide provides a step-by-step walkthrough of the steps required to migrate data from an Azure Stack Edge Pro FPGA device to an Azure Stack Edge Pro GPU device. This document is intended for information technology (IT) professionals and knowledge workers who are responsible for operating, deploying, and managing Azure Stack Edge devices in the datacenter.

In this article, the Azure Stack Edge Pro FPGA device is referred to as the *source* device and the Azure Stack Edge Pro GPU device is the *target* device.

Comparison summary

This section provides a comparative summary of capabilities between the Azure Stack Edge Pro GPU vs. the Azure Stack Edge Pro FPGA devices. The hardware in both the source and the target device is largely identical; only the hardware acceleration card and the storage capacity may differ.

CAPABILITY	AZURE STACK EDGE PRO GPU (TARGET DEVICE)	AZURE STACK EDGE PRO FPGA (SOURCE DEVICE)
Hardware	Hardware acceleration: 1 or 2 Nvidia T4 GPUs Compute, memory, network interface, power supply unit, and power cord specifications are identical to the device with FPGA.	Hardware acceleration: Intel Arria 10 FPGA Compute, memory, network interface, power supply unit, and power cord specifications are identical to the device with GPU.
Usable storage	4.19 TB After reserving space for parity resiliency and internal use	12.5 TB After reserving space for internal use
Security	Certificates	

CAPABILITY	AZURE STACK EDGE PRO GPU (TARGET DEVICE)	AZURE STACK EDGE PRO FPGA (SOURCE DEVICE)
Workloads	IoT Edge workloads VM workloads Kubernetes workloads	IoT Edge workloads
Pricing	Pricing	Pricing

Migration plan

To create your migration plan, consider the following information:

- Develop a schedule for migration.
- When you migrate data, you may experience a downtime. We recommend that you schedule migration during a downtime maintenance window as the process is disruptive. You will set up and restore configurations in this downtime as described later in this document.
- Understand the total length of downtime and communicate it to all the stakeholders.
- Identify the local data that needs to be migrated from the source device. As a precaution, ensure that all the data on the existing storage has a recent backup.

Migration considerations

Before you proceed with the migration, consider the following information:

- An Azure Stack Edge Pro GPU device can't be activated against an Azure Stack Edge Pro FPGA resource. You should create a new resource for the Azure Stack Edge Pro GPU device as described in [Create an Azure Stack Edge Pro GPU order](#).
- The Machine Learning models deployed on the source device that used the FPGA will need to be changed for the target device with GPU. For help with the models, you can contact Microsoft Support. The custom models deployed on the source device that did not use the FPGA (used CPU only) should work as-is on the target device (using CPU).
- The IoT Edge modules deployed on the source device may require changes before the modules can be successfully deployed on the target device.
- The source device supports NFS 3.0 and 4.1 protocols. The target device only supports NFS 3.0 protocol.
- The source device support SMB and NFS protocols. The target device supports storage via the REST protocol using storage accounts in addition to the SMB and NFS protocols for shares.
- The share access on the source device is via the IP address whereas the share access on the target device is via the device name.

Migration steps at-a-glance

This table summarizes the overall flow for migration, describing the steps required for migration and the location where to take these steps.

IN THIS PHASE	DO THIS STEP	ON THIS DEVICE
Prepare source device*	1. Record configuration data 2. Back up share data 3. Prepare IoT Edge workloads	Source device
Prepare target device*	1. Create a new order 2. Configure and activate	Target device

IN THIS PHASE	DO THIS STEP	ON THIS DEVICE
Migrate data	1. Migrate data from shares 2. Redeploy IoT Edge workloads	Target device
Verify data	Verify migrated data	Target device
Clean up, return	Erase data and return	Source device

* The source and target devices can be prepared in parallel.

Prepare source device

The preparation includes that you identify the Edge cloud shares, Edge local shares, and the IoT Edge modules deployed on the device.

1. Record configuration data

Do these steps on your source device via the local UI.

Record the configuration data on the *source* device. Use the [Deployment checklist](#) to help you record the device configuration. During migration, you'll use this configuration information to configure the new target device.

2. Back up share data

The device data can be of one of the following types:

- Data in Edge cloud shares
- Data in local shares

Data in Edge cloud shares

Edge cloud shares tier data from your device to Azure. Do these steps on your *source* device via the Azure portal.

- Make a list of all the Edge cloud shares and users that you have on the source device.
- Make a list of all the bandwidth schedules that you have. You will recreate these bandwidth schedules on your target device.
- Depending on the network bandwidth available, configure bandwidth schedules on your device to maximize the data tiered to the cloud. That minimizes the local data on the device.
- Ensure that the shares are fully tiered to the cloud. The tiering can be confirmed by checking the share status in the Azure portal.

Data in Edge local shares

Data in Edge local shares stays on the device. Do these steps on your *source* device via the Azure portal.

- Make a list of the Edge local shares on the device.
- Since you'll be doing a one-time migration of the data, create a copy of the Edge local share data to another on-premises server. You can use copy tools such as `robocopy` (SMB) or `rsync` (NFS) to copy the data. Optionally you may have already deployed a third-party data protection solution to back up the data in your local shares. The following third-party solutions are supported for use with Azure Stack Edge Pro FPGA devices:

THIRD-PARTY SOFTWARE	REFERENCE TO THE SOLUTION
Cohesity	https://www.cohesity.com/solution/cloud/azure/ For details, contact Cohesity.

THIRD-PARTY SOFTWARE	REFERENCE TO THE SOLUTION
Commvault	https://www.commvault.com/azure For details, contact Commvault.
Veritas	http://veritas.com/azure For details, contact Veritas.
Veeam	https://www.veeam.com/kb4041 For details, contact Veeam.

3. Prepare IoT Edge workloads

- If you have deployed IoT Edge modules and are using FPGA acceleration, you may need to modify the modules before these will run on the GPU device. Follow the instructions in [Modify IoT Edge modules](#).

Prepare target device

1. Create new order

You need to create a new order (and a new resource) for your *target* device. The target device must be activated against the GPU resource and not against the FPGA resource.

To place an order, [Create a new Azure Stack Edge resource](#) in the Azure portal.

2. Set up, activate

You need to set up and activate the *target* device against the new resource you created earlier.

Follow these steps to configure the *target* device via the Azure portal:

- Gather the information required in the [Deployment checklist](#). You can use the information that you saved from the source device configuration.
- [Unpack, rack mount and cable your device](#).
- [Connect to the local UI of the device](#).
- Configure the network using a different set of IP addresses (if using static IPs) than the ones that you used for your old device. See how to [configure network settings](#).
- Assign the same device name as your old device and provide a DNS domain. See how to [configure device setting](#).
- Configure certificates on the new device. See how to [configure certificates](#).
- Get the activation key from the Azure portal and activate the new device. See how to [activate the device](#).

You are now ready to restore the share data and deploy the workloads that you were running on the old device.

Migrate data

You will now copy data from the source device to the Edge cloud shares and Edge local shares on your *target* device.

1. From Edge cloud shares

Follow these steps to sync the data on the Edge cloud shares on your target device:

- [Add shares](#) corresponding to the share names created on the source device. When you create the shares, make sure that **Select blob container** is set to **Use existing**, and then select the container that was used with the previous device.
- [Add users](#) that had access to the previous device.
- [Refresh the share](#) data from Azure. Refreshing the share will pull down all the cloud data from the existing

container to the shares.

- Recreate the bandwidth schedules to be associated with your shares. See [Add a bandwidth schedule](#) for detailed steps.

2. From Edge local shares

You may have deployed a third-party backup solution to protect the local shares data for your IoT workloads. You will now need to restore that data.

After the replacement device is fully configured, enable the device for local storage.

Follow these steps to recover the data from local shares:

- Configure compute on the device.
- Add all the local shares on the target device. See the detailed steps in [Add a local share](#).
- Accessing the SMB shares on the source device will use the IP addresses whereas on the target device, you'll use device name. See [Connect to an SMB share on Azure Stack Edge Pro GPU](#). To connect to NFS shares on the target device, you'll need to use the new IP addresses associated with the device. See [Connect to an NFS share on Azure Stack Edge Pro GPU](#).

If you copied your share data to an intermediate server over SMB or NFS, you can copy the data from the intermediate server to shares on the target device. If both the source and the target device are *online*, you can also copy the data directly from the source device.

If you have used third-party software to back up the data in the local shares, you will need to run the recovery procedure that's provided by the data protection solution of choice. See references in the following table.

THIRD-PARTY SOFTWARE	REFERENCE TO THE SOLUTION
Cohesity	https://www.cohesity.com/solution/cloud/azure/ For details, contact Cohesity.
Commvault	https://www.commvault.com/azure For details, contact Commvault.
Veritas	http://veritas.com/azure For details, contact Veritas.
Veeam	https://www.veeam.com/kb4041 For details, contact Veeam.

3. Redeploy IoT Edge workloads

Once the IoT Edge modules are prepared, you will need to deploy IoT Edge workloads on your target device. If you face any errors in deploying IoT Edge modules, see:

- [Common issues and resolutions for Azure IoT Edge](#).
- [IoT Edge runtime errors](#).

Verify data

After migration, verify that all the data has migrated and the workloads have been deployed on the target device.

Erase data, return

After the data migration is complete, erase local data and return the source device. Follow the steps in [Return your Azure Stack Edge Pro device](#).

Next steps

[Learn how to deploy IoT Edge workloads on Azure Stack Edge Pro GPU device](#)

Azure Stack Edge Pro with FPGA 2101 release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

The following release notes identify the critical open issues and the resolved issues for the 2101 release of Azure Stack Edge Pro FPGA with a built-in Field Programmable Gate Array (FPGA).

The release notes are continuously updated. As critical issues that require a workaround are discovered, they are added. Before you deploy your Azure Stack Edge device, carefully review the information in the release notes.

This release corresponds to software version:

- **Azure Stack Edge 2101 (1.6.1475.2528) - KB 4599267**

NOTE

Update 2101 can be applied only to devices that are running general availability (GA) versions of the software or later.

What's new

This release contains the following bug fix:

- **Upload issue** - This release fixes an upload problem, where upload restarts caused by a failure can slow the rate of upload completion. This problem can occur when uploading a dataset that primarily consists of files that are large relative to available bandwidth, particularly, but not limited to, when bandwidth throttling is active. This change ensures sufficient opportunity for upload completion before restarting upload for a given file.

This release also contains the following updates:

- All cumulative Windows updates and .NET framework updates released through October 2020.
- The baseboard management controller (BMC) firmware version is upgraded from 3.32.32.32 to 3.36.36.36 during factory install to address incompatibility with newer Dell power supply units.
- This release supports IoT Edge 1.0.9.3 on Azure Stack Edge devices.

Known issues in this release

No new issues are release noted for this release. All the release noted issues have carried over from the previous releases. To see a list of known issues, go to [Known issues in the GA release](#).

Next steps

- [Prepare to deploy Azure Stack Edge](#)

Azure Stack Edge and Azure Data Box Gateway 2007 release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

The following release notes identify the critical open issues and the resolved issues for the 2007 release for Azure Stack Edge and Data Box Gateway.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Azure Stack Edge/Data Box Gateway, carefully review the information contained in the release notes.

This release corresponds to the software versions:

- **Azure Stack Edge 2007 (1.6.1280.1667)** - KB 4566549
- **Data Box Gateway 2007 (1.6.1280.1667)** - KB 4566550

NOTE

Update 2007 can be applied only to all devices that are running general availability (GA) versions of the software or later.

What's new

This release contains the following bug fix:

- **Upload issue** - This release fixes an upload problem where upload restarts due to failures can slow the rate of upload completion. This problem can occur when uploading a dataset that primarily consists of files that are large in size relative to available bandwidth, particularly, but not limited to, when bandwidth throttling is active. This change ensures that sufficient opportunity is given for upload completion before restarting upload for a given file.

This release also contains the following updates:

- The base image for the Windows VHD has been updated.
- All cumulative Windows updates and .NET framework updates are included that were released through May 2020.
- This release supports IoT Edge 1.0.9.3 on Azure Stack Edge devices.

Known issues in this release

No new issues are release noted for this release. All the release noted issues have carried over from the previous releases. To see a list of known issues, go to [Known issues in the GA release](#).

Next steps

- [Prepare to deploy Azure Stack Edge](#)
- [Prepare to deploy Azure Data Box Gateway](#)

Azure Stack Edge and Azure Data Box Gateway 1911 release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

The following release notes identify the critical open issues and the resolved issues for the 1911 release for Azure Stack Edge and Data Box Gateway.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Azure Stack Edge/Data Box Gateway, carefully review the information contained in the release notes.

This release corresponds to the software versions:

- **Azure Stack Edge 1911 (1.6.1049.786)**
- **Data Box Gateway 1911 (1.6.1049.786)**

NOTE

Update 1911 can be applied only to all devices that are running general availability (GA) versions of the software or later.

What's new

There are no new features in the 1911 release, only bug fixes.

Known issues in this release

No new issues are release noted for this release. All the release noted issues have carried over from the previous releases. To see a list of known issues, go to [Known issues in the GA release](#).

Next steps

- [Prepare to deploy Azure Stack Edge](#)
- [Prepare to deploy Azure Data Box Gateway](#)

Azure Data Box Edge and Azure Data Box Gateway 1906 release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

The following release notes identify the critical open issues and the resolved issues for the 1906 release for Azure Data Box Edge and Azure Data Box Gateway.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Data Box Edge/Data Box Gateway, carefully review the information contained in the release notes.

This release corresponds to the software versions:

- **Data Box Gateway 1906 (1.6.978.743)**
- **Data Box Edge 1906 (1.6.978.743)**

NOTE

Update 1906 can be applied only to Data Box Edge devices that are running general availability (GA) or 1905 version of the software.

What's new

- **Bug fix in the recovery key management workflow** - In the earlier release, there was a bug owing to which the recovery key was not getting applied. This bug is fixed in this release. We strongly recommend that you apply this update as the recovery key allows you to recover the data on the device, in the event the device doesn't boot up. For more information, see how to [save the recovery key when deploying Data Box Edge or Data Box Gateway](#).
- **Field Programmable Gate Array (FPGA) logging improvements** - Starting 1905 release, logging and alert enhancements related to FPGA were made. This continues to be a required update for Data Box Edge if you are using the Edge compute feature with the FPGA. For more information, see how to [transform data with Edge compute on your Data Box Edge](#).

Known issues in GA release

No new issues are release noted for this release. All the release noted issues have carried over from the previous releases. To see a list of known issues, go to [Known issues in the GA release](#).

Next steps

- [Prepare to deploy Azure Data Box Gateway](#)
- [Prepare to deploy Azure Data Box Edge](#)

Azure Data Box Edge and Azure Data Box Gateway 1905 release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

Overview

The following release notes identify the critical open issues and the resolved issues for the 1905 release for Azure Data Box Edge and Azure Data Box Gateway.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Data Box Edge/Data Box Gateway, carefully review the information contained in the release notes.

This release corresponds to the software versions:

- **Data Box Gateway 1905 (1.6.887.626)**
- **Data Box Edge 1905 (1.6.887.626)**

NOTE

Update 1905 can be applied only to Data Box Edge devices that are running GA version of the software.

What's new

- **Field Programmable Gate Array (FPGA) logging improvements** - In this release, we have made logging and alert enhancements related to FPGA. This is a required update for Data Box Edge if you are using the Edge compute feature with the FPGA. For more information, see how to [transform data with Edge compute on your Data Box Edge](#).

Known issues in GA release

No new issues are release noted for this release. All the release noted issues have carried over from the previous releases. To see a list of known issues, go to [Known issues in the GA release](#).

Next steps

- [Prepare to deploy Azure Data Box Gateway](#)
- [Prepare to deploy Azure Data Box Edge](#)

Azure Data Box Edge/Azure Data Box Gateway General Availability release notes

9/21/2022 • 2 minutes to read • [Edit Online](#)

Overview

The following release notes identify the critical open issues and the resolved issues for General Availability (GA) release for Azure Data Box Edge and Azure Data Box Gateway.

The release notes are continuously updated, and as critical issues requiring a workaround are discovered, they are added. Before you deploy your Data Box Edge/Data Box Gateway, carefully review the information contained in the release notes.

The GA release corresponds to the software versions:

- **Data Box Gateway 1903 (1.5.814.447)**
- **Data Box Edge 1903 (1.5.814.447)**

What's new

- **New virtual disk images** - New VHDX and VMDK are now available in the Azure portal. Download these images to provision, configure, and deploy new Data Box Gateway GA devices. The Data Box Gateway devices created in the earlier preview releases cannot be updated to this version. For more information, go to [Prepare to deploy Azure Data Box Gateway](#).
- **NFS support** - NFS support is currently in preview and available for v3.0 and v4.1 clients that access the Data Box Edge and Data Box Gateway devices.
- **Storage resiliency** - Your Data Box Edge device can withstand the failure of one data disk with the Storage resiliency feature. This feature is currently in preview. You can enable storage resiliency by selecting the **Resilient** option in the **Storage settings** in the local web UI.

Known issues in GA release

The following table provides a summary of known issues for the Data Box Gateway running release.

NO.	FEATURE	ISSUE	WORKAROUND/COMMENTS

No.	Feature	Issue	Workaround/Comments
1.	File types	The following file types are not supported: character files, block files, sockets, pipes, symbolic links.	Copying these files results in 0-length files getting created on the NFS share. These files remain in an error state and are also reported in <i>error.xml</i> . Symbolic links to directories result in directories never getting marked offline. As a result, you may not see the gray cross on the directories that indicates that the directories are offline and all the associated content was completely uploaded to Azure.
2.	Deletion	Due to a bug in this release, if an NFS share is deleted, then the share may not be deleted. The share status will display <i>Deleting</i> .	This occurs only when the share is using an unsupported file name.
3.	Copy	Data copy fails with Error: The requested operation could not be completed due to a file system limitation.	The Alternate Data Stream (ADS) associated with file size greater than 128 KB is not supported.

Next steps

- [Prepare to deploy Azure Data Box Gateway](#).
- [Prepare to deploy Azure Data Box Edge](#).

Azure Stack Edge Hardware Additional Terms

9/21/2022 • 5 minutes to read • [Edit Online](#)

APPLIES TO: Azure Stack Edge Pro - GPU Azure Stack Edge Pro 2 Azure Stack Edge Pro R Azure Stack Edge Mini R

This article documents additional terms for Azure Stack Edge hardware.

Availability of the Azure Stack Edge Device

Microsoft is not obligated to continue to offer the Azure Stack Edge Device or any other hardware product in connection with the Service. The Azure Stack Edge Device may not be offered in all regions or jurisdictions, and even where it is offered, it may be subject to availability. Microsoft reserves the right to refuse to offer the Azure Stack Edge Device to anyone in its sole discretion and judgment.

Use of the Azure Stack Edge Device

As part of the Service, Microsoft allows Customer to use the Azure Stack Edge Device for as long as Customer has an active subscription to the Service. If Customer no longer has an active subscription and fails to return the Azure Stack Edge Device, Microsoft may deem the Azure Stack Edge Device as lost as described in the "Title and Risk of Loss; Shipment and Return Responsibilities" Section.

Title and Risk of Loss; Shipment and Return Responsibilities

Title and Risk of Loss

All right, title and interest in each Azure Stack Edge Device is and shall remain the property of Microsoft, and except as described in these Additional Terms, no rights are granted to any Azure Stack Edge Device (including under any patent, copyright, trade secret, trademark or other proprietary rights). Customer will compensate Microsoft for any loss, damage or destruction to or of any Azure Stack Edge Device once it has been delivered by the carrier to Customer's designated address until the Microsoft-designated carrier accepts the Azure Stack Edge Device for return delivery, including while it is at any of Customer's locations (other than expected wear and tear that do not compromise the structure or functionality) or such circumstances as described in the "Responsibilities if a Government Customer Moves an Azure Stack Edge Device between Customer's Locations" Section. Customer is responsible for inspecting the Azure Stack Edge Device upon receipt from the carrier and for promptly reporting any damages to Microsoft Support at adbeops@microsoft.com.

If Customer prefers to arrange Customer's own pick-up and/or return of the Azure Stack Edge Device pursuant to the "Shipment and Return of Azure Stack Edge Device" Section below, Customer is responsible for the entire risk of loss of, or any damage to the Azure Stack Edge Device until it has been returned to and accepted by Microsoft. Microsoft may charge Customer for a lost device fee for the Azure Stack Edge Device (or equivalent) as described on the pricing pages for the specific Azure Stack Edge Device models under the **FAQ** section at <https://azure.microsoft.com/pricing/details/azure-stack/edge/> for the following reasons: (i) the Azure Stack Edge Device is lost or materially damaged while it is Customer's responsibility as described above, (ii) Customer does not provide the Azure Stack Edge Device to the Microsoft-designated carrier for return or return the Azure Stack Edge Device pursuant to the "Shipment and Return of Azure Stack Edge Device" Section below within 30 days from the end of Customer's use of the Service. Microsoft reserves the right to change the fee charged for lost or damaged devices, including charging different amounts for different device form factors.

Shipment and Return of Azure Stack Edge Device

Customer will be responsible for a one-time metered shipping fee for the shipment of the Azure Stack Edge

Device from Microsoft to Customer and return shipping of the same, in addition to any metered amounts for carrier charges, any taxes, or applicable customs fees. When returning an Azure Stack Edge Device to Microsoft, Customer will package and ship the same in accordance with Microsoft's instructions, including using a carrier designated by Microsoft and the packaging materials provided by Microsoft. If Customer prefers to arrange Customer's own pick-up and/or return of the same, then Customer is responsible for the costs of shipping the Azure Stack Edge Device, including protections against any loss or damage of the Azure Stack Edge Device (e.g., insurance coverage) while in transit. Customer will package and ship the Azure Stack Edge Device in accordance with Microsoft's packaging instructions. Customer is also responsible to ensure that it removes all Customer's data from the Azure Stack Edge Device prior to returning it to Microsoft, including following any Microsoft-issued processes for wiping or clearing the Azure Stack Edge Device.

Responsibilities if a Government Customer Moves an Azure Stack Edge Device between Customer's Locations

Government Customer agrees to comply with and be responsible for all applicable import, export and general trade laws and regulations should Customer decide to transport the Azure Stack Edge Device beyond the country border in which Customer receives the Azure Stack Edge Device. For clarity, but not limited to, if a government Customer is in possession of an Azure Stack Edge Device, only the government Customer may, at government Customer's sole risk and expense, transport the Azure Stack Edge Device to its different locations in accordance with this section and the requirements of the Additional Terms. Customer is responsible for obtaining at Customer's own risk and expense any export license, import license and other official authorization for the exportation and importation of the Azure Stack Edge Device and Customer's data to any different Customer location. Customer shall also be responsible for customs clearance to any different Customer location, and will bear all duties, taxes, and other official charges payable upon importation as well as all costs and risks of carrying out customs formalities in a timely manner.

If Customer transports the Azure Stack Edge Device to a different location, Customer agrees to return the Azure Stack Edge Device to the country location where Customer received it initially, prior to shipping the Azure Stack Edge Device back to Microsoft. Customer acknowledges that there are inherent risks in shipping data on and in connection with the Azure Stack Edge Device, and that Microsoft will have no liability to Customer for any damage, theft, or loss occurring to an Azure Stack Edge Device or any data stored on one, including during transit. It is Customer's responsibility to obtain the appropriate support agreement from Microsoft to meet Customer's operating objectives for the Azure Stack Edge Device; however, depending on the location to which Customer intends to move the Azure Stack Edge Device, Microsoft's ability to provide hardware servicing and support may be delayed, or may not be available.

Fees

Microsoft will charge Customer specified fees in connection with Customer's use of the Azure Stack Edge Device as part of the Service, with [the current schedule of fees for each Azure Stack Edge model](#). Customer may use other Azure services in connection with Customer's use of the Service, and Microsoft deems such services as separate services that may be subject to separate metered fees and costs. By way of example only, Azure Storage, Azure Compute, and Azure IoT Hub are separate Azure services, and if used (even in connection with its use of the Service), separate Azure metered services will apply.

Next steps

- [Azure Stack Edge](#).
- [Azure Stack Edge pricing](#).