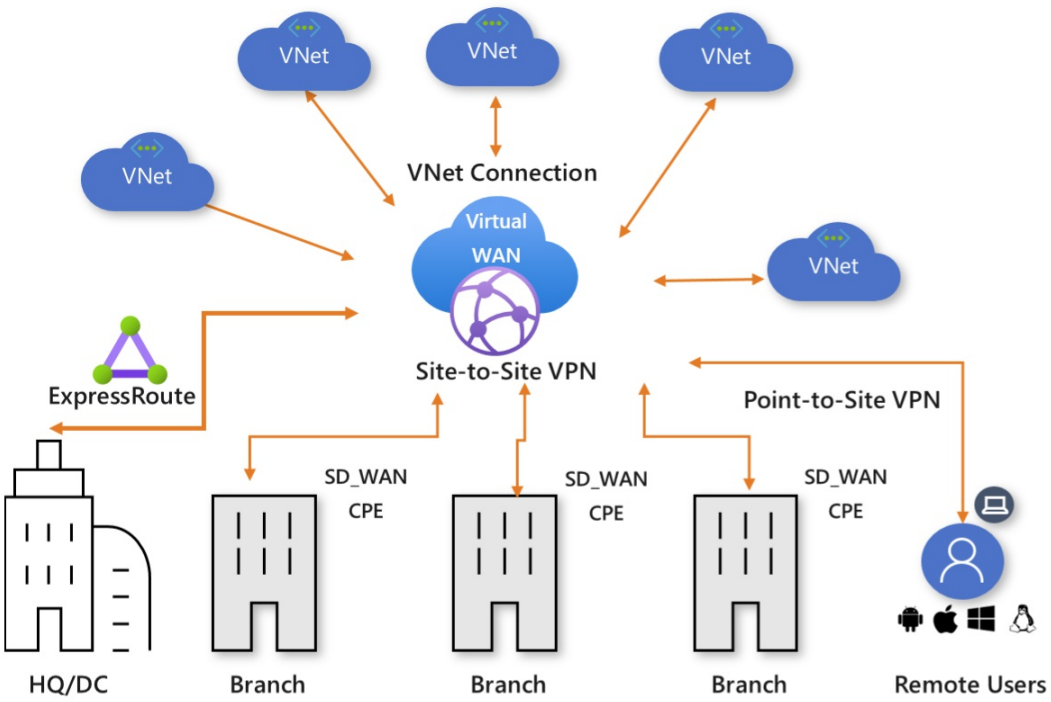
Contents

About Azure Virtual WAN

2/6/2020 • 16 minutes to read • Edit Online

Azure Virtual WAN is a networking service that provides optimized and automated branch connectivity to, and through, Azure. Azure regions serve as hubs that you can choose to connect your branches to. You can leverage the Azure backbone to also connect branches and enjoy branch-to-VNet connectivity. We have a list of partners that support connectivity automation with Azure Virtual WAN VPN. For more information, see the Virtual WAN partners and locations article.

Azure Virtual WAN brings together many Azure cloud connectivity services such as site-to-site VPN, User VPN (point-to-site), and ExpressRoute into a single operational interface. Connectivity to Azure VNets is established by using virtual network connections. It enables global transit network architecture based on a classic hub-and-spoke connectivity model where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.



This article provides a quick view into the network connectivity in Azure Virtual WAN. Virtual WAN offers the following advantages:

- **Integrated connectivity solutions in hub and spoke:** Automate site-to-site configuration and connectivity between on-premises sites and an Azure hub.
- **Automated spoke setup and configuration:** Connect your virtual networks and workloads to the Azure hub seamlessly.
- **Intuitive troubleshooting:** You can see the end-to-end flow within Azure, and then use this information to take required actions.

Basic and Standard virtual WANs

There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

VIRTUAL WAN TYPE	HUB TYPE	AVAILABLE CONFIGURATIONS
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub

> **NOTE**
> You can upgrade from Basic to Standard, but cannot revert from Standard back to Basic.

For steps to upgrade a virtual WAN, see Upgrade a virtual WAN from Basic to Standard.

Architecture

For information about Virtual WAN architecture and how to migrate to Virtual WAN, see the following articles:

- Virtual WAN architecture
- Global transit network architecture

Virtual WAN resources

To configure an end-to-end virtual WAN, you create the following resources:

- **virtualWAN:** The virtualWAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. It contains links to all your virtual hubs that you would like to have within the virtual WAN. Virtual WAN resources are isolated from each other and cannot contain a common hub. Virtual hubs across Virtual WAN do not communicate with each other.
- **Hub:** A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (vpnsite), you can connect to a VPN Gateway inside the virtual hub, connect ExpressRoute circuits to a virtual hub, or even connect mobile users to a Point-to-site gateway in the virtual hub. The hub is the core of your network in a region. There can only be one hub per Azure region.

  A hub gateway is not the same as a virtual network gateway that you use for ExpressRoute and VPN Gateway. For example, when using Virtual WAN, you don't create a site-to-site connection from your on-premises site directly to your VNet. Instead, you create a site-to-site connection to the hub. The traffic always goes through the hub gateway. This means that your VNets do not need their own virtual network gateway. Virtual WAN lets your VNets take advantage of scaling easily through the virtual hub and the virtual hub gateway.
- **Hub virtual network connection:** The Hub virtual network connection resource is used to connect the hub seamlessly to your virtual network.
- **(Preview) Hub-to-Hub connection** - Hubs are all connected to each other in a virtual WAN. This implies that a branch, user, or VNet connected to a local hub can communicate with another branch or VNet using the full mesh architecture of the connected hubs. You can also connect VNets within a hub transiting through the virtual hub, as well as VNets across hub, using the hub-to-hub connected framework.
- **Hub route table:** You can create a virtual hub route and apply the route to the virtual hub route table.

You can apply multiple routes to the virtual hub route table.

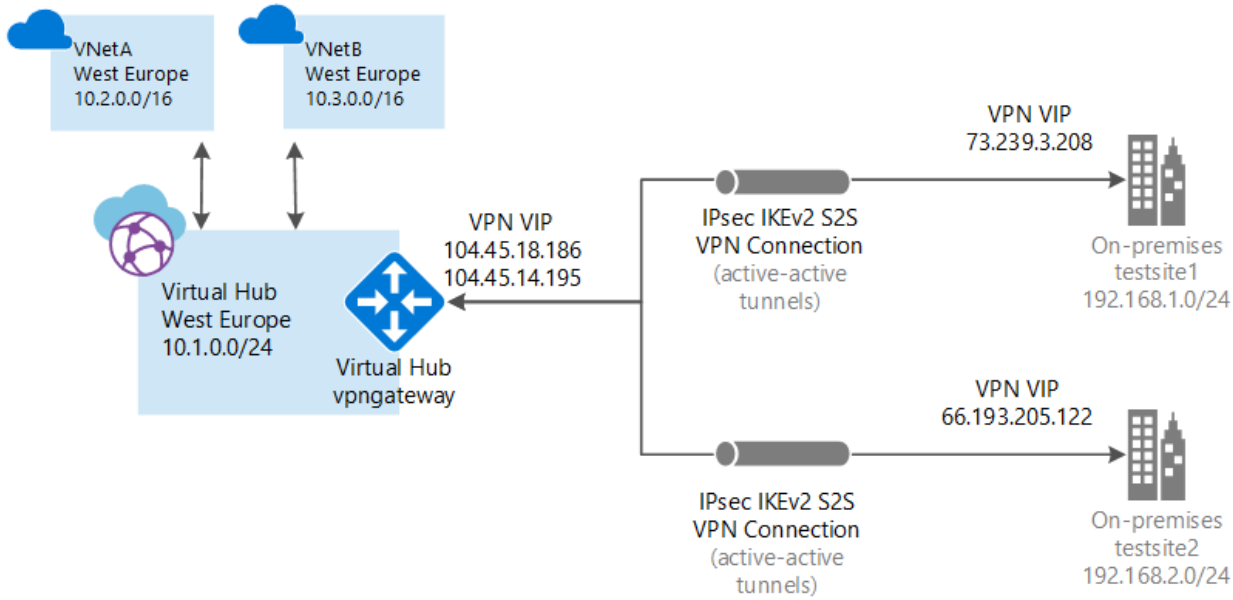
Additional Virtual WAN resources

- **Site:** This resource is used for site-to-site connections only. The site resource is **vpnsite**. It represents your on-premises VPN device and its settings. By working with a Virtual WAN partner, you have a built-in solution to automatically export this information to Azure.

Types of connectivity

Virtual WAN allows the following types of connectivity: Site-to-Site VPN, User VPN (Point-to-Site), and ExpressRoute.

Site-to-site VPN connections



When you create a virtual WAN site-to-site connection, you can work with an available partner. If you don't want to use a partner, you can configure the connection manually. For more information, see Create a site-to-site connection using Virtual WAN.

Virtual WAN partner workflow

When you work with a Virtual WAN partner, the workflow is:

1. The branch device (VPN/SDWAN) controller is authenticated to export site-centric information into Azure by using an Azure Service Principal.
2. The branch device (VPN/SDWAN) controller obtains the Azure connectivity configuration and updates the local device. This automates the configuration download, editing, and updating of the on-premises VPN device.
3. Once the device has the right Azure configuration, a site-to-site connection (two active tunnels) is established to the Azure WAN. Azure supports both IKEv1 and IKEv2. BGP is optional.

Partners for site-to-site virtual WAN connections

For a list of the available partners and locations, see the Virtual WAN partners and locations article.

User VPN (point-to-site) connections

You can connect to your resources in Azure over an IPsec/IKE (IKEv2) or OpenVPN connection. This type of connection requires a VPN client to be configured on the client computer. For more information, see Create a point-to-site connection.

ExpressRoute connections

ExpressRoute lets you connect on-premises network to Azure over a private connection. To create the

connection, see Create an ExpressRoute connection using Virtual WAN.

Locations

For location information, see the Virtual WAN partners and locations article.

FAQ

What is the difference between an Azure virtual network gateway (VPN Gateway) and an Azure Virtual WAN VPN gateway?

Virtual WAN provides large-scale site-to-site connectivity and is built for throughput, scalability, and ease of use. When you connect a site to a Virtual WAN VPN gateway, it is different from a regular virtual network gateway that uses a gateway type 'VPN'. Similarly, when you connect an ExpressRoute circuit to a Virtual WAN hub, it uses a different resource for the ExpressRoute gateway than the regular virtual network gateway that uses gateway type 'ExpressRoute'. Virtual WAN supports up to 20 Gbps aggregate throughput both for VPN and ExpressRoute. Virtual WAN also has automation for connectivity with an ecosystem of CPE branch device partners. CPE branch devices have built-in automation that auto-provisions and connects into Azure Virtual WAN. These devices are available from a growing ecosystem of SD-WAN and VPN partners. See the Preferred Partner List.

How is Virtual WAN different from an Azure virtual network gateway?

A virtual network gateway VPN is limited to 30 tunnels. For connections, you should use Virtual WAN for large-scale VPN. You can connect up to 1,000 branch connections per region (virtual hub) with aggregate of 20 Gbps per hub. A connection is an active-active tunnel from the on-premises VPN device to the virtual hub. You can have one hub per region, which means you can connect more than 1,000 branches across hubs.

What is a Virtual WAN Gateway Scale Unit

A scale unit is an unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps . 1 scale unit of ExpressRoute = 2 Gbps. Example : 10 scale unit of VPN would imply 500 Mbps * 10 = 5 Gbps

Which device providers (Virtual WAN partners) are supported?

At this time, many partners support the fully automated Virtual WAN experience. For more information, see Virtual WAN partners.

What are the Virtual WAN partner automation steps?

For partner automation steps, see Virtual WAN partner automation.

Am I required to use a preferred partner device?

No. You can use any VPN-capable device that adheres to the Azure requirements for IKEv2/IKEv1 IPsec support.

How do Virtual WAN partners automate connectivity with Azure Virtual WAN?

Software-defined connectivity solutions typically manage their branch devices using a controller, or a device provisioning center. The controller can use Azure APIs to automate connectivity to the Azure Virtual WAN. The automation includes uploading branch information, downloading the Azure configuration, setting up IPSec tunnels into Azure Virtual hubs, and automatically setting up connectivity form the branch device to Azure Virtual WAN. When you have hundreds of branches, connecting using Virtual WAN CPE Partners is easy because the onboarding experience takes away the need to set up, configure, and manage large-scale IPsec connectivity. For more information, see Virtual WAN partner automation.

How is Virtual WAN supporting SD-WAN devices?

Virtual WAN partners automate IPsec connectivity to Azure VPN end points. If the Virtual WAN partner is an SD-WAN provider, then it is implied that the SD-WAN controller manages automation and IPsec connectivity

to Azure VPN end points. If the SD-WAN device requires its own end point instead of Azure VPN for any proprietary SD-WAN functionality, you can deploy the SD-WAN end point in an Azure VNet and coexist with Azure Virtual WAN.

Does Virtual WAN change any existing connectivity features?

There are no changes to existing Azure connectivity features.

Are there new Resource Manager resources available for Virtual WAN?

Yes, Virtual WAN introduces new Resource Manager resources. For more information, please see the Overview.

How many VPN devices can connect to a single hub?

Up to 1,000 connections are supported per virtual hub. Each connection consists of four links and each link connection supports two tunnels that are in an active-active configuration. The tunnels terminate in an Azure virtual hub vpngateway.

Can the on-premises VPN device connect to multiple Hubs?

Yes. Traffic flow, when commencing, is from the on-premises device to the closest Microsoft network edge, and then to the virtual hub.

Can I deploy and use my favorite network virtual appliance (in an NVA VNet) with Azure Virtual WAN?

Yes, you can connect your favorite network virtual appliance (NVA) VNet to the Azure Virtual WAN. First, connect the network virtual appliance VNet to the hub with a Hub Virtual Network connection. Then, create a virtual hub route with a next hop pointing to the Virtual Appliance. You can apply multiple routes to the virtual hub Route Table. Any spokes connected to the NVA VNet must additionally be connected to the virtual hub to ensure that the spoke VNet routes are propagated to on-premises systems.

Can I create a Network Virtual Appliance inside the virtual hub?

A Network Virtual Appliance (NVA) cannot be deployed inside a virtual hub. However, you can create it in a spoke VNet that is connected to the virtual hub and enable a route in the hub to direct traffic for destination VNet via the NVA IP address (of the NIC).

Can a spoke VNet have a virtual network gateway?

No. The spoke VNet cannot have a virtual network gateway if it is connected to the virtual hub.

Is there support for BGP?

Yes, BGP is supported. When you create a VPN site, you can provide the BGP parameters in it. This will imply that any connections created in Azure for that site will be enabled for BGP. Additionally, if you had a VNet with an NVA, and if this NVA VNet was attached to a Virtual WAN hub, in order to ensure that routes from an NVA VNet are advertised appropriately, spokes that are attached to NVA VNet must disable BGP. Additionally, connect these spoke VNets to the virtual hub VNet to ensure spoke VNet routes are propagated to on-premises systems.

Can I direct traffic using UDR in the virtual hub?

Yes, you can direct traffic to a VNet using a virtual hub route table. This allows you to set routes for destination VNets in Azure via a specific IP address (typically of the NVA NIC).

Is there any licensing or pricing information for Virtual WAN?

Yes. See the Pricing page.

How do I calculate price of a hub?

- You would pay for the services in the hub. For example, lets say you have 10 branches or on-premises devices requiring to connect to Azure Virtual WAN would imply connecting to VPN end points in the hub. Lets say this is VPN of 1 scale unit = 500 Mbps, this is charged at $0.361/hr. Each connection is charged at $0.05/hr. For 10 connections, the total charge of service/hr would be $0.361 + $.5/hr. Data charges for traffic leaving Azure apply.

- There is additional hub charge. See the Pricing page.
- If you had ExpressRoute gateway due to ExpressRoute circuits connecting to a virtual hub, then you would pay for the scale unit price. Each scale unit in ER is 2 Gbps and each connection unit is charged at the same rate as the VPN Connection unit.

How do new partners that are not listed in your launch partner list get onboarded?

All virtual WAN APIs are open API. You can go over the documentation to assess technical feasibility. If you have any question, send an email to azurevirtualwan@microsoft.com. An ideal partner is one that has a device that can be provisioned for IKEv1 or IKEv2 IPsec connectivity.

What if a device I am using is not in the Virtual WAN partner list? Can I still use it to connect to Azure Virtual WAN VPN?

Yes as long as the device supports IPsec IKEv1 or IKEv2. Virtual WAN partners automate connectivity from the device to Azure VPN end points. This implies automating steps such as 'branch information upload', 'IPsec and configuration' and 'connectivity'.Since your device is not from a Virtual WAN partner ecosystem, you will need to do the heavy lifting of manually taking the Azure configuration and updating your device to set up IPsec connectivity.

Is it possible to construct Azure Virtual WAN with a Resource Manager template?

A simple configuration of one Virtual WAN with one hub and one vpnsite can be created using an quickstart template. Virtual WAN is primarily a REST or portal driven service.

Is Global VNet peering supported with Azure Virtual WAN?

You can connect a VNet in a different region than your virtual WAN.

Can spoke VNets connected to a virtual hub communicate with each other (V2V Transit)?

Yes. Standard Virtual WAN supports Vnet to Vnet transitive connectivity via the Virtual WAN hub that the Vnets are connected to. In Virtual WAN terminology, we refer to these paths as “local Virtual WAN VNet transit” for VNets connected to a Virtual Wan Hub within a single region, and “global Virtual WAN VNet transit” for VNets connected through multiple Virtual WAN Hubs across two or more regions. VNet transit supports up to 3 Gbps of throughput during public preview. Throughput will expanded when global transit goes GA.

NOTE: Currently V2V transit preview requires a VPN GW to be deployed in a Virtual Hub to trigger the routing elements to be launched. This VPN GW is not used for the V2V transit path. This is a known limitation and will be removed at the time of V2V GA. You can delete the VPN Gateway in the hub(s) after it is fully launched as it is not needed for V2V transit functionality.

For some scenarios, spoke Vnets can also be directly peered with each other using Virtual Network Peering in addition to local or global Virtual WAN VNet transit. In this case, Vnet Peering takes precedence over the transitive connection via the Virtual WAN hub.

What is a branch connection to Azure Virtual WAN?

A connection from a branch device into Azure Virtual WAN supports up to four links. A link is the physical connectivity link at the branch location (for example: ATT, Verizon etc.). Each link connection is composed of two active/active IPsec tunnels.

Is branch-to-branch connectivity allowed in Virtual WAN?

Yes, branch-to-branch connectivity is available in Virtual WAN for VPN and VPN to ExpressRoute.

Does branch-to-branch traffic traverse through the Azure Virtual WAN?

Yes.

Does Virtual WAN require ExpressRoute from each site?

No, the Virtual WAN does not require ExpressRoute from each site. It uses standard IPsec site-to-site connectivity via internet links from the device to an Azure Virtual WAN hub. Your sites may be connected to a

provider network using an ExpressRoute circuit. For Sites that are connected using ExpressRoute in a virtual hub, sites can have branch to branch traffic flow between VPN and ExpressRoute.

Is there a network throughput limit when using Azure Virtual WAN?

Number of branches is limited to 1000 connections per hub/region and a total of 20 Gbps in the hub. You can have 1 hub per region.

How many VPN connections does a Virtual WAN hub support?

An Azure Virtual WAN hub can support up to 1,000 S2S connections, 10,000 P2S connections, and 4 ExpressRoute connections simultaneously.

What is the total VPN throughput of a VPN tunnel and a connection?

The total VPN throughput of a hub is up to 20 Gbps based on the chosen scale unit. Throughput is shared by all existing connections. Each tunnel in a connection can support up to 1 Gbps.

I don't see the 20 Gbps setting for the virtual hub in the portal. How do I configure that?

Navigate to the VPN gateway inside a hub on the portal and click on the scale unit to change it to the appropriate setting.

Does Virtual WAN allow the on-premises device to utilize multiple ISPs in parallel, or is it always a single VPN tunnel?

A connection coming into a virtual WAN VPN is always an active-active tunnel (for resiliency within the same hub/region) using a link available at the branch. This link may be an ISP link at the on-premises branch. Virtual WAN 'VPNSite' provides the ability to add link information to the site. If you have multiple ISPs at the branch and each of the ISPs provided a link, that information can be set up in the VPN site info in Azure. However, managing failover across ISPs at the branch is completely a branch-centric routing operation.

What is global transit architecture?

For information about global transit architecture, see Global transit network architecture and Virtual WAN.

How is traffic routed on the Azure backbone?

The traffic follows the pattern: branch device ->ISP->Microsoft network edge->Microsoft DC (hub VNet)->Microsoft network edge->ISP->branch device

In this model, what do you need at each site? Just an internet connection?

Yes. An internet connection and physical device that supports IPsec, preferably from our integrated Virtual WAN partners. Optionally, you can manually manage the configuration and connectivity to Azure from your preferred device.

How do I enable default route (0.0.0.0/0) in a connection (VPN, ExpressRoute, or Virtual Network):

A virtual hub can propagate a learned default route to a virtual network/site-to-site VPN/ExpressRoute connection if the flag is 'Enabled' on the connection. This flag is visible when the user edits a virtual network connection, a VPN connection, or an ExpressRoute connection. By default, this flag is disabled when a site or an ExpressRoute circuit is connected to a hub. It is enabled by default when a virtual network connection is added to connect a VNet to a virtual hub. The default route does not originate in the Virtual WAN hub; the default route is propagated if it is already learned by the Virtual WAN hub as a result of deploying a firewall in the hub, or if another connected site has forced-tunneling enabled.

What are the differences between the Virtual WAN types (Basic and Standard)?

The 'Basic' WAN type lets you create a basic hub (SKU = Basic). A 'Standard' WAN type lets you create standard hub (SKU = Standard). Basic hubs are limited to site-to-site VPN functionality. Standard hubs let you have ExpressRoute, User VPN (P2S), full mesh hub, and VNet-to-VNet transit through the hubs. You pay a base charge of $0.25/hr for standard hubs and a data processing fee for transiting through the hubs during VNet-to-VNet connectivity, as well as data processing for hub to hub traffic. For more information, see Basic and

Standard virtual WANs. For pricing, see the Pricing page.

Next steps

Create a site-to-site connection using Virtual WAN

Migrate to Azure Virtual WAN

2/6/2020 • 11 minutes to read • Edit Online

Azure Virtual WAN lets companies simplify their global connectivity in order to benefit from the scale of the Microsoft global network. This article provides technical details for companies that want to migrate from an existing customer-managed hub-and-spoke topology, to a design that leverages Microsoft-managed Virtual WAN hubs.

For information about the benefits that Azure Virtual WAN enables for enterprises adopting a cloud-centric modern enterprise global network, see Global transit network architecture and Virtual WAN.

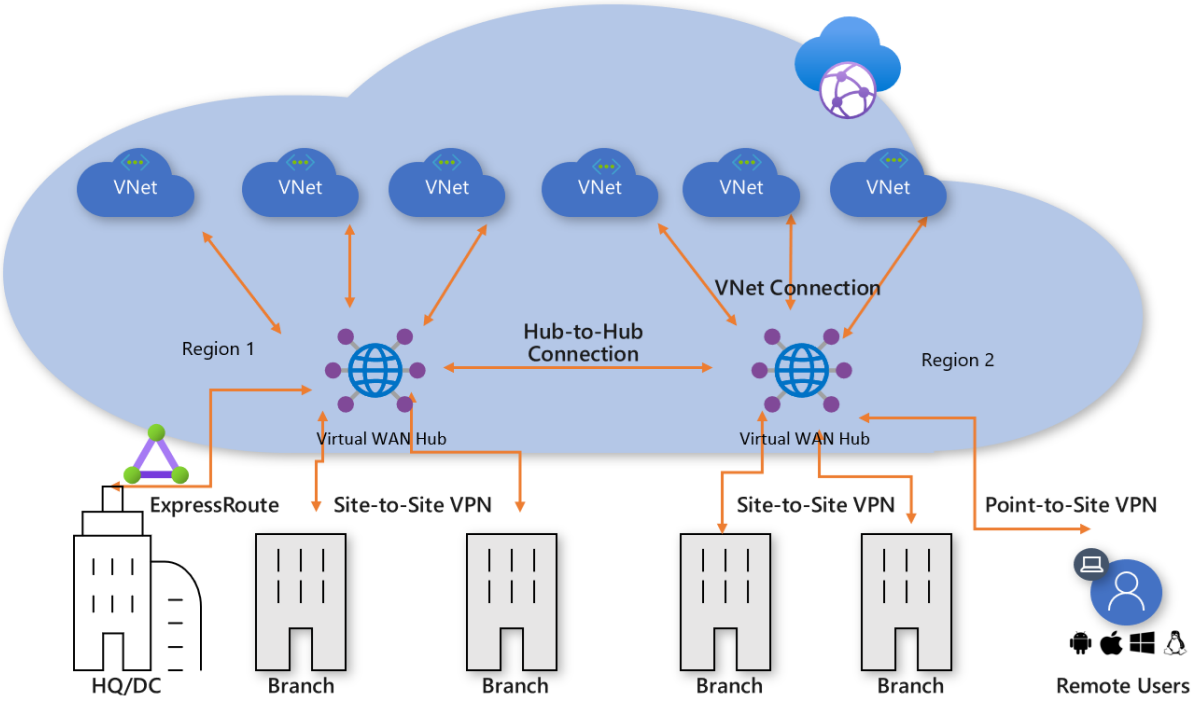


Figure: Azure Virtual WAN

The Azure Virtual Datacenter (VDC) hub-and-spoke connectivity model has been adopted by thousands of our customers to leverage the default transitive routing behavior of Azure Networking in order to build simple and scalable cloud networks. Azure Virtual WAN builds on these concepts and introduces new capabilities that allow global connectivity topologies, not only between on-premises locations and Azure, but also allowing customers to leverage the scale of the Microsoft network to augment their existing global networks.

This article shows how to migrate an existing hybrid environment to Virtual WAN.

Scenario

Contoso is a global financial organization with offices in both Europe and Asia. They are planning to move their existing applications from an on-premises data center in to Azure and have built out a foundation design based on the VDC architecture, including regional customer-managed hub virtual networks for hybrid connectivity. As part of the move to cloud-based technologies, the network team have been tasked with ensuring that their connectivity is optimized for the business moving forward.

The following figure shows a high-level view of the existing global network including connectivity to multiple Azure regions.

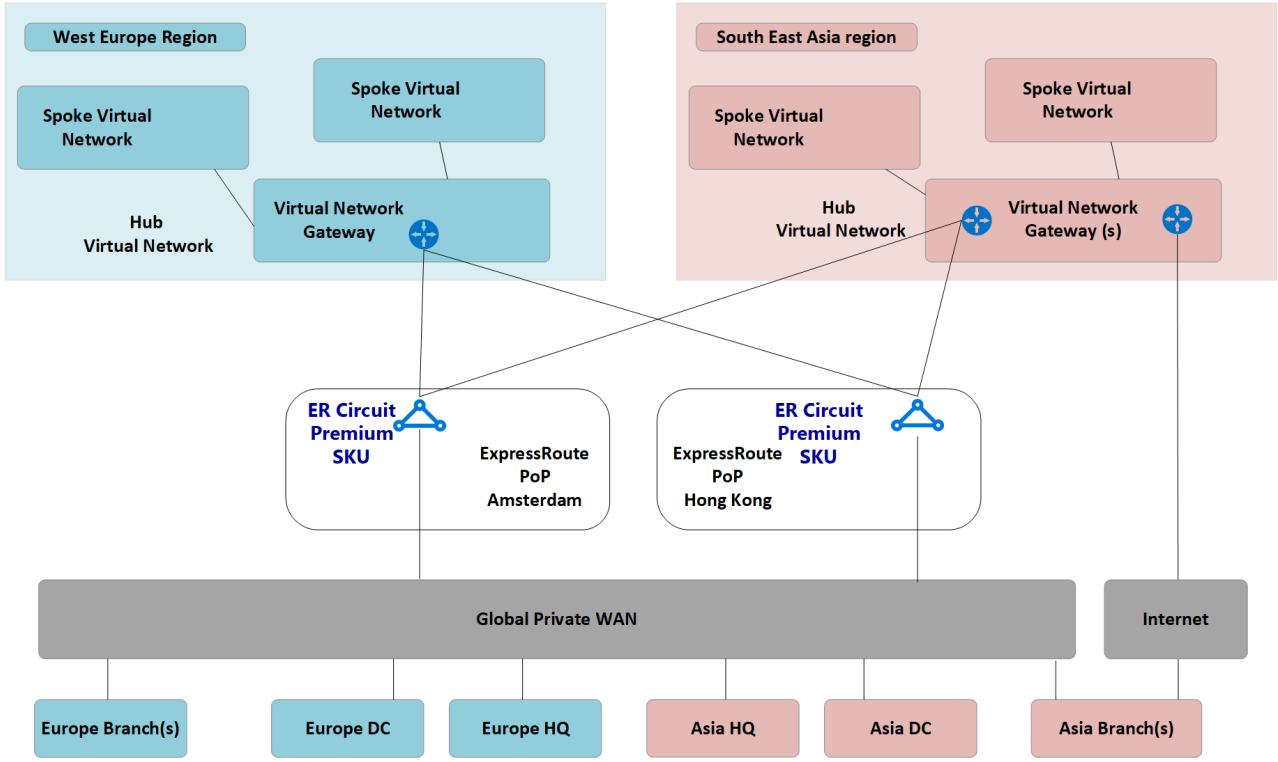


Figure: Contoso existing network topology

The following points can be understood from the existing network topology:

- A hub-and-spoke topology is used in multiple regions including ExpressRoute Premium circuits for connectivity back to a common private WAN.
- Some of these sites also have VPN tunnels directly in to Azure to reach applications hosted within the Microsoft cloud.

Requirements

The networking team have been tasked with delivering a global network model that can support the Contoso migration to the cloud and must optimize in the areas of cost, scale, and performance. In summary, the following requirements are to be met:

- Provide both head quarter (HQ) and branch offices with optimized path to cloud hosted applications.
- Remove the reliance on existing on-premises data centers (DC) for VPN termination while retaining the following connectivity paths:
  - **Branch -to- VNet**: VPN connected offices must be able to access applications migrated to the cloud in the local Azure region.
  - **Branch -to- Hub -to- Hub -to- VNet**: VPN connected offices must be able to access applications migrated to the cloud in the remote Azure region.
  - **Branch -to- branch**: Regional VPN connected offices must be able to communicate with each other and ExpressRoute connected HQ/DC sites.
  - **Branch -to- Hub -to- Hub -to- branch**: Globally separated VPN connected offices must be able to communicate with each other and any ExpressRoute connected HQ/DC sites.
  - **Branch -to- Internet**: Connected sites must be able to communicate with the Internet. This traffic must be filtered and logged.
  - **VNet -to- VNet**: Spoke virtual networks in the same region must be able to communicate with each other.
  - **VNet -to- Hub -to- Hub -to- VNet**: Spoke virtual networks in the different regions must be able to communicate with each other.
- Provide the ability for Contoso roaming users (laptop and phone) to access company resources while not on

the corporate network.

Azure Virtual WAN architecture

The following figure shows a high-level view of the updated target topology using Azure Virtual WAN to meet the requirements detailed in the previous section.

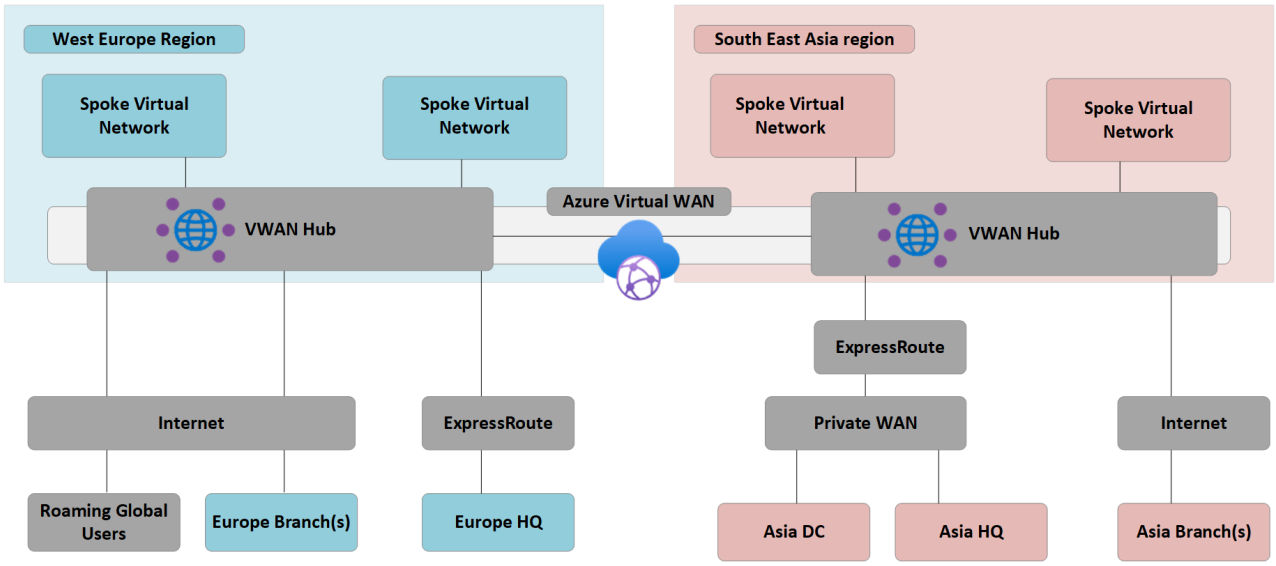


Figure: Azure Virtual WAN architecture

Summary:

- HQ in Europe remains ExpressRoute connected, Europe on-premises DC are fully migrated to Azure and now decommissioned.
- Asia DC and HQ remain connected to Private WAN. Azure Virtual WAN now used to augment the local carrier network and provide global connectivity.
- Azure Virtual WAN hubs deployed in both West Europe and South East Asia Azure regions to provide connectivity hub for ExpressRoute and VPN connected devices.
- Hubs also provide VPN termination for roaming users across multiple client types using OpenVPN connectivity to the global mesh network, allowing access to not only applications migrated to Azure, but also any resources remaining on-premises.
- Internet connectivity for resources within a virtual network provided by Azure Virtual WAN.

Internet connectivity for remote sites also provided by Azure Virtual WAN. Local internet breakout supported via partner integration for optimized access to SaaS services such as Office 365.

Migrate to Virtual WAN

This section shows the various steps for migrating to Azure Virtual WAN.

Step 1: VDC hub-and-spoke single region

Review the architecture. The following figure shows a single region topology for Contoso prior to the rollout of Azure Virtual WAN:

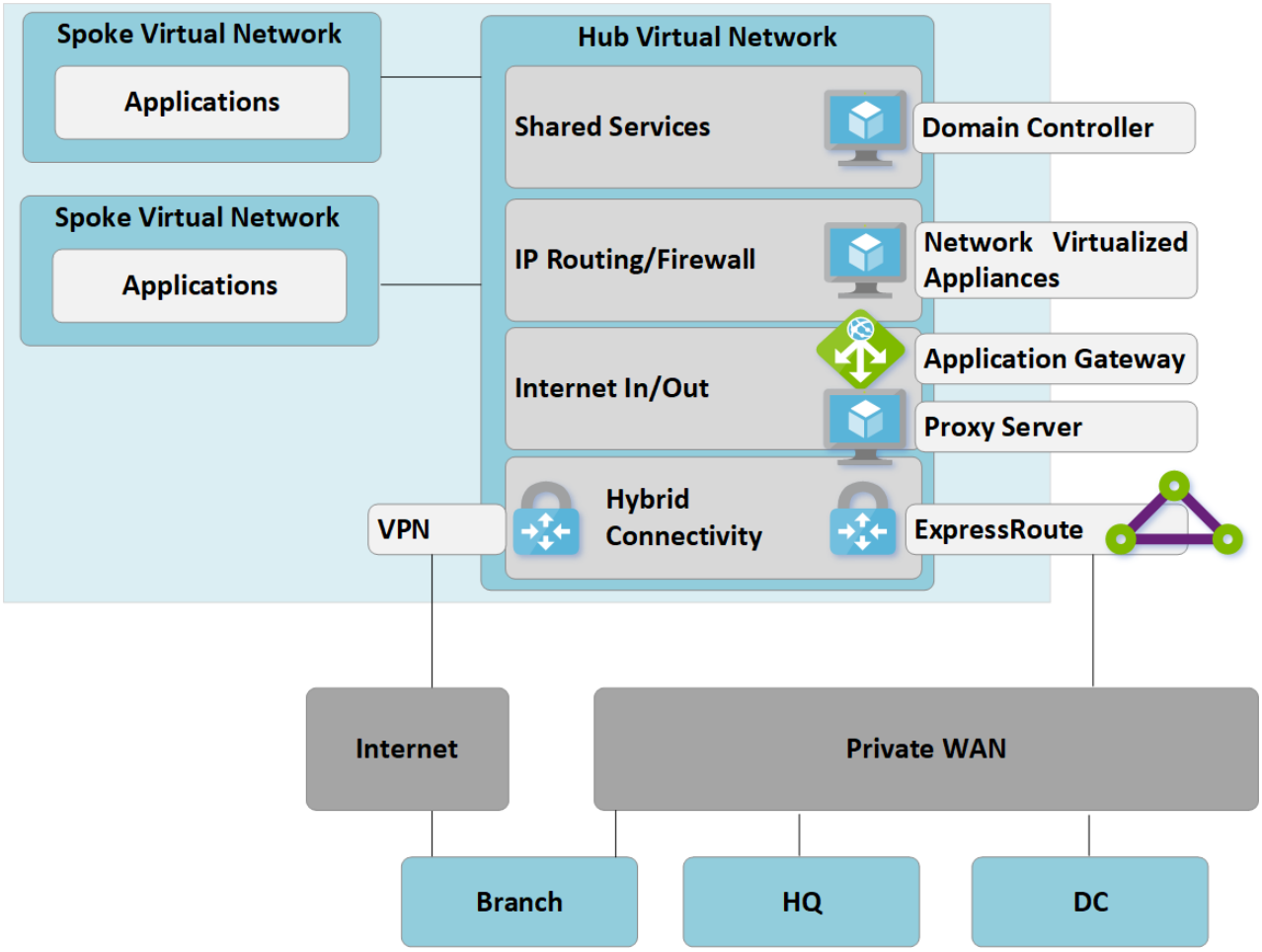


Figure 1: VDC hub-and-spoke single region

In keeping with the Virtual Data Center (VDC) approach, the customer-managed hub virtual network contains several function blocks:

- Shared services (any common function required by multiple spokes). Example: Contoso uses Windows Server domain controllers on Infrastructure-as-a-service (IaaS) virtual machines.
- IP/Routing firewall services are provided by a third-party network virtual appliance, enabling spoke-to-spoke layer-3 IP routing.
- Internet ingress/egress services including Azure Application Gateway for inbound HTTPS requests and third-party proxy services running on virtual machines for filtered outbound access to internet resources.
- ExpressRoute and VPN virtual network gateway for connectivity to on-premises networks.

Step 2: Deploy Virtual WAN hubs

Deploy a Virtual WAN hub in each region. Set up the Virtual WAN hub with VPN Gateway and ExpressRoute Gateway as described in the following articles:

- Tutorial: Create a Site-to-Site connection using Azure Virtual WAN
- Tutorial: Create an ExpressRoute association using Azure Virtual WAN

> **NOTE**
> Azure Virtual WAN must be using the Standard SKU to enable some of the traffic paths shown in this article.

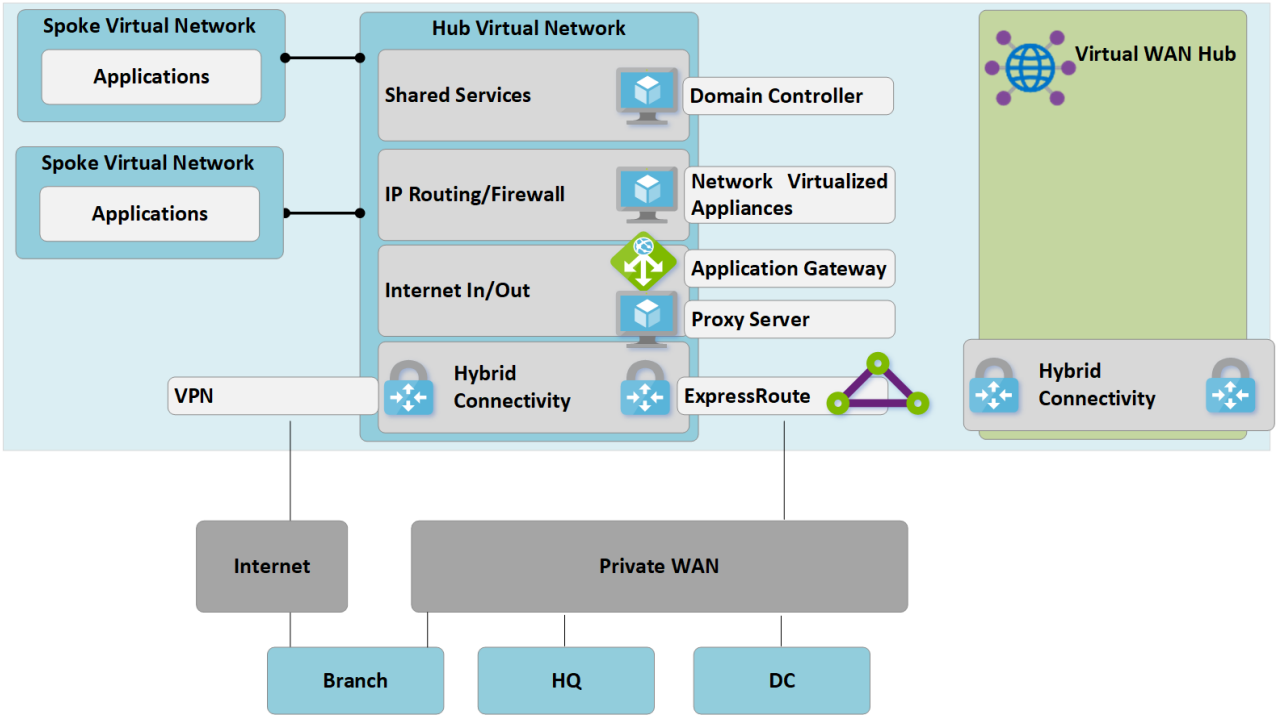


Figure 2: VDC hub-and-spoke to Virtual WAN migration

Step 3: Connect remote sites (ExpressRoute and VPN) to Virtual WAN

Connect the Virtual WAN hub to the existing ExpressRoute circuits and set up Site-to-site VPNs over the Internet to any remote branches.

> **NOTE**
> Express Routes Circuits must be upgraded to Premium SKU type to connect to Virtual WAN hub.

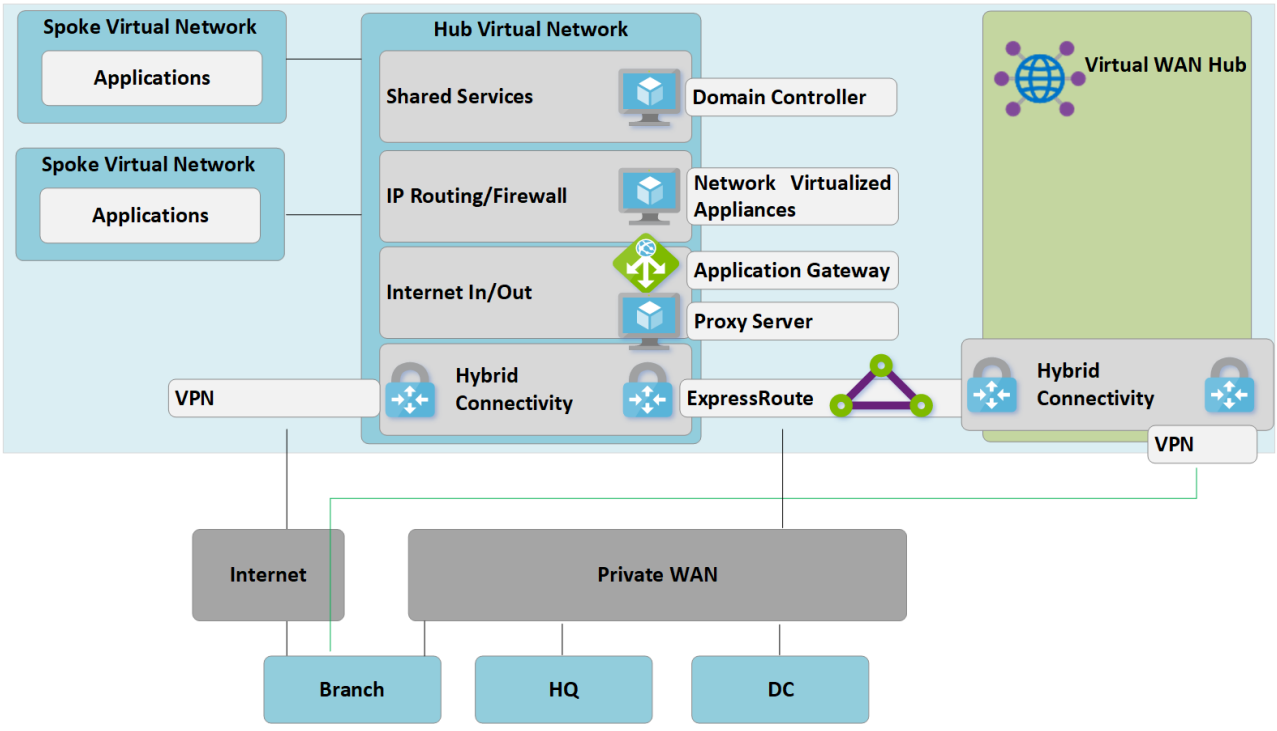


Figure 3: VDC hub-and-spoke to Virtual WAN migration

At this point, on-premises network equipment will begin to receive routes reflecting the IP address space assigned to the Virtual WAN-managed hub VNet. Remote VPN-connected branches at this stage will see two paths to any existing applications in the spoke virtual networks. These devices should be configured to continue to use the tunnel to the VDC hub to ensure symmetrical routing during the transition phase.

Step 4: Test hybrid connectivity via Virtual WAN

Prior to using the managed Virtual WAN hub for production connectivity, we recommend that you set up a test spoke virtual network and Virtual WAN VNet connection. Validate that connections to this test environment work via ExpressRoute and Site to Site VPN before continuing with the next steps.

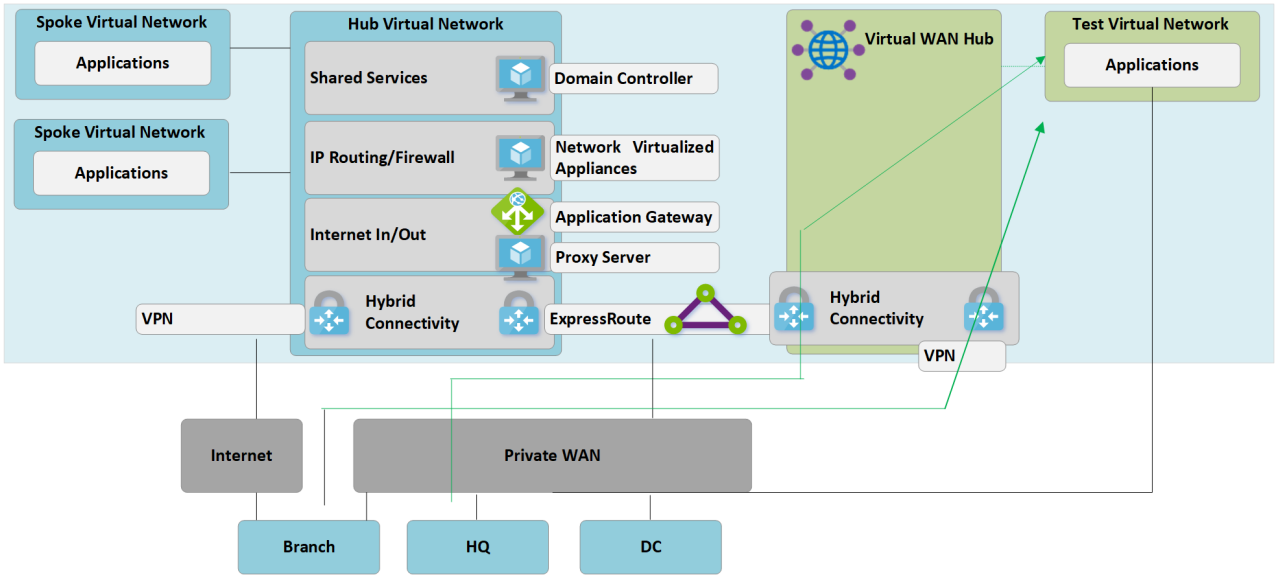


Figure 4: VDC hub-and-spoke to Virtual WAN migration

Step 5: Transition connectivity to virtual WAN hub

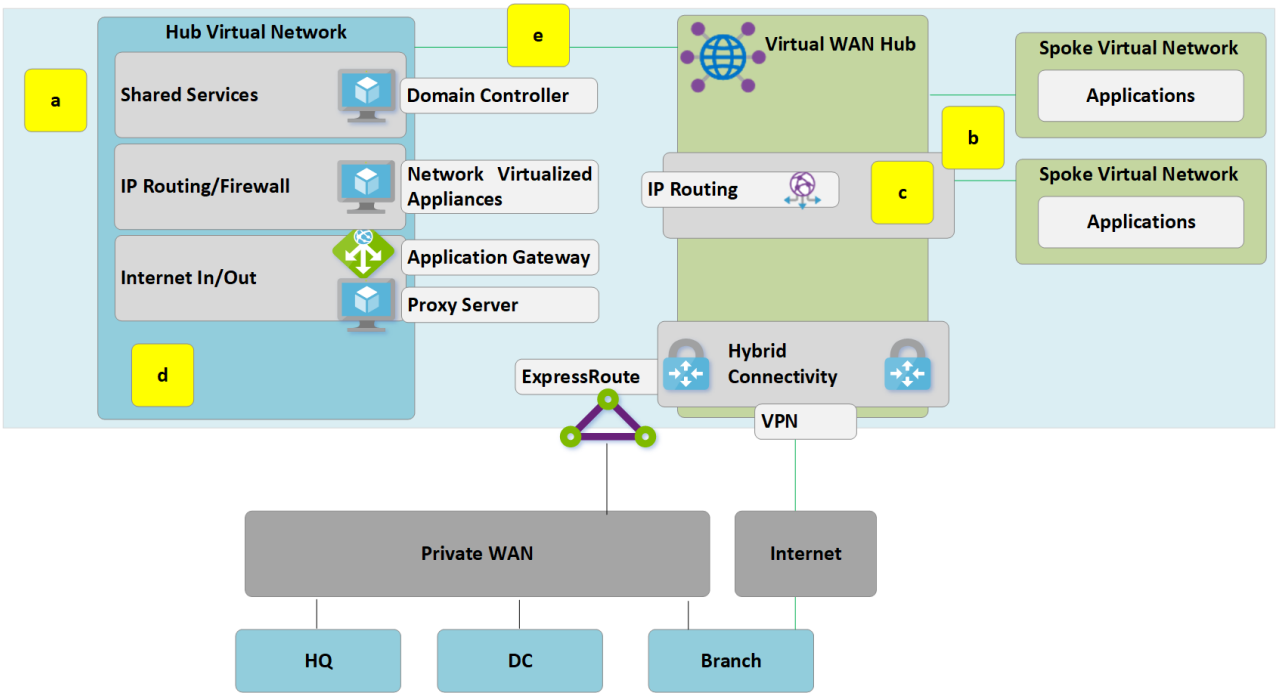


Figure 5: VDC hub-and-spoke to Virtual WAN migration

a. Delete the existing peering connections from Spoke virtual networks to the old VDC hub. Access to applications in spoke virtual networks is unavailable until steps a-c are complete.

b. Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.

c. Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

d. Existing ExpressRoute and VPN Gateways in the VDC hub are now decommissioned to permit the next step (e).

e. Connect the old VDC hub (hub virtual network) to the Virtual WAN hub via a new VNet connection.

Step 6: Old hub becomes shared services spoke

We have now redesigned our Azure network to make the Virtual WAN hub the central point in our new topology.

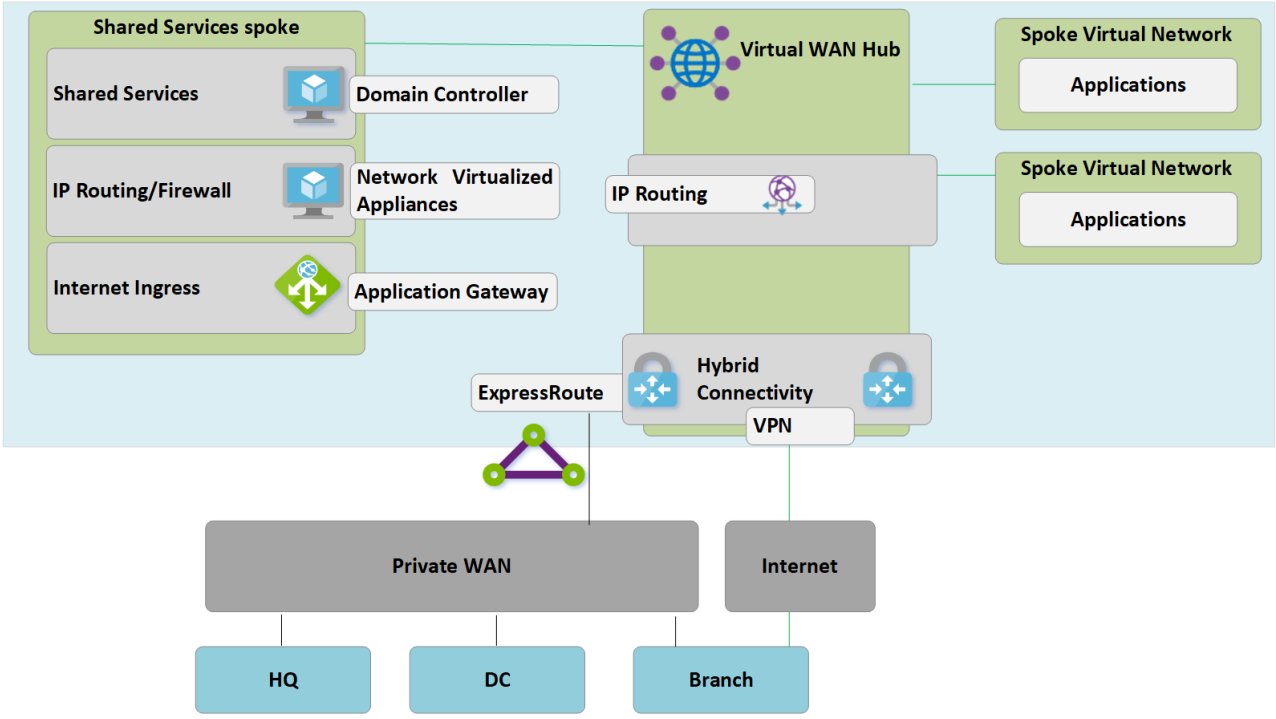


Figure 6: VDC hub-and-spoke to Virtual WAN migration

Because the Virtual WAN hub is a managed entity and does not allow deployment of custom resources such as virtual machines, the shared services block now exists as a spoke virtual network and hosts functions such as internet ingress via Azure Application Gateway or network virtualized appliance. Traffic between the shared services environment and backend virtual machines now transits the Virtual WAN-managed hub.

Step 7: Optimize on-premises connectivity to fully utilize Virtual WAN

At this stage, Contoso has mostly completed their migrations of business applications in into the Microsoft Cloud, with only a few legacy applications remaining within the on-premises DC.

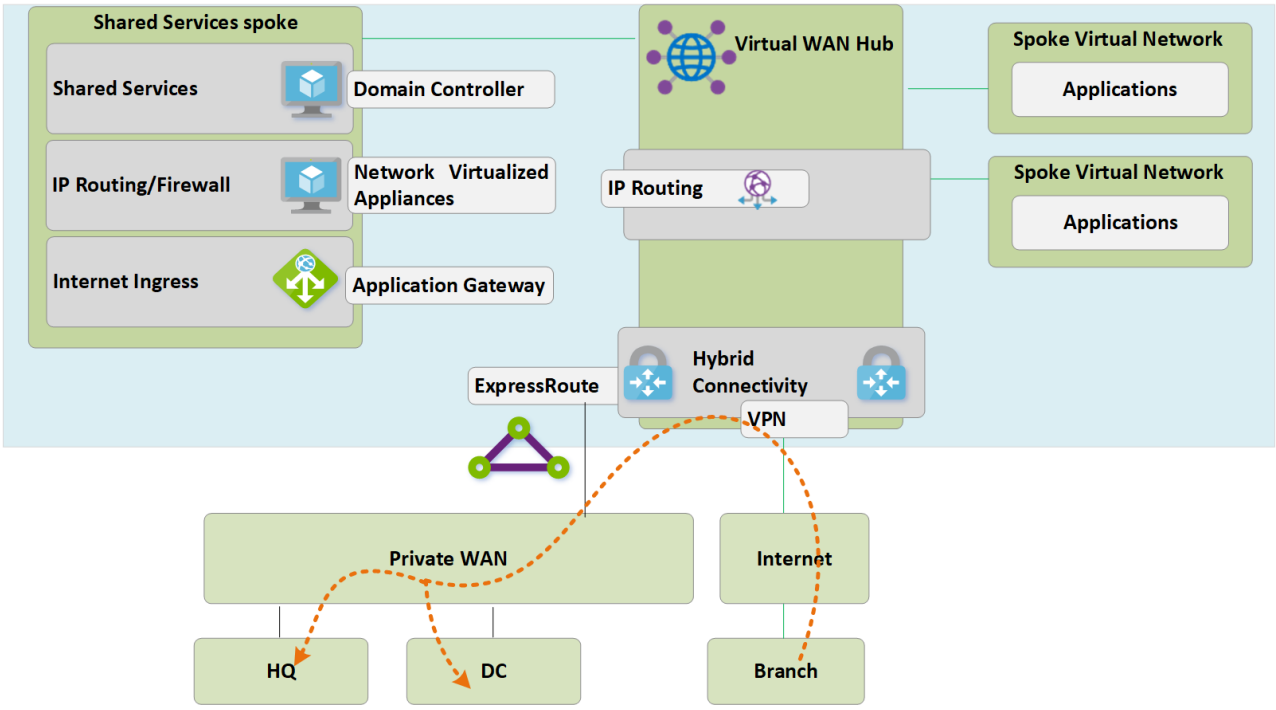


Figure 7: VDC hub-and-spoke to Virtual WAN migration

To leverage the full functionality of Azure Virtual WAN, Contoso decides to decommission their legacy on-premises VPN connections. Any branches continuing to access HQ or DC networks are able to transit the Microsoft global network using the built-in transit routing of Azure Virtual WAN.

NOTE

ExpressRoute Global Reach is an alternative choice for customers wishing to leverage the Microsoft backbone to complement their existing private WANs.

End-state architecture and traffic paths

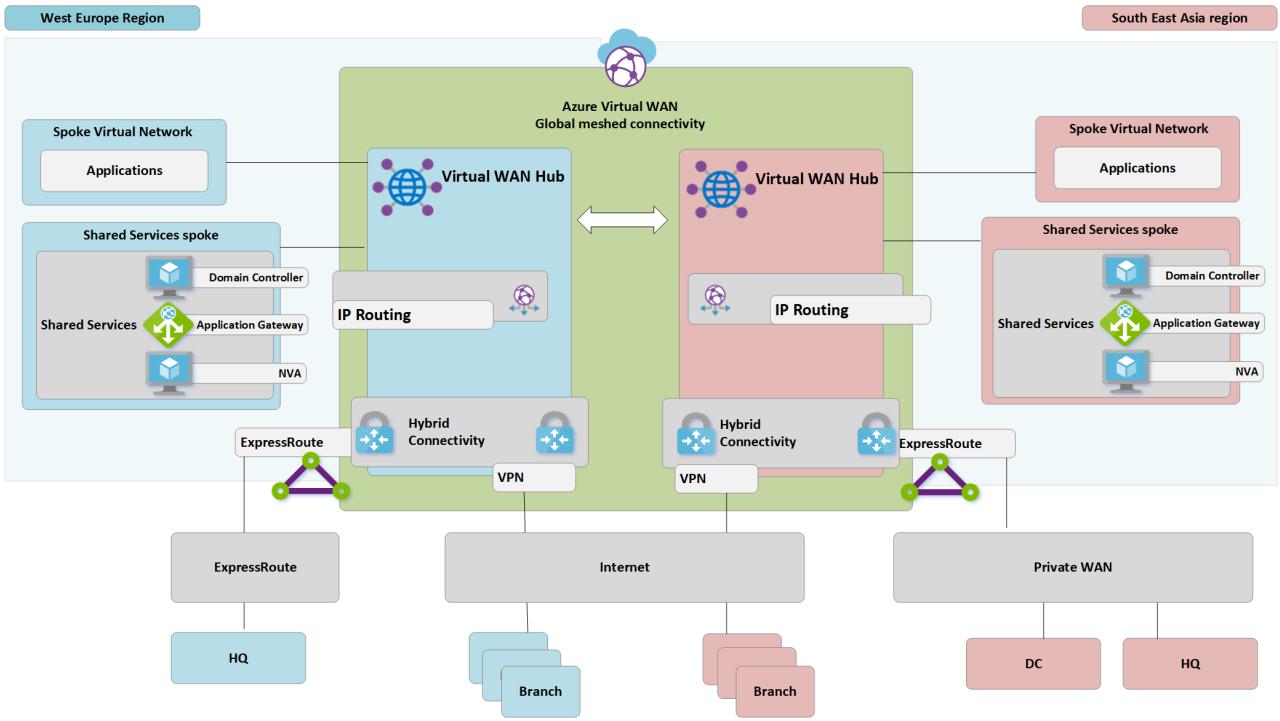


Figure: Dual region Virtual WAN

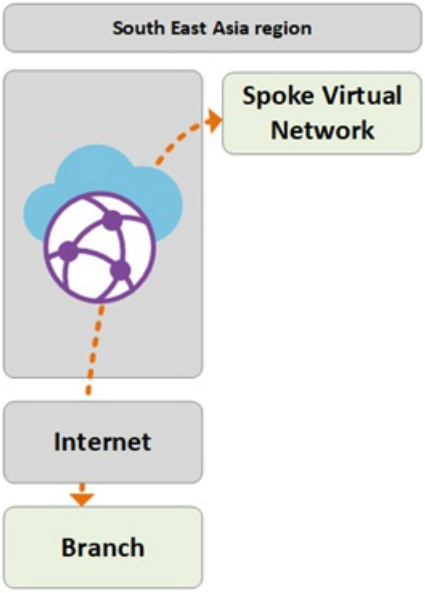
This section provides a summary of how this topology meets the original requirements by looking at some example traffic flows.

Path 1

Path 1 shows traffic flow from a S2S VPN connected branch in Asia to an Azure VNet in the South East Asia region.

The traffic is routed as follows:

- Asia branch is connected via resilient S2S BGP enabled tunnels into South East Asia Virtual WAN hub.
- Asia Virtual WAN hub routes traffic locally to connected VNet.

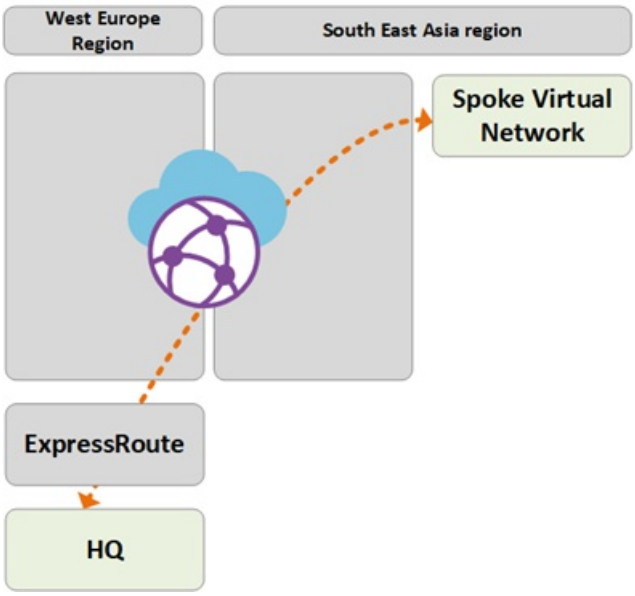


Path 2

Path 2 shows traffic flow from the ExpressRoute connected European HQ to an Azure VNet in the South East Asia region.

The traffic is routed as follows:

- European HQ is connected via premium ExpressRoute circuit into West Europe Virtual WAN hub.
- Virtual WAN hub-to-hub global connectivity enables transit of traffic to VNet connected in remote region.

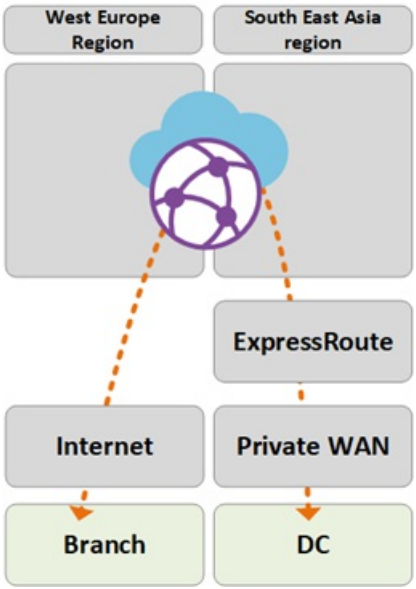


Path 3

Path 3 shows traffic flow from the Asia on-premises DC connected to Private WAN to a European S2S connected Branch.

The traffic is routed as follows:

- Asia DC is connected to local Private WAN carrier.
- ExpressRoute circuit locally terminates in Private WAN connects to the South East Asia Virtual WAN hub.
- Virtual WAN hub-to-hub global connectivity enables transit of traffic.

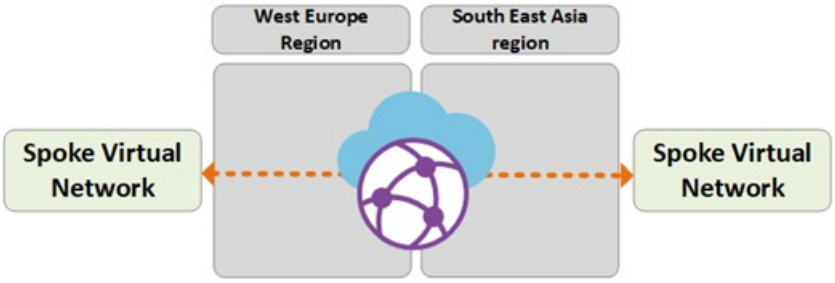


Path 4

Path 4 shows traffic flow from an Azure VNet in South East Asia region to an Azure VNet in West Europe region.

The traffic is routed as follows:

- Virtual WAN hub-to-hub global connectivity enables native transit of all connected Azure VNets without further user config.

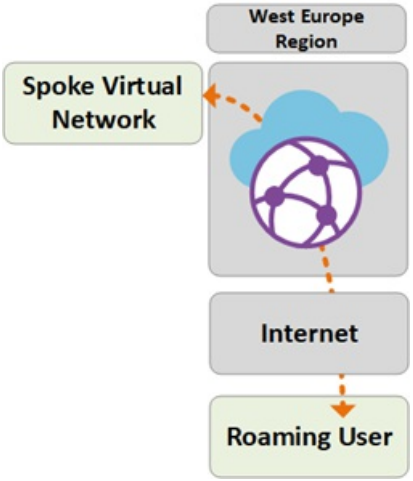


Path 5

Path 5 shows traffic flow from roaming VPN (P2S) users to an Azure VNet in the West Europe region.

The traffic is routed as follows:

- Laptop and mobile device users use the OpenVPN client for transparent connectivity in to the P2S VPN gateway in West Europe.
- West Europe Virtual WAN hub routes traffic locally to connected VNet.



Security and policy control via Azure Firewall

Contoso has now validated connectivity between all branches and VNets in line with the requirements discussed earlier in this article. To meet their requirements for security control and network isolation, they need to continue to separate and log traffic via the hub network. Previously this function was performed by a network virtual appliance (NVA). Contoso also wants to decommission their existing proxy services and utilize native Azure services for outbound Internet filtering.

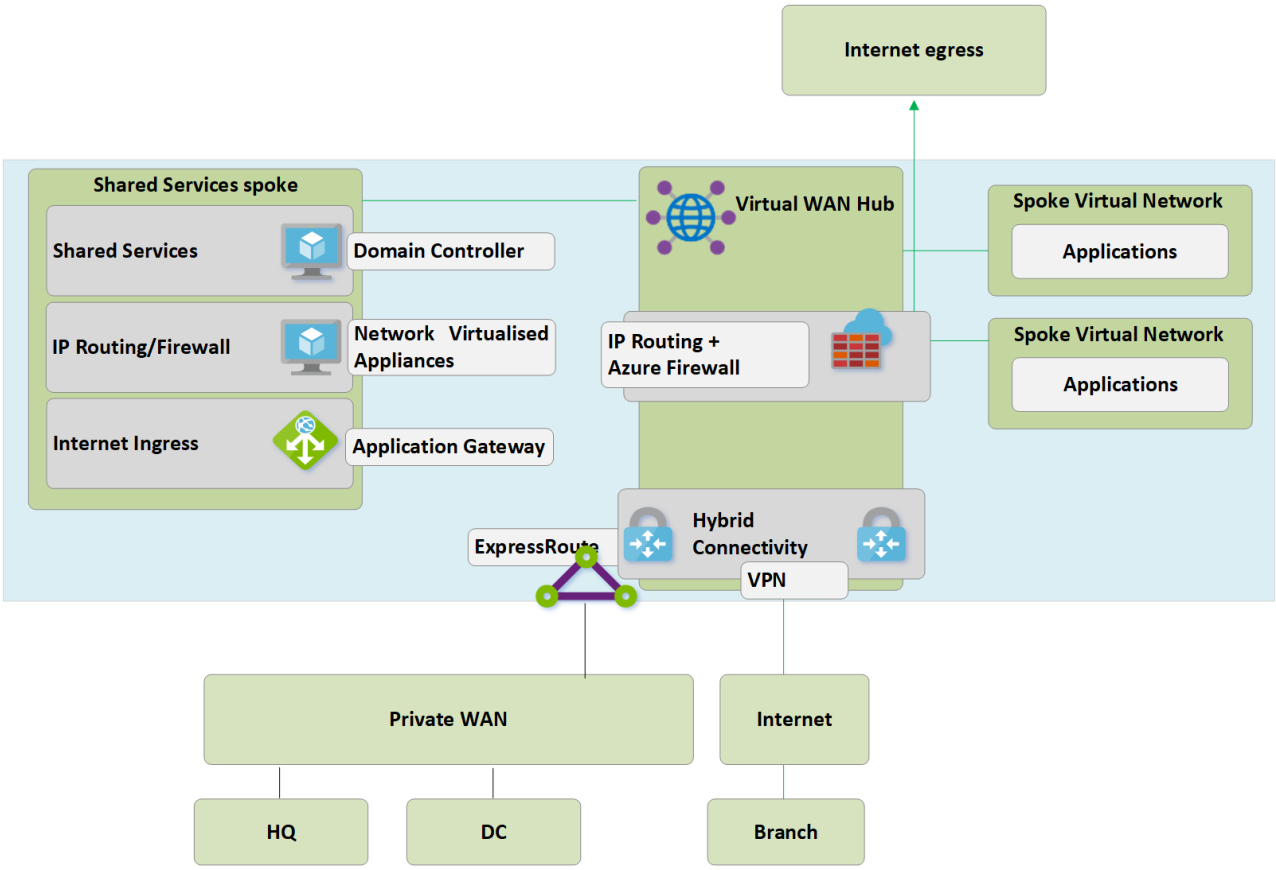


Figure: Azure Firewall in Virtual WAN (Secured Virtual hub)

The following high-level steps are required to introduce Azure Firewall into the Virtual WAN hubs to enable a unified point of policy control. For more information about this process and the concept of Secure Virtual Hubs, see Azure Firewall Manager.

1. Create Azure Firewall policy.
2. Link firewall policy to Azure Virtual WAN hub. This step allows the existing Virtual WAN hub to function as a secured virtual hub, and deploys the required Azure Firewall resources.

> **NOTE**
>
> If the Azure Firewall is deployed in a Standard Virtual WAN hub (SKU : Standard): V2V, B2V, V2I and B2I FW policies are only enforced on the traffic originating from the VNets and Branches connected to the specific hub where the Azure FW is deployed (Secured Hub). Traffic originating from remote VNets and Branches that are attached to other Virtual WAN hubs in the same Virtual WAN will not be "firewalled", even though the remote Branches and VNet are interconnected via Virtual WAN hub to hub links. Cross-hub firewalling support is on the Azure Virtual WAN and Firewall Manager roadmap.

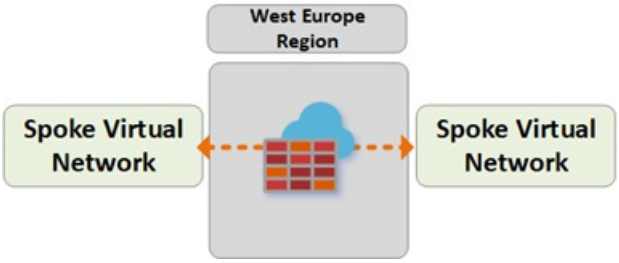
The following paths show the connectivity paths enabled by using Azure secured virtual hubs:

Path 6

Path 6 shows secure traffic flow between VNets within the same region.

The traffic is routed as follows:

- Virtual Networks connected to the same Secured Virtual Hub now route traffic to via the Azure Firewall.
- Azure Firewall can apply policy to these flows.

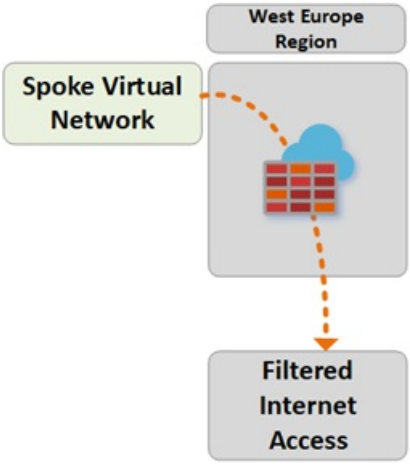


Path 7

Path 7 shows traffic flow from an Azure VNet to the Internet or third-party Security Service.

The traffic is routed as follows:

- Virtual Networks connected to the Secure Virtual Hub can send traffic to public, destinations on the Internet, using the Secure Hub as a central point of Internet access.
- This traffic can be filtered locally using Azure Firewall FQDN rules, or sent to a third-party security service for inspection.

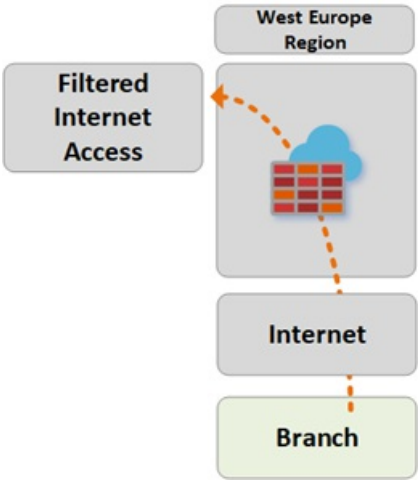


Path 8

Path 8 shows traffic flow from branch-to-Internet or third-party Security Service.

The traffic is routed as follows:

- Branches connected to the Secure Virtual Hub can send traffic to public destinations on the Internet by using the Secure Hub as a central point of Internet access.
- This traffic can be filtered locally using Azure Firewall FQDN rules, or sent to a third-party security service for inspection.



Next steps

Learn more about Azure Virtual WAN

Global transit network architecture and Virtual WAN

2/6/2020 • 7 minutes to read • Edit Online

Modern enterprises require ubiquitous connectivity between hyper-distributed applications, data, and users across the cloud and on-premises. Global transit network architecture is being adopted by enterprises to consolidate, connect, and control the cloud-centric modern, global enterprise IT footprint.

The global transit network architecture is based on a classic hub-and-spoke connectivity model where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.

In this model, a spoke can be:

- Virtual network (VNets)
- Physical branch site
- Remote user
- Internet

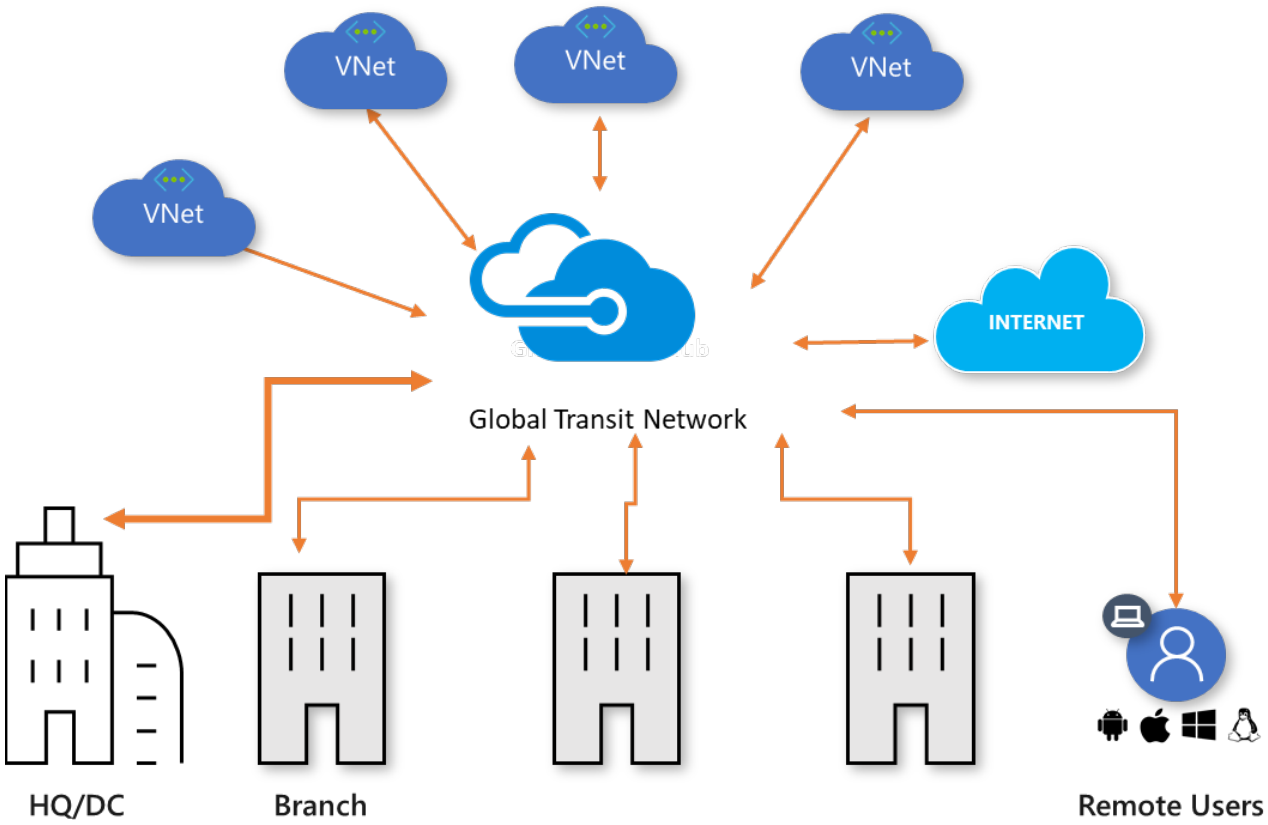


Figure 1: Global transit hub-and-spoke network

Figure 1 shows the logical view of the global transit network where geographically distributed users, physical sites, and VNets are interconnected via a networking hub hosted in the cloud. This architecture enables logical one-hop transit connectivity between the networking endpoints.

Global transit network with Virtual WAN

Azure Virtual WAN is a Microsoft-managed cloud networking service. All the networking components that this service is composed of are hosted and managed by Microsoft. For more information about Virtual WAN, see the Virtual WAN Overview article.

Azure Virtual WAN allows a global transit network architecture by enabling ubiquitous, any-to-any connectivity between globally distributed sets of cloud workloads in VNets, branch sites, SaaS and PaaS applications, and users.

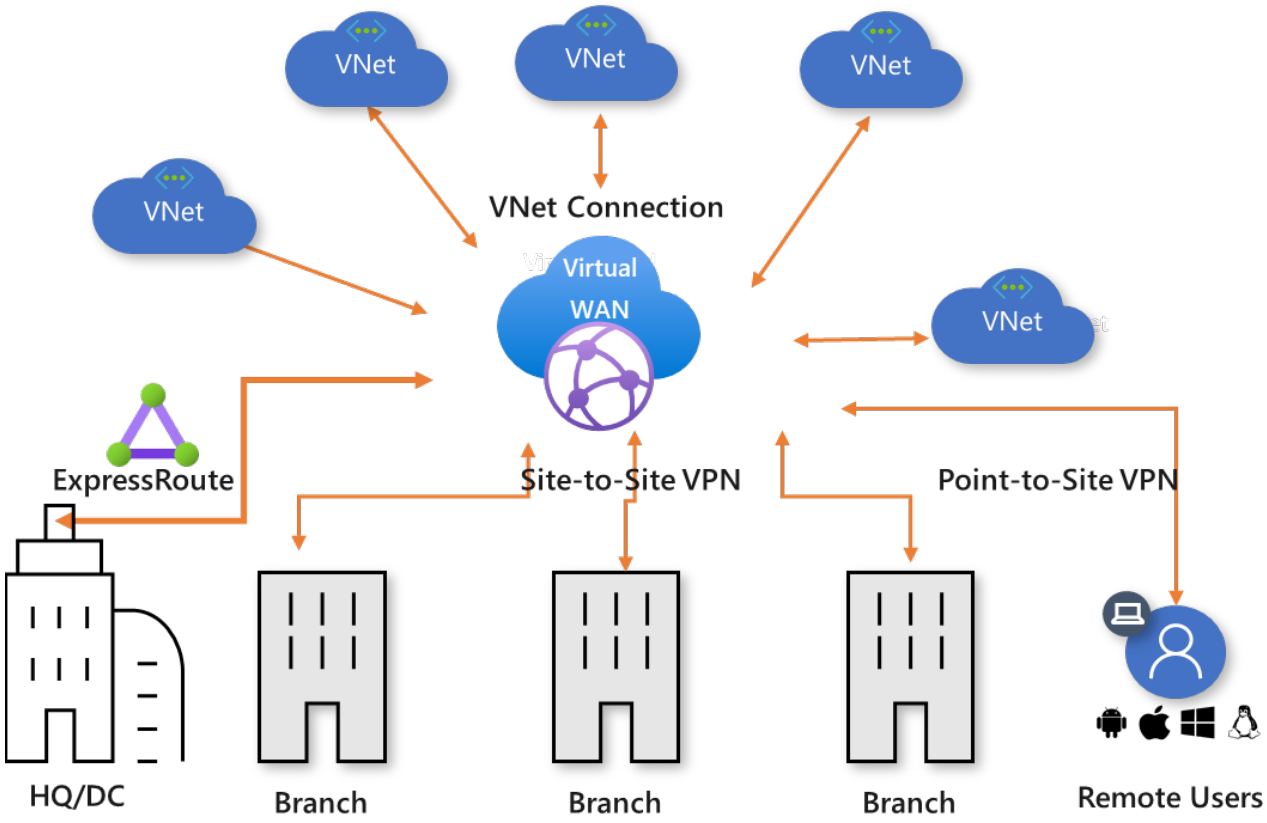


Figure 2: Global transit network and Virtual WAN

In the Azure Virtual WAN architecture, virtual WAN hubs are provisioned in Azure regions, to which you can choose to connect your branches, VNets, and remote users. The physical branch sites are connected to the hub by Premium ExpressRoute or site-to site-VPNs, VNets are connected to the hub by VNet connections, and remote users can directly connect to the hub using User VPN (point-to-site VPNs). Virtual WAN also supports cross-region VNet connection where a VNet in one region can be connected to a virtual WAN hub in a different region.

You can establish a virtual WAN by creating a single virtual WAN hub in the region that has the largest number of spokes (branches, VNets, users), and then connecting the spokes that are in other regions to the hub. This is a good option when an enterprise footprint is mostly in one region with a few remote spokes.

Hub-to-hub connectivity

An Enterprise cloud footprint can span multiple cloud regions and it is optimal (latency-wise) to access the cloud from a region closest to their physical site and users. One of the key principles of global transit network architecture is to enable cross-region connectivity between all cloud and on-premises network endpoints. This means that traffic from a branch that is connected to the cloud in one region can reach another branch or a VNet in a different region using hub-to-hub connectivity enabled by Azure Global Network.

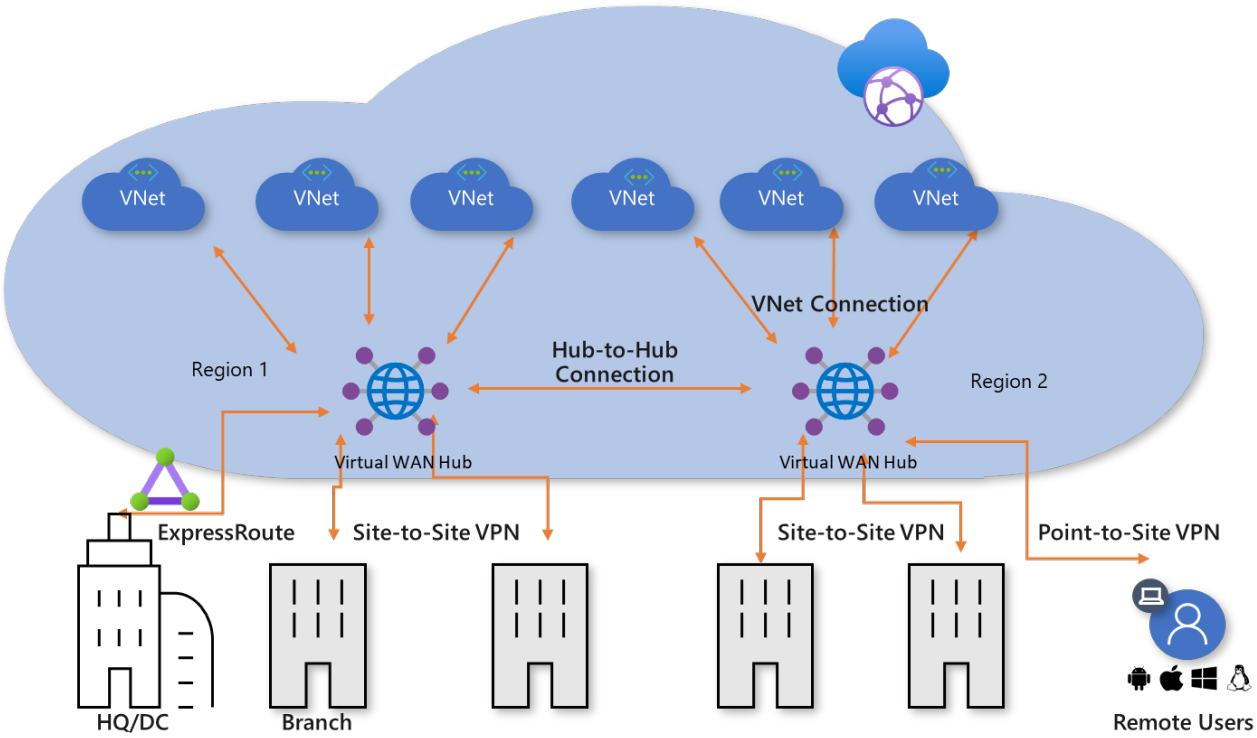


Figure 3: Virtual WAN cross-region connectivity

When multiple hubs are enabled in a single virtual WAN, the hubs are automatically interconnected via hub-to-hub links, thus enabling global connectivity between branches and Vnets that are distributed across multiple regions.

Additionally, hubs that are all part of the same virtual WAN, can be associated with different regional access and security policies. For more information, see Security and policy control later in this article.

Any-to-any connectivity

Global transit network architecture enables any-to-any connectivity via virtual WAN hubs. This architecture eliminates or reduces the need for full mesh or partial mesh connectivity between spokes, that are more complex to build and maintain. In addition, routing control in hub-and-spoke vs. mesh networks is easier to configure and maintain.

Any-to-any connectivity (in the context of a global architecture) allows an enterprise with globally distributed users, branches, datacenters, VNets, and applications to connect to each other through the "transit" hub(s). Azure Virtual WAN acts as the global transit system.

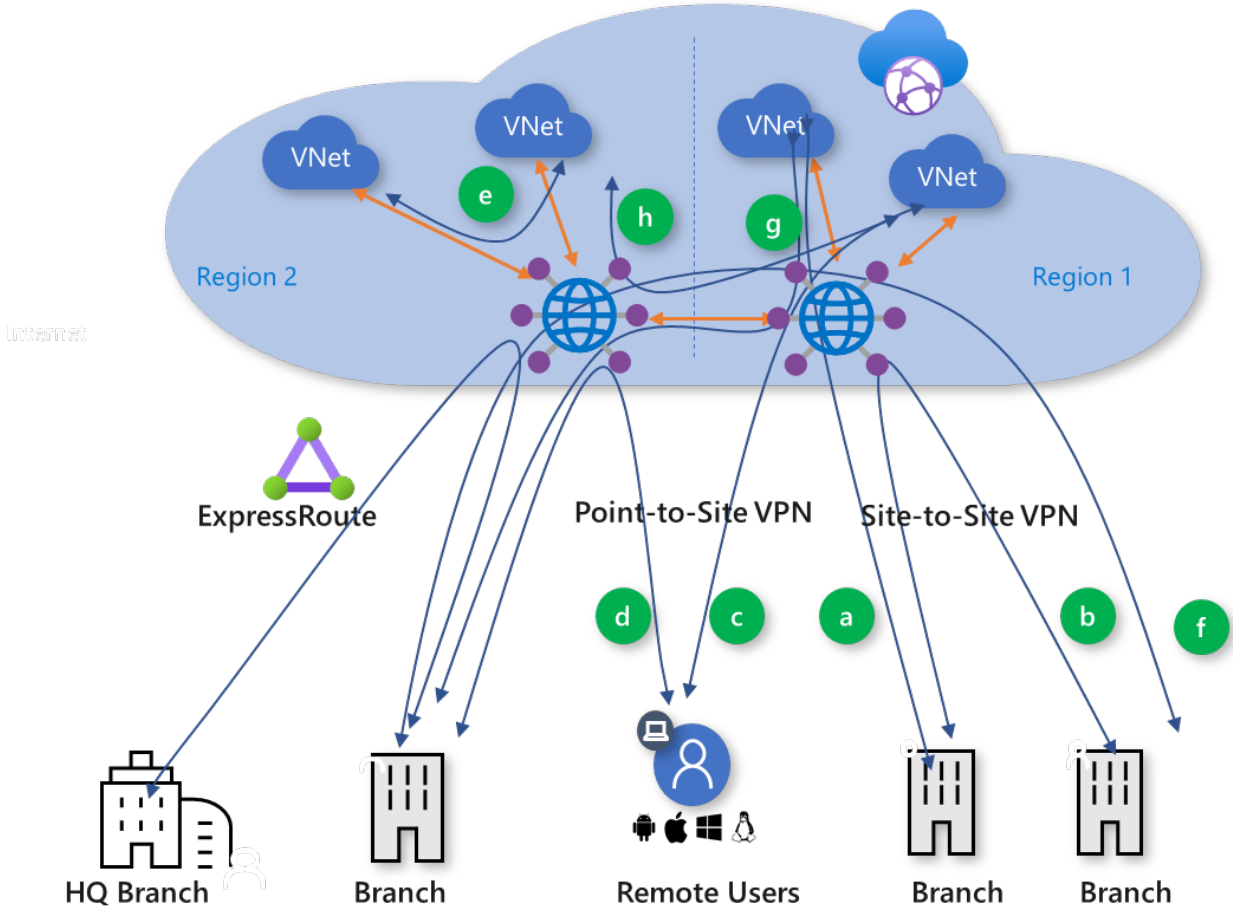


Figure 4: Virtual WAN traffic paths

Azure Virtual WAN supports the following global transit connectivity paths. The letters in parentheses map to Figure 4.

- Branch-to-VNet (a)
- Branch-to-branch (b)
  - ExpressRoute Global Reach and Virtual WAN
- Remote User-to-VNet (c)
- Remote User-to-branch (d)
- VNet-to-VNet (e)
- Branch-to-hub-hub-to-Branch (f)
- Branch-to-hub-hub-to-VNet (g)
- VNet-to-hub-hub-to-VNet (h)

Branch-to-VNet (a) and Branch-to-VNet Cross-region (g)

Branch-to-VNet is the primary path supported by Azure Virtual WAN. This path allows you to connect branches to Azure IAAS enterprise workloads that are deployed in Azure VNets. Branches can be connected to the virtual WAN via ExpressRoute or site-to-site VPN. The traffic transits to VNets that are connected to the virtual WAN hubs via VNet Connections. Explicit gateway transit is not required for Virtual WAN because Virtual WAN automatically enables gateway transit to branch site. See Virtual WAN Partners article on how to connect an SD-WAN CPE to Virtual WAN.

ExpressRoute Global Reach and Virtual WAN

ExpressRoute is a private and resilient way to connect your on-premises networks to the Microsoft Cloud. Virtual WAN supports Express Route circuit connections. Connecting a branch site to Virtual WAN with Express Route requires 1) Premium Circuit 2) Circuit to be in a Global Reach enabled location.

ExpressRoute Global Reach is an add-on feature for ExpressRoute. With Global Reach, you can link ExpressRoute

circuits together to make a private network between your on-premises networks. Branches that are connected to Azure Virtual WAN using ExpressRoute require the ExpressRoute Global Reach to communicate with each other.

In this model, each branch that is connected to the virtual WAN hub using ExpressRoute can connect to VNets using the branch-to-VNet path. Branch-to-branch traffic won't transit the hub because ExpressRoute Global Reach enables a more optimal path over Azure WAN.

Branch-to-branch (b) and Branch-to-Branch cross-region (f)

Branches can be connected to an Azure virtual WAN hub using ExpressRoute circuits and/or site-to-site VPN connections. You can connect the branches to the virtual WAN hub that is in the region closest to the branch.

This option lets enterprises leverage the Azure backbone to connect branches. However, even though this capability is available, you should weigh the benefits of connecting branches over Azure Virtual WAN vs. using a private WAN.

Remote User-to-VNet (c)

You can enable direct, secure remote access to Azure using point-to-site connection from a remote user client to a virtual WAN. Enterprise remote users no longer have to hairpin to the cloud using a corporate VPN.

Remote User-to-branch (d)

The Remote User-to-branch path lets remote users who are using a point-to-site connection to Azure access on-premises workloads and applications by transiting through the cloud. This path gives remote users the flexibility to access workloads that are both deployed in Azure and on-premises. Enterprises can enable central cloud-based secure remote access service in Azure Virtual WAN.

VNet-to-VNet transit (e) and VNet-to-VNet cross-region (h)

The VNet-to-VNet transit enables VNets to connect to each other in order to interconnect multi-tier applications that are implemented across multiple VNets. Optionally, you can connect VNets to each other through VNet Peering and this may be suitable for some scenarios where transit via the VWAN hub is not necessary.

Security and policy control

The Azure Virtual WAN hubs interconnect all the networking end points across the hybrid network and potentially see all transit network traffic. Virtual WAN hubs can be converted to Secured Virtual Hubs by deploying the Azure Firewall inside VWAN hubs to enable cloud-based security, access, and policy control. Orchestration of Azure Firewalls in virtual WAN hubs can be performed by Azure Firewall Manager.

Azure Firewall Manager provides the capabilities to manage and scale security for global transit networks. Azure Firewall Manager provides ability to centrally manage routing, global policy management, advanced Internet security services via third-party along with the Azure Firewall.

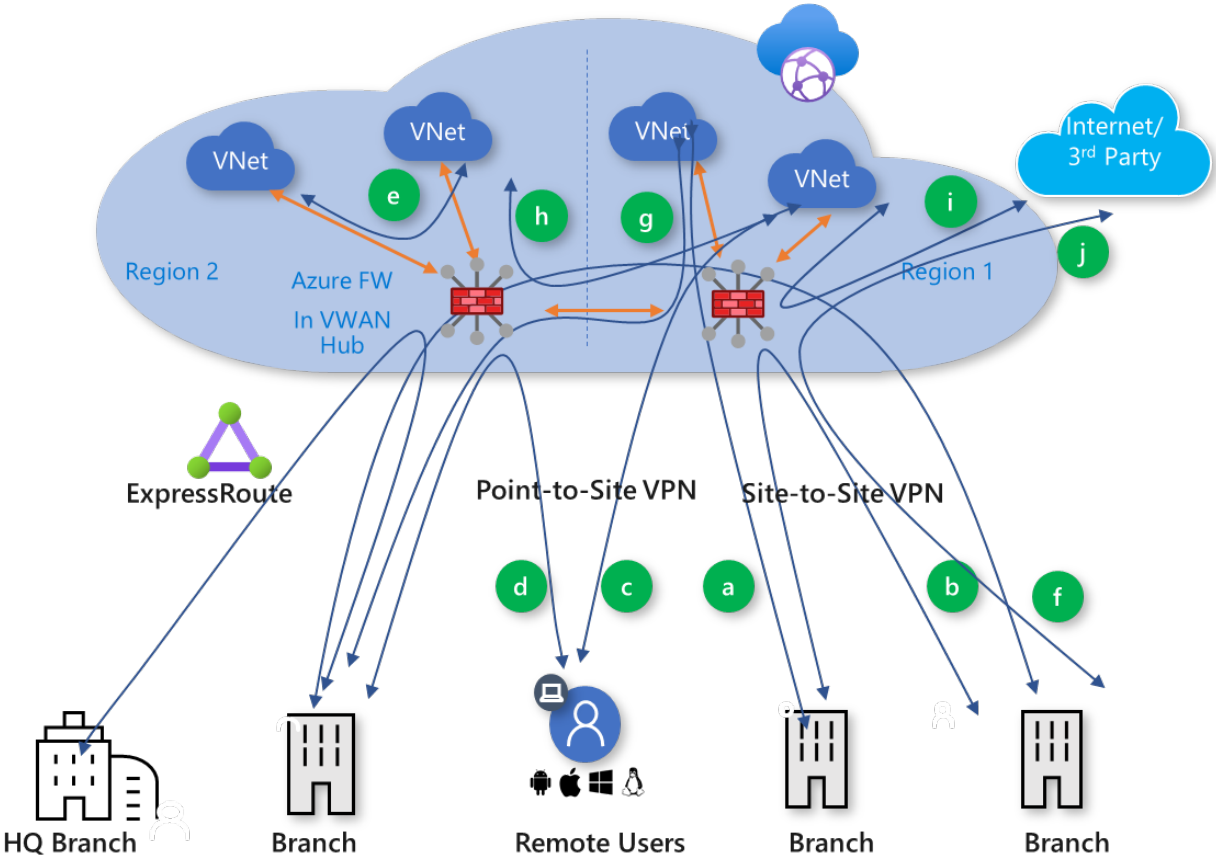


Figure 5: Secured virtual hub with Azure Firewall

Azure Firewall to the virtual WAN supports the following global secured transit connectivity paths. The letters in parentheses map to Figure 5.

- VNet-to-VNet secure transit (e)
- VNet-to-Internet or third-party Security Service (i)
- Branch-to-Internet or third-party Security Service (j)

VNet-to-VNet secured transit (e)

The VNet-to-VNet secured transit enables VNets to connect to each other via the Azure Firewall in the virtual WAN hub.

VNet-to-Internet or third-party Security Service (i)

The VNet-to-Internet or third-party secured transit enables VNets to connect to the internet or a supported third-party security services via the Azure Firewall in the virtual WAN hub.

Branch-to-Internet or third-party Security Service (j)

The branch-to-Internet or third-party Secure transit enables branches to connect to the internet or a supported third-party security services via the Azure Firewall in the virtual WAN hub.

Next steps

Create a connection using Virtual WAN and Deploy Azure Firewall in VWAN hub(s).

- Site-to-site connections using Virtual WAN
- ExpressRoute connections using Virtual WAN
- Azure Firewall Manager to Deploy Azure FW in VWAN

Tutorial: Create a Site-to-Site connection using Azure Virtual WAN

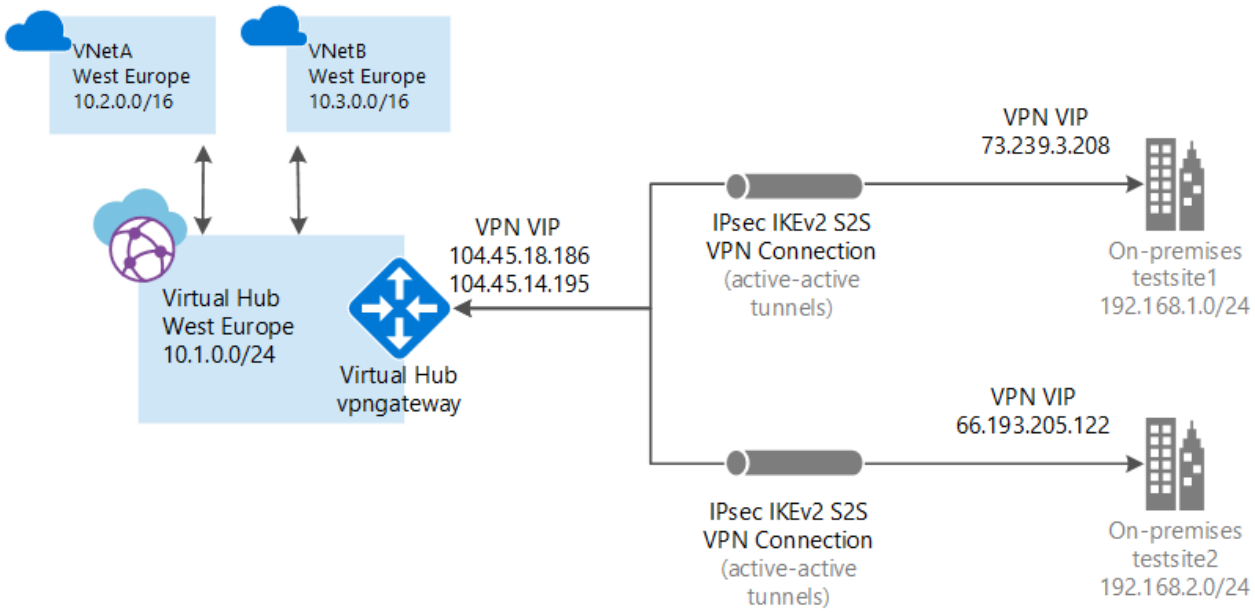
1/27/2020 • 13 minutes to read • Edit Online

This tutorial shows you how to use Virtual WAN to connect to your resources in Azure over an IPsec/IKE (IKEv1 and IKEv2) VPN connection. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it. For more information about Virtual WAN, see the Virtual WAN Overview.

In this tutorial you learn how to:

- Create a virtual WAN
- Create a hub
- Create a site
- Connect a site to a hub
- Connect a VPN site to a hub
- Connect a VNet to a hub
- Download a configuration file
- View your virtual WAN

> **NOTE**
> If you have many sites, you typically would use a Virtual WAN partner to create this configuration. However, you can create this configuration yourself if you are comfortable with networking and proficient at configuring your own VPN device.



Before you begin

Verify that you have met the following criteria before beginning your configuration:

- You have a virtual network that you want to connect to. Verify that none of the subnets of your on-premises networks overlap with the virtual networks that you want to connect to. To create a virtual

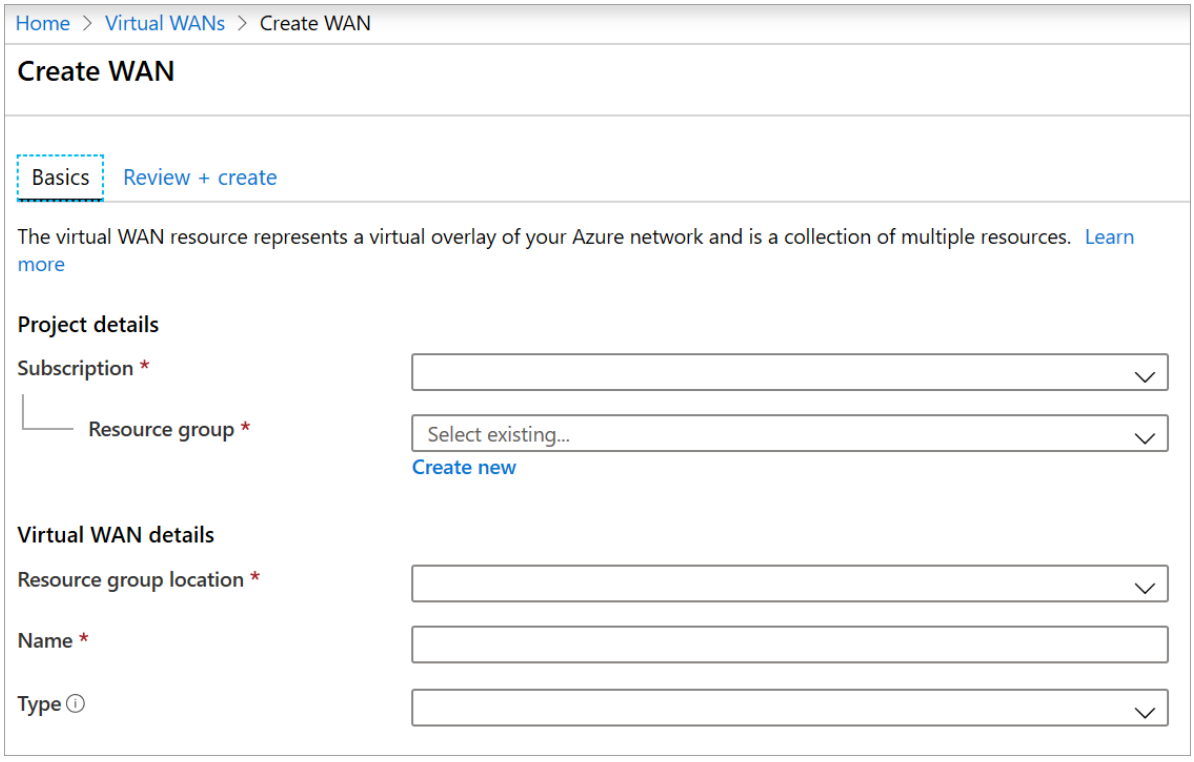
network in the Azure portal, see the Quickstart.

- Your virtual network does not have any virtual network gateways. If your virtual network has a gateway (either VPN or ExpressRoute), you must remove all gateways. This configuration requires that virtual networks are connected instead, to the Virtual WAN hub gateway.
- Obtain an IP address range for your hub region. The hub is a virtual network that is created and used by Virtual WAN. The address range that you specify for the hub cannot overlap with any of your existing virtual networks that you connect to. It also cannot overlap with your address ranges that you connect to on premises. If you are unfamiliar with the IP address ranges located in your on-premises network configuration, coordinate with someone who can provide those details for you.
- If you don't have an Azure subscription, create a free account.

Create a virtual WAN

From a browser, navigate to the Azure portal and sign in with your Azure account.

1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create** to open the Create WAN page.
3. On the **Create WAN** page, on the **Basics** tab, fill in the following fields:



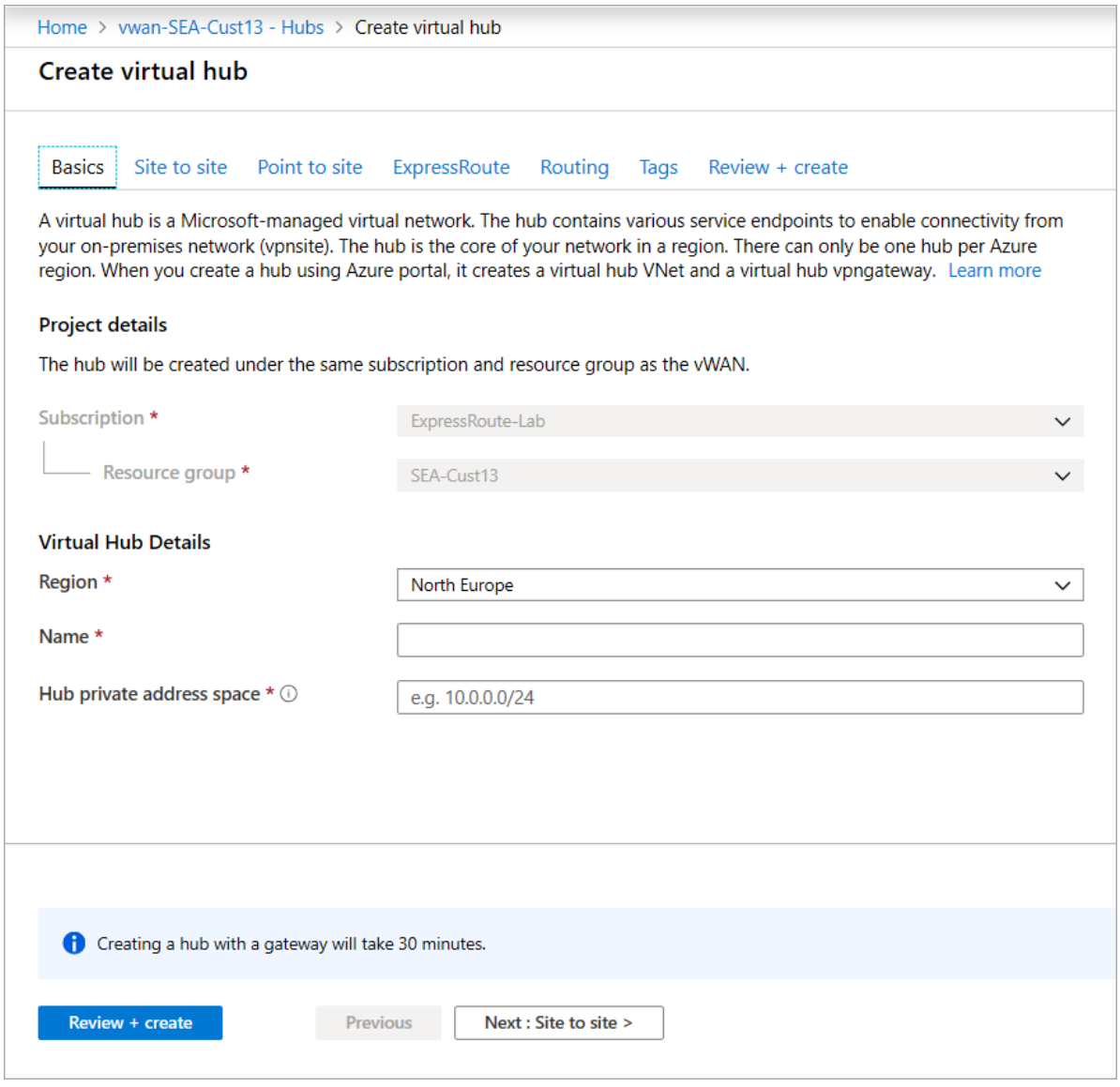
   - **Subscription** - Select the subscription that you want to use.
   - **Resource group** - Create new or use existing.
   - **Resource group location** - Choose a resource location from the dropdown. A WAN is a global resource and does not live in a particular region. However, you must select a region in order to more easily manage and locate the WAN resource that you create.
   - **Name** - Type the Name that you want to call your WAN.
   - **Type:** Basic or Standard. If you create a Basic WAN, you can create only a Basic hub. Basic hubs are capable of VPN site-to-site connectivity only.
4. After you finish filling out the fields, select **Review +Create**.

5. Once validation passes, select **Create** to create the virtual WAN.

Create a hub

A hub is a virtual network that can contain gateways for site-to-site, ExpressRoute, or point-to-site functionality. Once the hub is created, you'll be charged for the hub, even if you don't attach any sites. It takes 30 minutes to create the site-to-site VPN gateway in the virtual hub.

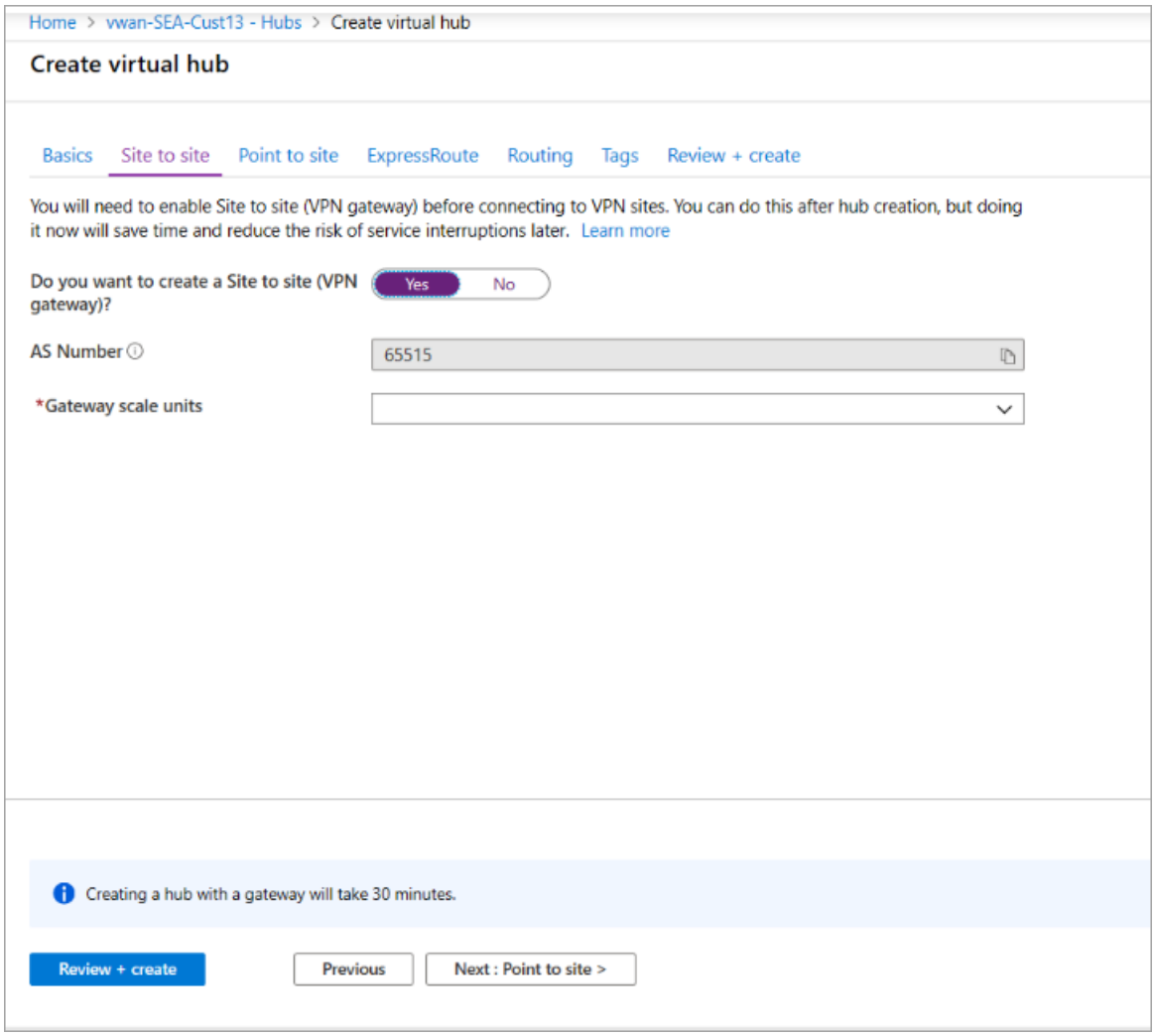
1. Locate the Virtual WAN that you created. On the Virtual WAN page, under the **Connectivity** section, select **Hubs**.
2. On the Hubs page, select **+New Hub** to open the **Create virtual hub** page.



3. On the **Create virtual hub** page **Basics** tab, complete the following fields:

   Project details

   - Region (previously referred to as Location)
   - Name
   - Hub private address space. The minimum address space is /24 to create a hub, which implies anything range from /25 to /32 will produce an error during creation.
4. Select **Next: Site-to-site**.



5. On the **Site-to-site** tab, complete the following fields:

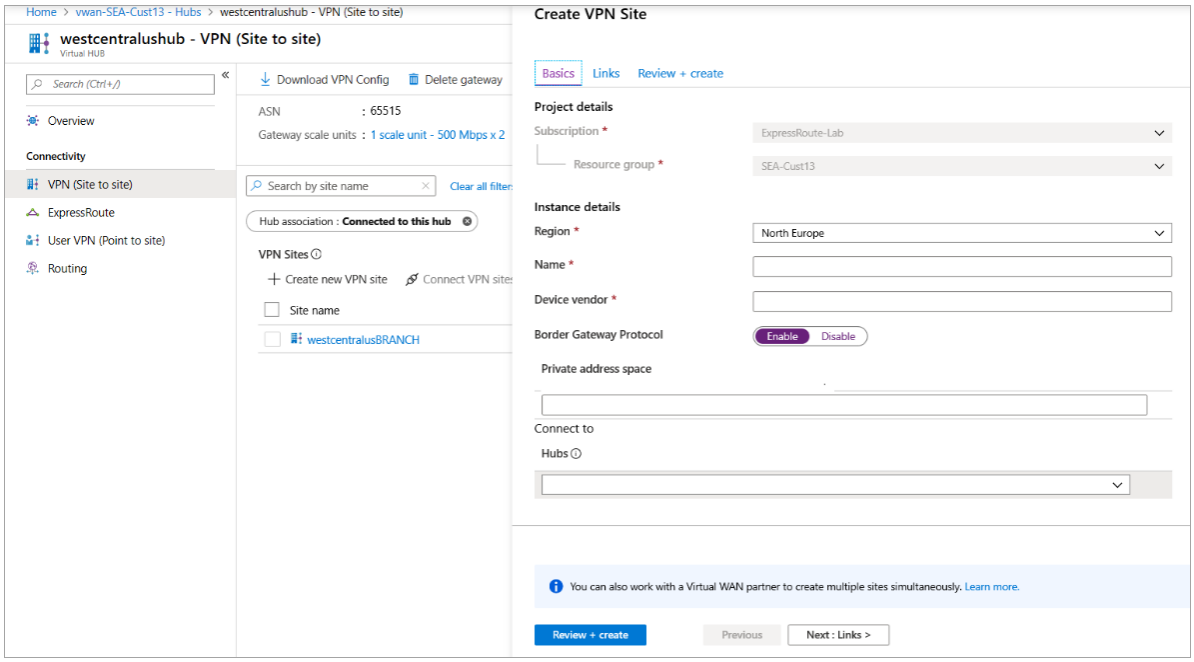
   - Select **Yes** to create a Site-to-site VPN.
   - The AS Number field is not editable in the virtual hub at this time.
   - Select the **Gateway scale units** value from the dropdown. The scale unit lets you pick the aggregate throughput of the VPN gateway being created in the virtual hub to connect sites to. If you pick 1 scale unit = 500 Mbps, it implies that two instances for redundancy will be created, each having a maximum throughput of 500 Mbps. For example, if you had five branches, each doing 10 Mbps at the branch, you will need an aggregate of 50 Mbps at the head end. Planning for aggregate capacity of the Azure VPN gateway should be done after assessing the capacity needed to support the number of branches to the hub.
6. Select **Review + Create** to validate.
7. Select **Create** to create the hub. After 30 minutes, **Refresh** to view the hub on the **Hubs** page. Select **Go to resource** to navigate to the resource.

Create a site

You are now ready to create the sites corresponding to your physical locations. Create as many sites as you need that correspond to your physical locations. For example, if you have a branch office in NY, a branch office in London, and a branch office and LA, you'd create three separate sites. These sites contain your on-premises VPN device endpoints. You can create up to 1000 sites per Virtual Hub in a Virtual WAN. If you had multiple hubs, you can create 1000 per each of those hubs. If you have Virtual WAN partner (link insert) CPE device, check with them to learn about their automation to Azure. Typically automation implies simple click experience to export large-scale branch information into azure and setting up connectivity from the CPE to Azure Virtual WAN VPN gateway. For more information, see Automation guidance from Azure to CPE partners.

1. On the portal page for your virtual wan, in the **Connectivity** section, select **VPN sites** to open the VPN sites page.

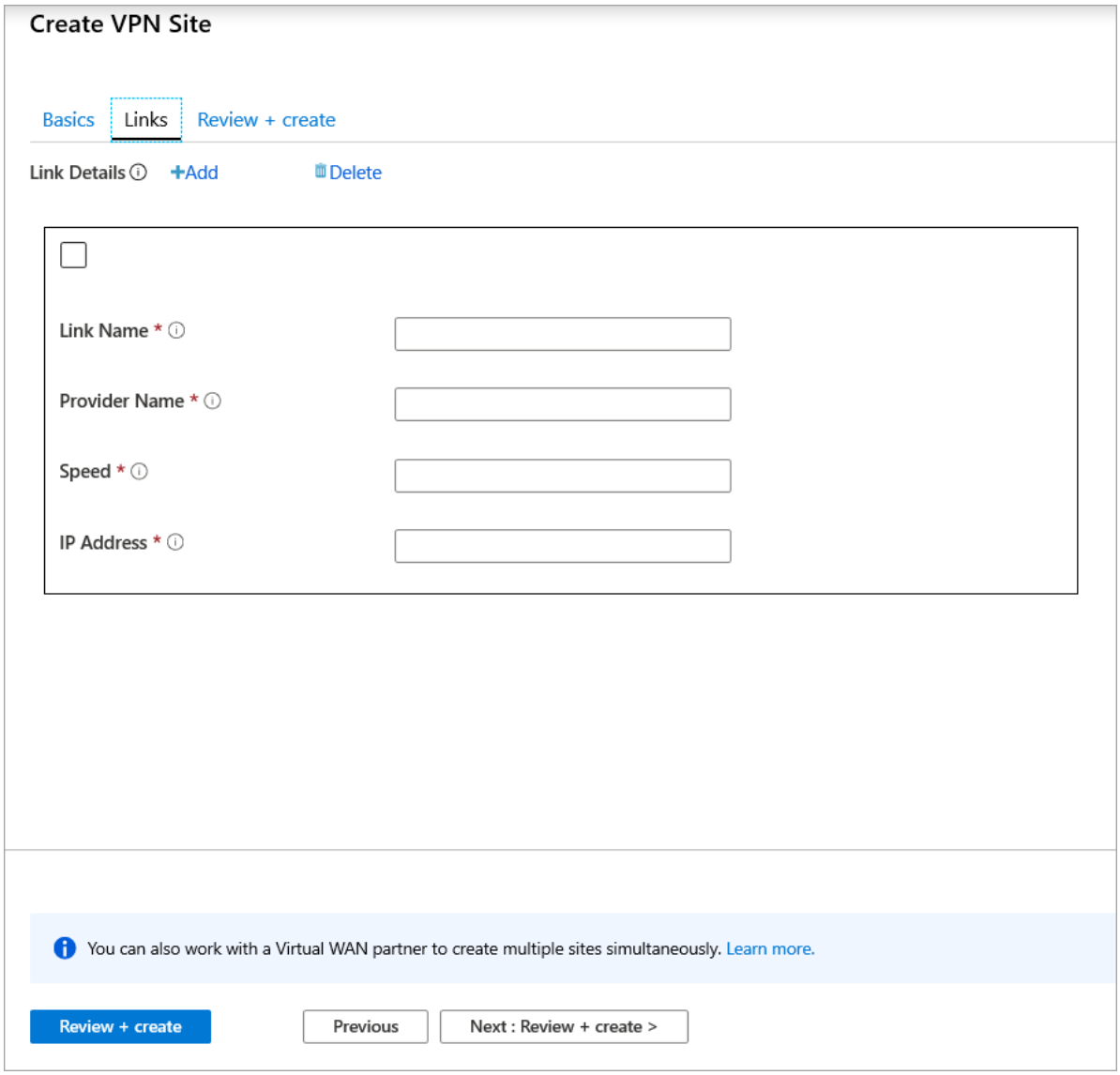
2. On the **VPN sites** page, click **+Create site**.



3. On the **Create VPN Site** page, on the **Basics** tab, complete the following fields:

   - **Region** - Previously referred to as location. This is the location you want to create this site resource in.
   - **Name** - The name by which you want to refer to your on-premises site.
   - **Device vendor** - The name of the VPN device vendor (for example: Citrix, Cisco, Barracuda). Doing so can help the Azure Team better understand your environment to add additional optimization possibilities in the future, or to help you troubleshoot.
   - **Border Gateway Protocol** - Enable implies all connections from the site will be BGP enabled. You will eventually set up the BGP information for each link from the VPN Site in the Links section. Configuring BGP on a Virtual WAN is equivalent to configuring BGP on an Azure virtual network gateway VPN. Your on-premises BGP peer address must not be the same as the public IP address of your VPN to device or the VNet address space of the VPN site. Use a different IP address on the VPN device for your BGP peer IP. It can be an address assigned to the loopback interface on the device. However, it cannot be an APIPA (169.254.x.x) address. Specify this address in the corresponding VPN site representing the location. For BGP prerequisites, see About BGP with Azure VPN Gateway. You can always edit a VPN connection to update its BGP parameters (Peering IP on the link and the AS #) once the VPN Site BGP setting is enabled.
   - **Private address space** - The IP address space that is located on your on-premises site. Traffic destined for this address space is routed to your local site. This is required when BGP is not enabled for the site.
   - **Hubs** - The hub that you want your Site to connect to. A site can only be connected to the hubs that have a VPN Gateway. If you do not see a hub, please create a VPN gateway in that hub first.

4. Select **Links** to add information about the physical links at the branch. If you have a virtual wan partner CPE device, check with them to see if this information is exchanged with Azure as a part of the branch information upload set up from their systems.



- **Link Name** - A name you want to provide for the physical link at the VPN Site. Example: mylink1.
- **Provider Name** - The name of the physical link at the VPN Site. Example: ATT, Verizon.
- **Speed** - This is the speed of the VPN device at the branch location. Example: 50, which means 50 Mbps is the speed of the VPN device at the branch site.
- **IP Address** - Public IP address of the on-prem device using this link. Optionally, you can provide the private IP address of your on-premises VPN device that is behind ExpressRoute.

5. You can use the checkbox to delete or add additional links. Four links per VPN Site are supported. For example, if you have four ISP (Internet service provider) at the branch location, you can create four links. one per each ISP, and provide the information for each link.

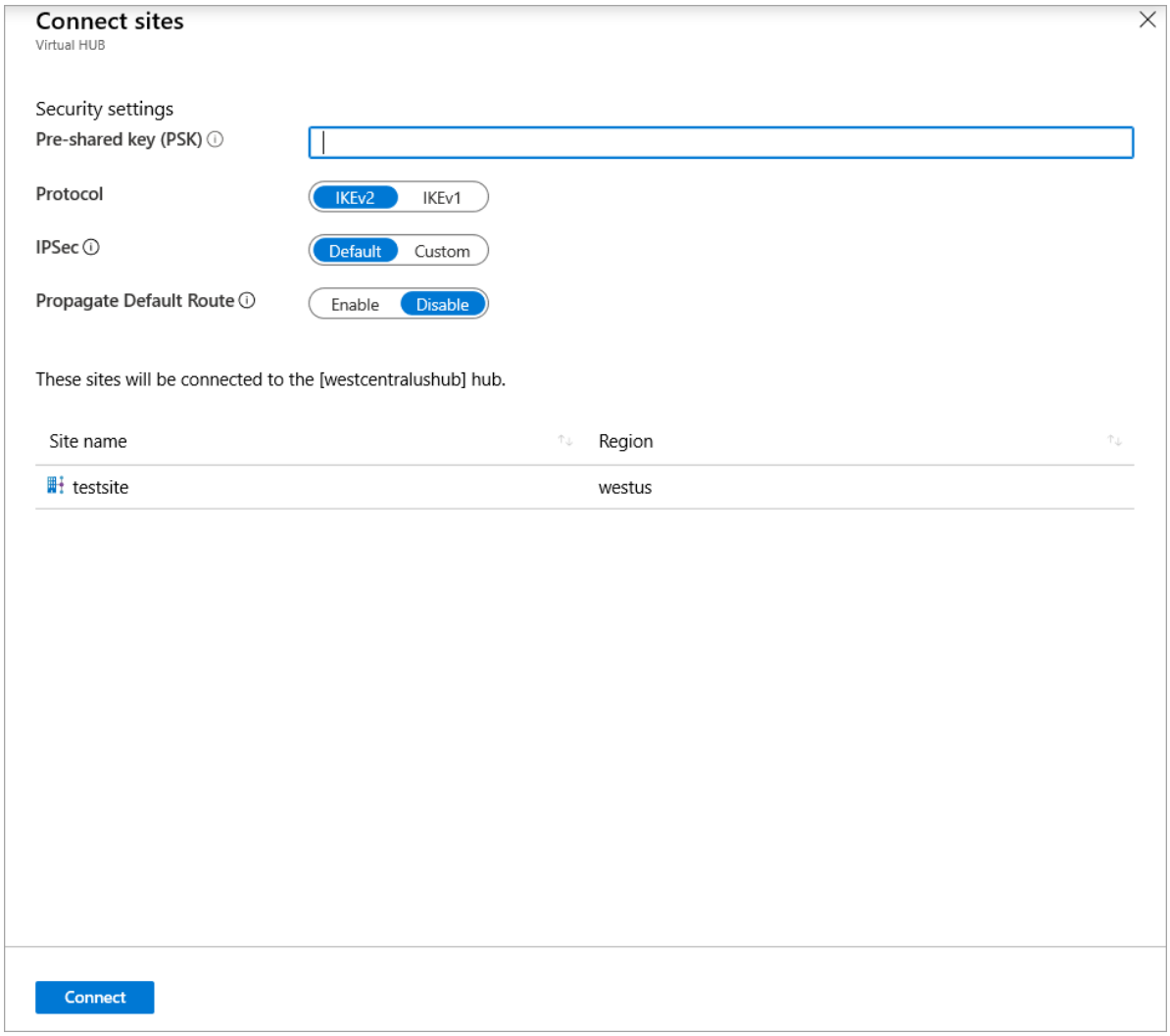
6. Once you have finished filling out the fields, select **Review + create** to verify and create the site.

7. View the status on the VPN sites page. The site will go to **Connection Needed** because the site has not yet been connected to the hub.

Connect the VPN site to the hub

In this step, you connect your VPN site to the hub.

1. Select **Connect VPN Sites** to open the **Connect sites** page.

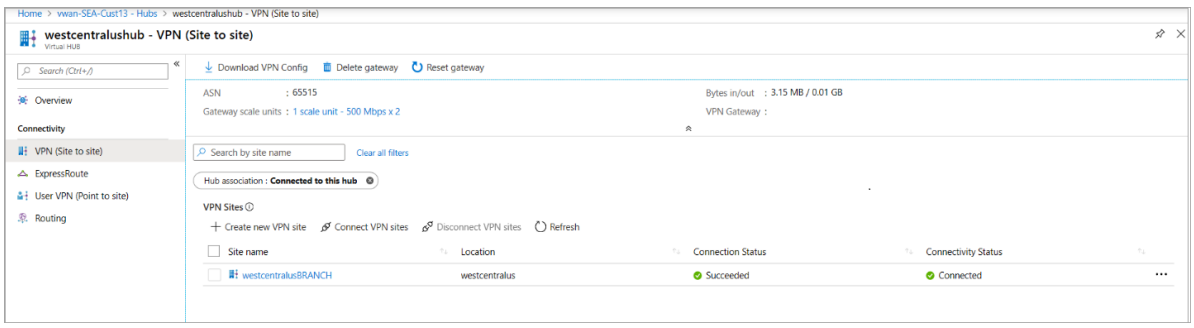


Complete the following fields:

- Enter a pre-shared key. If you don't enter a key, Azure autogenerates one for you.
- Select the Protocol and IPsec settings. Refer to [default/custom IPSec details] (https://docs.microsoft.com/azure/virtual-wan/virtual-wan-ipsec)
- Select the appropriate option for **Propagate Default Route**. The **Enable** option allows the virtual hub to propagate a learned default route to this connection. This flag enables default route propagation to a connection only if the default route is already learned by the Virtual WAN hub as a result of deploying a firewall in the hub, or if another connected site has forced tunneling enabled. The default route does not originate in the Virtual WAN hub.

2. Select **Connect**.

3. In a few minutes, the site will show the connection and connectivity status.



Connection Status: This is the status of the Azure resource for the connection that connects the VPN Site to the Azure hub's VPN gateway. Once this control plane operation is successful, Azure VPN gateway and the on-premises VPN device will proceed to establish connectivity.

Connectivity Status: This is the actual connectivity (data path) status between Azure's VPN gateway in the hub and VPN Site. It can show any of the following states:

- **Unknown**: This state is typically seen if the backend systems are working to transition to another status.
- **Connecting**: Azure VPN gateway is trying to reach out to the actual on-premises VPN site.
- **Connected**: Connectivity is established between Azure VPN gateway and on-premises VPN site.
- **Disconnected**: This status is seen if, for any reason (on-premises or in Azure), the connection was disconnected.

4. Within a hub VPN site, you can additionally do the following:

   - Edit or delete the VPN Connection.
   - Delete the site in the Azure portal.
   - Download a branch-specific configuration for details about the Azure side using the context (...) menu next to the site. If you want to download the configuration for all connected sites in your hub, select **Download VPN Config** on the top menu.

Connect the VNet to the hub

In this step, you create the connection between your hub and a VNet. Repeat these steps for each VNet that you want to connect.

1. On the page for your virtual WAN, click **Virtual network connections**.
2. On the virtual network connection page, click **+Add connection**.
3. On the **Add connection** page, fill in the following fields:

   - **Connection name** - Name your connection.
   - **Hubs** - Select the hub you want to associate with this connection.
   - **Subscription** - Verify the subscription.
   - **Virtual network** - Select the virtual network you want to connect to this hub. The virtual network cannot have an already existing virtual network gateway.

4. Click **OK** to create the virtual network connection.

Download VPN configuration

Use the VPN device configuration to configure your on-premises VPN device.

1. On the page for your virtual WAN, click **Overview**.
2. At the top of the **Hub ->VPNSite** page, click **Download VPN config**. Azure creates a storage account in the resource group 'microsoft-network-[location]', where location is the location of the WAN. After you have applied the configuration to your VPN devices, you can delete this storage account.
3. Once the file has finished creating, you can click the link to download it.
4. Apply the configuration to your on-premises VPN device.

Understanding the VPN device configuration file

The device configuration file contains the settings to use when configuring your on-premises VPN device. When you view this file, notice the following information:

- **vpnSiteConfiguration -** This section denotes the device details set up as a site connecting to the virtual WAN. It includes the name and public ip address of the branch device.
- **vpnSiteConnections -** This section provides information about the following settings:

- **Address space** of the virtual hub(s) VNet
  Example:

  ```
  "AddressSpace":"10.1.0.0/24"
  ```

- **Address space** of the VNets that are connected to the hub
  Example:

  ```
  "ConnectedSubnets":["10.2.0.0/16","10.3.0.0/16"]
  ```

- **IP addresses** of the virtual hub vpngateway. Because each connection of the vpngateway is composed of two tunnels in active-active configuration, you'll see both IP addresses listed in this file. In this example, you see "Instance0" and "Instance1" for each site.
  Example:

  ```
  "Instance0":"104.45.18.186"
  "Instance1":"104.45.13.195"
  ```

- **Vpngateway connection configuration details** such as BGP, pre-shared key etc. The PSK is the pre-shared key that is automatically generated for you. You can always edit the connection in the Overview page for a custom PSK.

Example device configuration file

```
{
    "configurationVersion":{
       "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
       "Version":"r403583d-9c82-4cb8-8570-1cbbcd9983b5"
    },
    "vpnSiteConfiguration":{
       "Name":"testsite1",
       "IPAddress":"73.239.3.208"
    },
    "vpnSiteConnections":[
       {
          "hubConfiguration":{
             "AddressSpace":"10.1.0.0/24",
             "Region":"West Europe",
             "ConnectedSubnets":[
                "10.2.0.0/16",
                "10.3.0.0/16"
             ]
          },
          "gatewayConfiguration":{
             "IpAddresses":{
                "Instance0":"104.45.18.186",
                "Instance1":"104.45.13.195"
             }
          },
          "connectionConfiguration":{
             "IsBgpEnabled":false,
             "PSK":"bkOWe5dPPqkx0DfFE3tyuP7y3oYqAEbI",
             "IPsecParameters":{
                "SADataSizeInKilobytes":102400000,
                "SALifeTimeInSeconds":3600
             }
          }
       }
    ]
 },
```

```
{
   "configurationVersion":{
      "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
      "Version":"1f33f891-e1ab-42b8-8d8c-c024d337bcac"
   },
   "vpnSiteConfiguration":{
      "Name":" testsite2",
      "IPAddress":"66.193.205.122"
   },
   "vpnSiteConnections":[
      {
         "hubConfiguration":{
            "AddressSpace":"10.1.0.0/24",
            "Region":"West Europe"
         },
         "gatewayConfiguration":{
            "IpAddresses":{
               "Instance0":"104.45.18.187",
               "Instance1":"104.45.13.195"
            }
         },
         "connectionConfiguration":{
            "IsBgpEnabled":false,
            "PSK":"XzODPyAYQqFs4ai9WzrJour0qLzeg7Qg",
            "IPsecParameters":{
               "SADataSizeInKilobytes":102400000,
               "SALifeTimeInSeconds":3600
            }
         }
      }
   ]
},
{
   "configurationVersion":{
      "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
      "Version":"cd1e4a23-96bd-43a9-93b5-b51c2a945c7"
   },
   "vpnSiteConfiguration":{
      "Name":" testsite3",
      "IPAddress":"182.71.123.228"
   },
   "vpnSiteConnections":[
      {
         "hubConfiguration":{
            "AddressSpace":"10.1.0.0/24",
            "Region":"West Europe"
         },
         "gatewayConfiguration":{
            "IpAddresses":{
               "Instance0":"104.45.18.187",
               "Instance1":"104.45.13.195"
            }
         },
         "connectionConfiguration":{
            "IsBgpEnabled":false,
            "PSK":"YLkSdSYd4wjjEThR3aIxaXaqNdxUwSo9",
            "IPsecParameters":{
               "SADataSizeInKilobytes":102400000,
               "SALifeTimeInSeconds":3600
            }
         }
      }
   ]
}
```


Configuring your VPN device

> **NOTE**
> If you are working with a Virtual WAN partner solution, VPN device configuration automatically happens. The device controller obtains the configuration file from Azure and applies to the device to set up connection to Azure. This means you don't need to know how to manually configure your VPN device.

If you need instructions to configure your device, you can use the instructions on the VPN device configuration scripts page with the following caveats:

- The instructions on the VPN devices page are not written for Virtual WAN, but you can use the Virtual WAN values from the configuration file to manually configure your VPN device.
- The downloadable device configuration scripts that are for VPN Gateway do not work for Virtual WAN, as the configuration is different.
- A new Virtual WAN can support both IKEv1 and IKEv2.
- Virtual WAN can use both policy based and route-based VPN devices and device instructions.

View your virtual WAN

1. Navigate to the virtual WAN.
2. On the **Overview** page, each point on the map represents a hub. Hover over any point to view the hub health summary, connection status, and bytes in and out.
3. In the Hubs and connections section, you can view hub status, VPN sites, etc. You can click on a specific hub name and navigate to the VPN Site for additional details.

Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

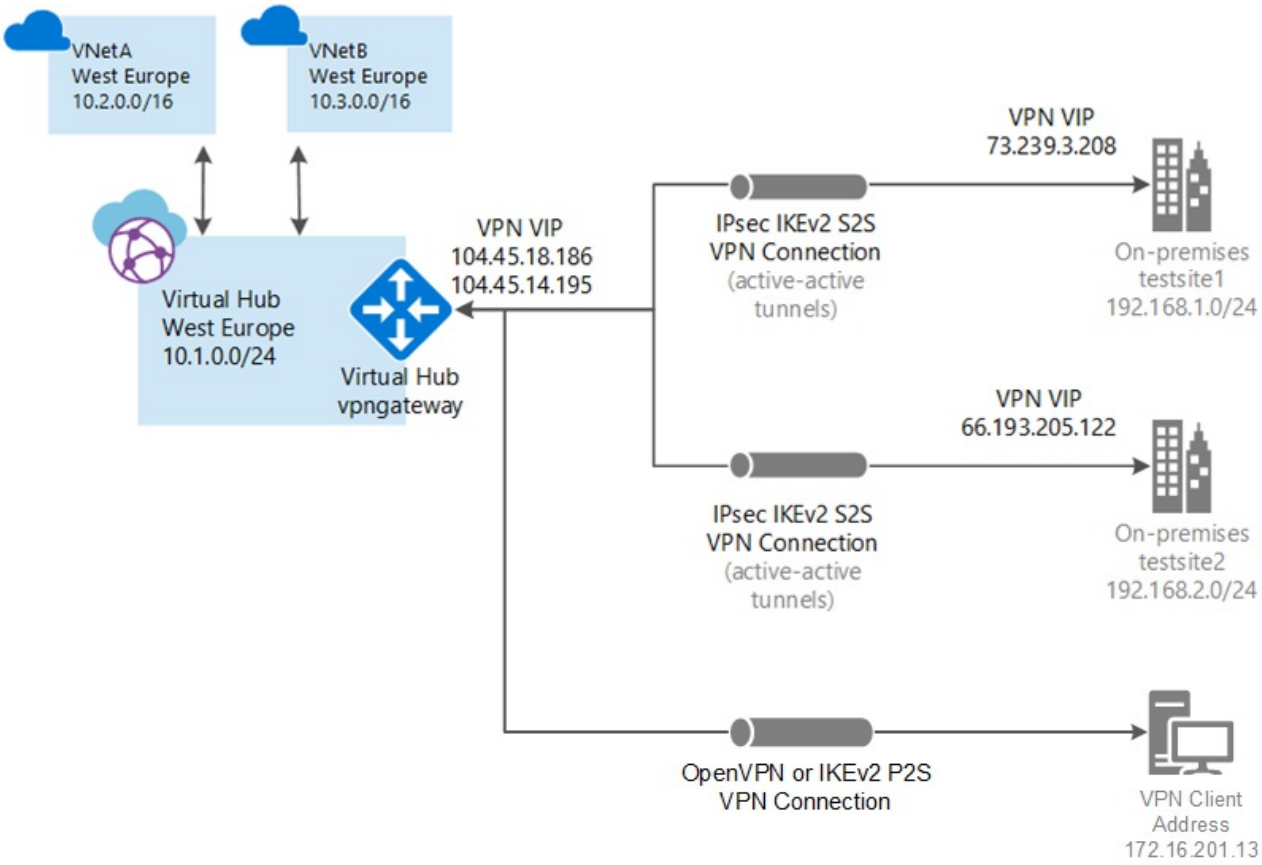
Tutorial: Create a User VPN connection using Azure Virtual WAN

12/16/2019 • 6 minutes to read • Edit Online

This tutorial shows you how to use Virtual WAN to connect to your resources in Azure over an IPsec/IKE (IKEv2) or OpenVPN VPN connection. This type of connection requires a client to be configured on the client computer. For more information about Virtual WAN, see the Virtual WAN Overview

In this tutorial, you learn how to:

- Create a WAN
- Create a hub
- Create a P2S configuration
- Download a VPN client profile
- Apply P2S configuration to a hub
- Connect a VNet to a hub
- Download and apply the VPN client configuration
- View your virtual WAN
- View resource health



Before you begin

Verify that you have met the following criteria before beginning your configuration:

- You have a virtual network that you want to connect to. Verify that none of the subnets of your on-premises networks overlap with the virtual networks that you want to connect to. To create a virtual network in the

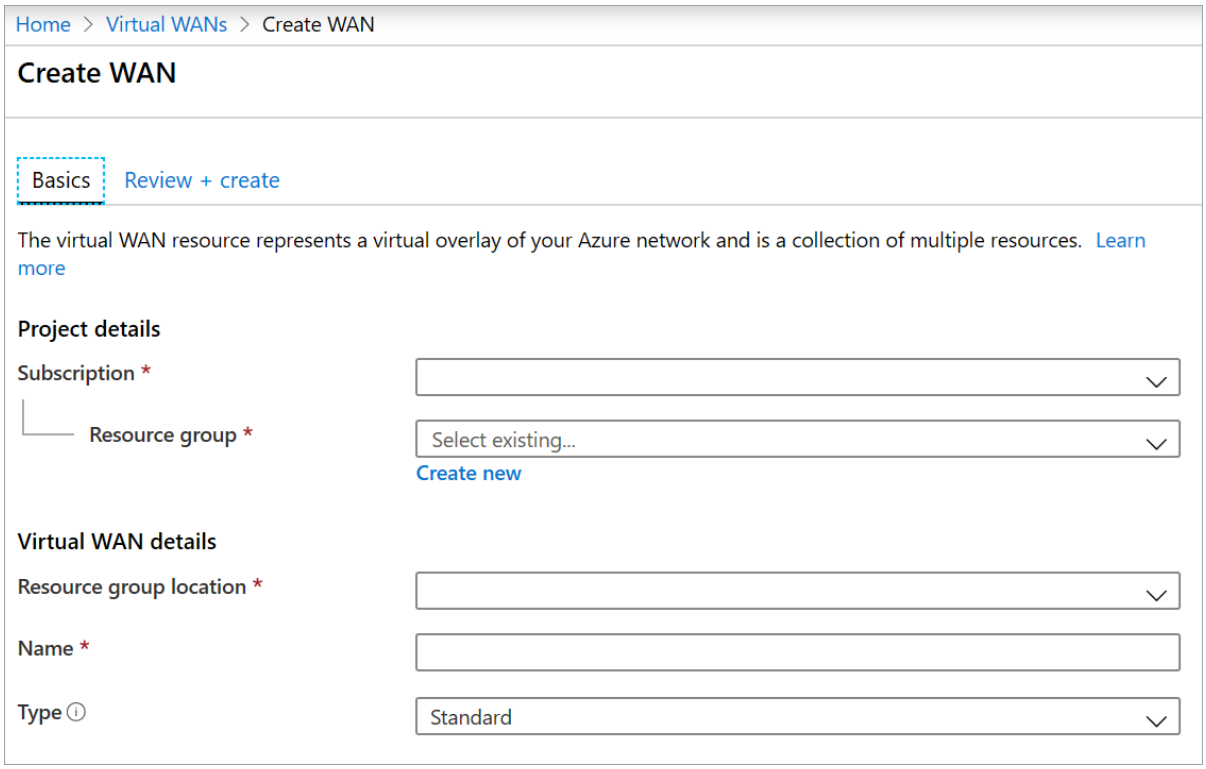
Azure portal, see the Quickstart.

- Your virtual network does not have any virtual network gateways. If your virtual network has a gateway (either VPN or ExpressRoute), you must remove all gateways. This configuration requires that virtual networks are connected instead, to the Virtual WAN hub gateway.
- Obtain an IP address range for your hub region. The hub is a virtual network that is created and used by Virtual WAN. The address range that you specify for the hub cannot overlap with any of your existing virtual networks that you connect to. It also cannot overlap with your address ranges that you connect to on premises. If you are unfamiliar with the IP address ranges located in your on-premises network configuration, coordinate with someone who can provide those details for you.
- If you don't have an Azure subscription, create a free account.

Create a virtual WAN

From a browser, navigate to the Azure portal and sign in with your Azure account.

1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create** to open the Create WAN page.
3. On the **Create WAN** page, on the **Basics** tab, fill in the following fields:



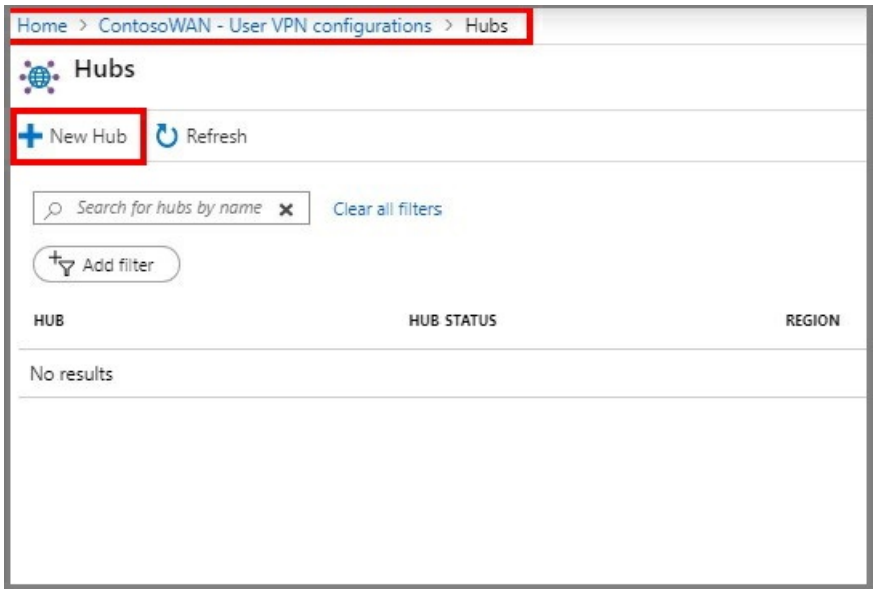
- **Subscription** - Select the subscription that you want to use.
- **Resource group** - Create new or use existing.
- **Resource group location** - Choose a resource location from the dropdown. A WAN is a global resource and does not live in a particular region. However, you must select a region in order to more easily manage and locate the WAN resource that you create.
- **Name** - Type the Name that you want to call your WAN.
- **Type:** Standard. If you create a Basic WAN, you can create only a Basic hub. Basic hubs are capable of VPN site-to-site connectivity only.

4. After you finish filling out the fields, select **Review +Create**.

5. Once validation passes, select **Create** to create the virtual WAN.

Create an empty virtual hub

1. Under your virtual WAN, select Hubs and click **+New Hub**

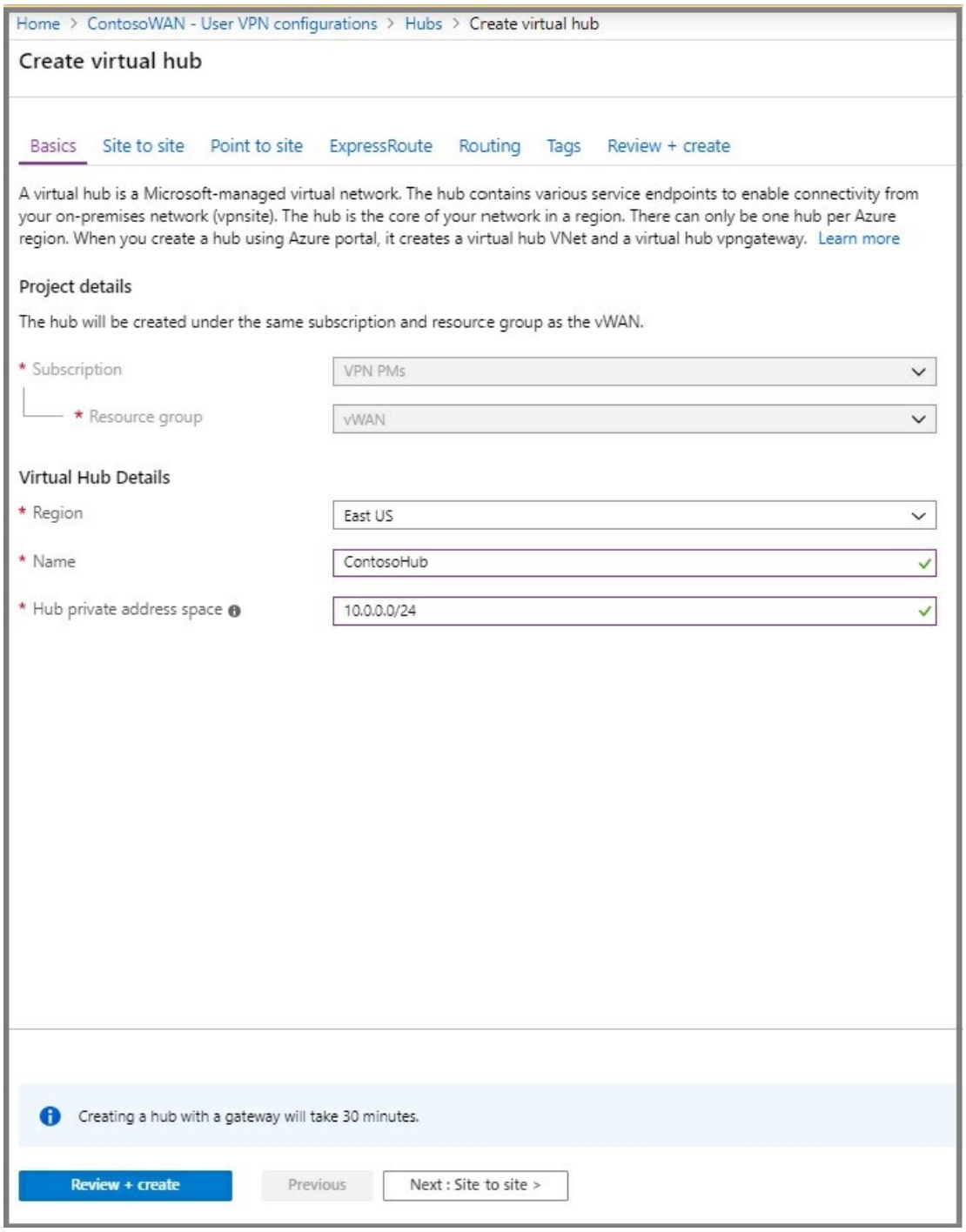


2. On the create virtual hub page, fill in the following fields.

   Region - Select the region that you want to deploy the virtual hub in.

   Name - Enter the name that you want to call your virtual hub.

   Hub private address space - The hub's address range in CIDR notation.

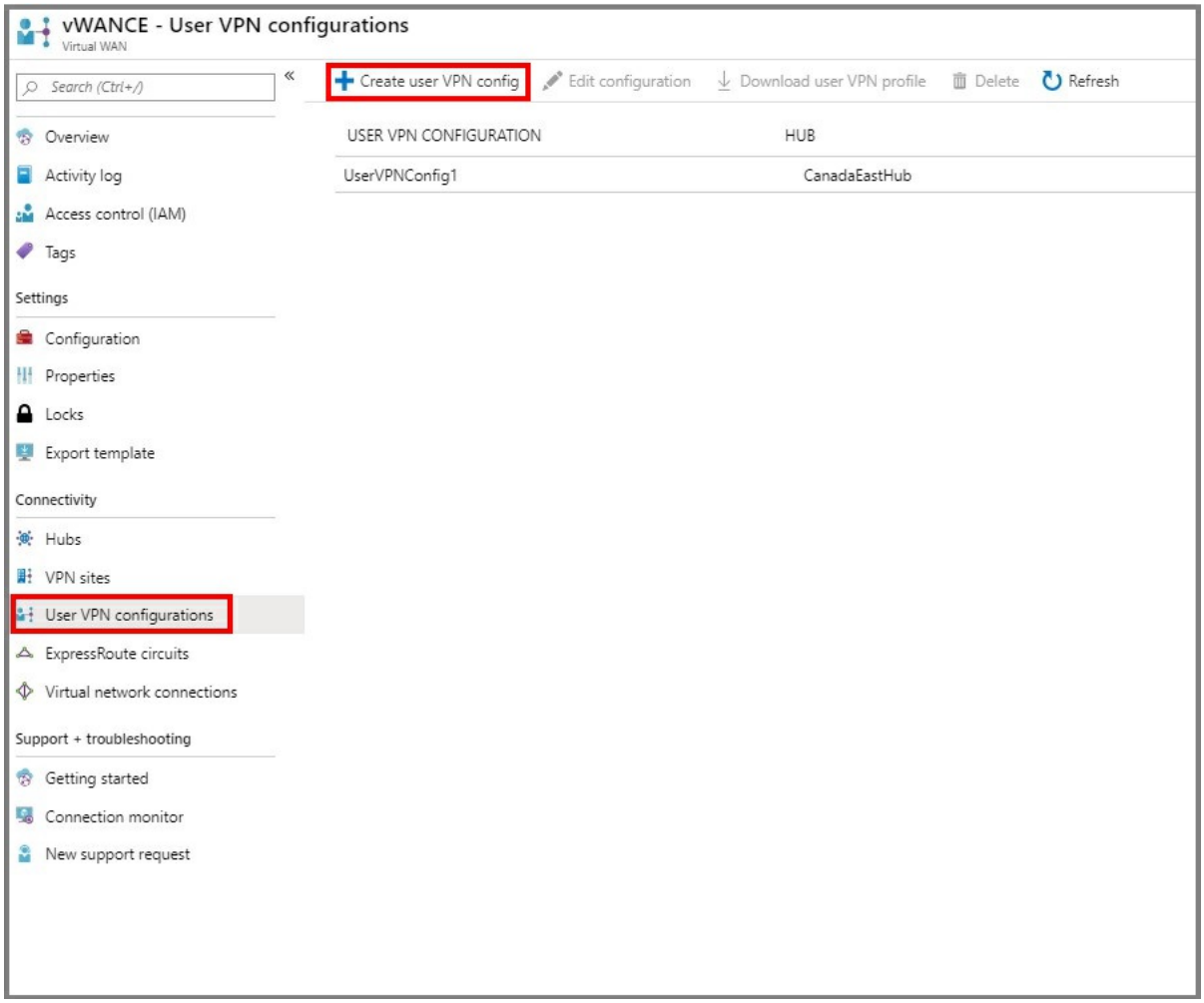


3. Click **Review + create**
4. On the **validation passed** page, click **create**

Create a P2S configuration

A P2S configuration defines the parameters for connecting remote clients.

1. Navigate to **All resources**.
2. Click the virtual WAN that you created.
3. Click **+Create user VPN config** at the top of the page to open the **Create new User VPN configuration** page.



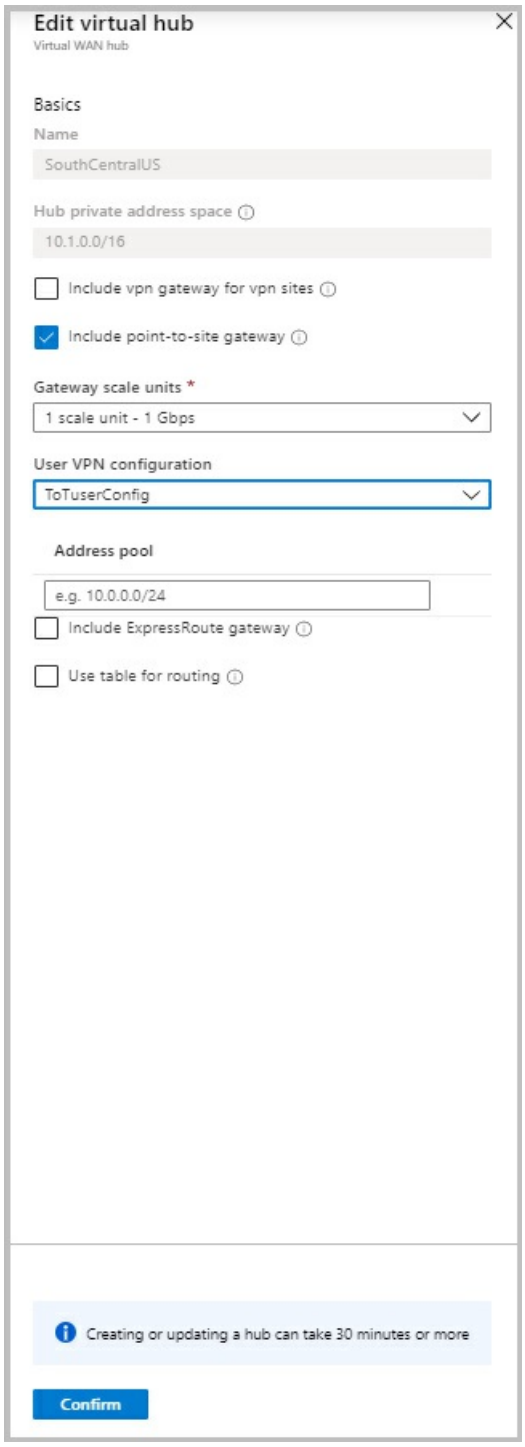
4. On the **Create new user VPN configuration** page, fill in the following fields:

   Configuration name - This is the name by which you want to refer to your configuration.

   Tunnel type - The protocol to use for the tunnel.

   Root Certificate Name - A descriptive name for the certificate.

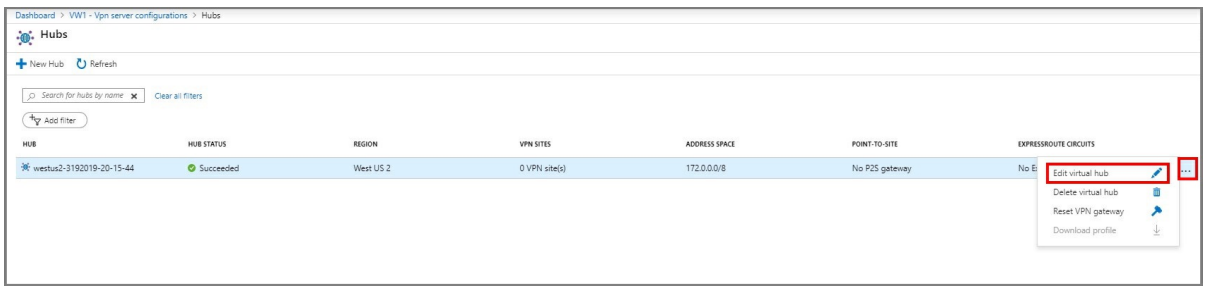
   Public Certificate Data - Base-64 encoded X.509 certificate data.



5. Click **Create** to create the configuration.

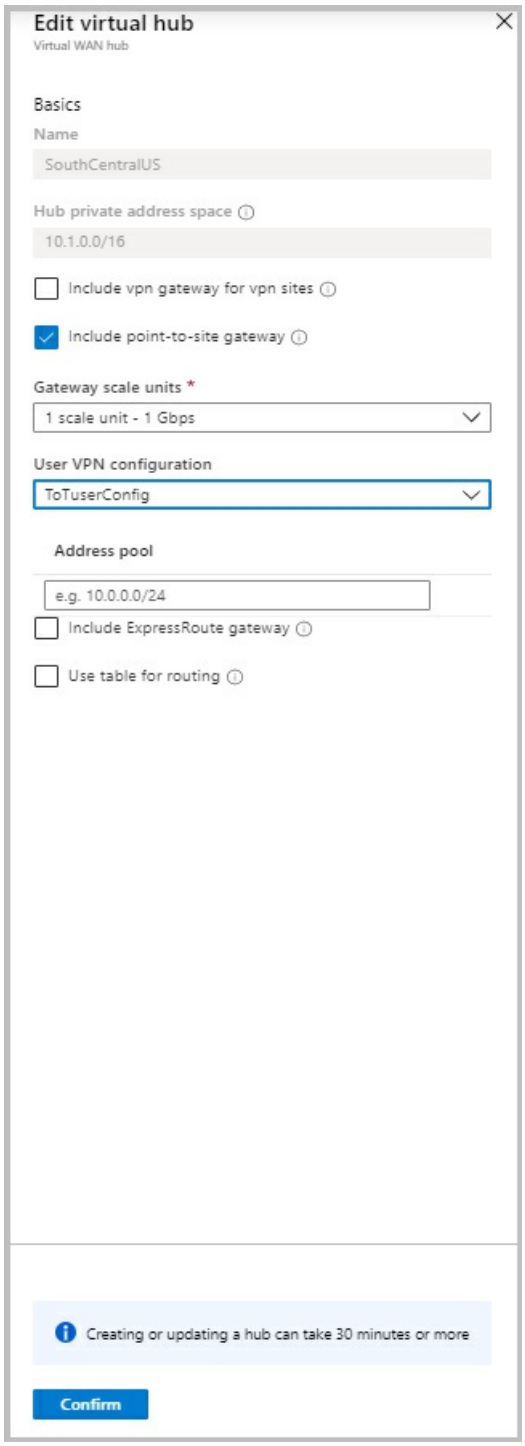
Edit hub assignment

1. Navigate to the **Hubs** blade under the virtual WAN
2. Select the hub that you want to associate the vpn server configuration to and click **...**



3. Click **Edit virtual hub**.

4. Check the **Include point-to-site gateway** check box and pick the **Gateway scale unit** that you want.



5. Enter the **Address pool** from which the VPN clients will be assigned IP addresses.
6. Click **Confirm**
7. The operation will can take up to 30 minutes to complete.

Download VPN profile

Use the VPN profile to configure your clients.

1. On the page for your virtual WAN, click **User VPN configurations**.
2. At the top of the page, click **Download user VPN config**.
3. Once the file has finished creating, you can click the link to download it.
4. Use the profile file to configure the VPN clients.

Configure user VPN clients

Use the downloaded profile to configure the remote access clients. The procedure for each operating system is different, please follow the correct instructions below:

Microsoft Windows

OpenVPN

1. Download and install the OpenVPN client from the official website.
2. Download the VPN profile for the gateway. This can be done from the User VPN configurations tab in Azure portal, or New-AzureRmVpnClientConfiguration in PowerShell.
3. Unzip the profile. Open the vpnconfig.ovpn configuration file from the OpenVPN folder in notepad.
4. Fill in the P2S client certificate section with the P2S client certificate public key in base64. In a PEM formatted certificate, you can simply open the .cer file and copy over the base64 key between the certificate headers. See here how to export a certificate to get the encoded public key.
5. Fill in the private key section with the P2S client certificate private key in base64. See here how to extract private key.
6. Do not change any other fields. Use the filled in configuration in client input to connect to the VPN.
7. Copy the vpnconfig.ovpn file to C:\Program Files\OpenVPN\config folder.
8. Right-click the OpenVPN icon in the system tray and click connect.

IKEv2

1. Select the VPN client configuration files that correspond to the architecture of the Windows computer. For a 64-bit processor architecture, choose the 'VpnClientSetupAmd64' installer package. For a 32-bit processor architecture, choose the 'VpnClientSetupX86' installer package.
2. Double-click the package to install it. If you see a SmartScreen popup, click More info, then Run anyway.
3. On the client computer, navigate to Network Settings and click VPN. The VPN connection shows the name of the virtual network that it connects to.
4. Before you attempt to connect, verify that you have installed a client certificate on the client computer. A client certificate is required for authentication when using the native Azure certificate authentication type. For more information about generating certificates, see Generate Certificates. For information about how to install a client certificate, see Install a client certificate.

View your virtual WAN

1. Navigate to the virtual WAN.
2. On the Overview page, each point on the map represents a hub. Hover over any point to view the hub health summary.
3. In the Hubs and connections section, you can view hub status, site, region, VPN connection status, and bytes in and out.

View your resource health

1. Navigate to your WAN.
2. On your WAN page, in the **SUPPORT + Troubleshooting** section, click **Health** and view your resource.

Clean up resources

When you no longer need these resources, you can use Remove-AzureRmResourceGroup to remove the resource group and all of the resources it contains. Replace "myResourceGroup" with the name of your resource group and run the following PowerShell command:

```
Remove-AzResourceGroup -Name myResourceGroup -Force
```

Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Tutorial: Create an ExpressRoute association using Azure Virtual WAN

2/14/2020 • 6 minutes to read • Edit Online

This tutorial shows you how to use Virtual WAN to connect to your resources in Azure over an ExpressRoute circuit. For more information about Virtual WAN and Virtual WAN resources, see the Virtual WAN Overview.

In this tutorial, you learn how to:

- Create a virtual WAN
- Create a hub and a gateway
- Connect a VNet to a hub
- Connect a circuit to a hub gateway
- Test connectivity
- Change a gateway size
- Advertise a default route

Before you begin

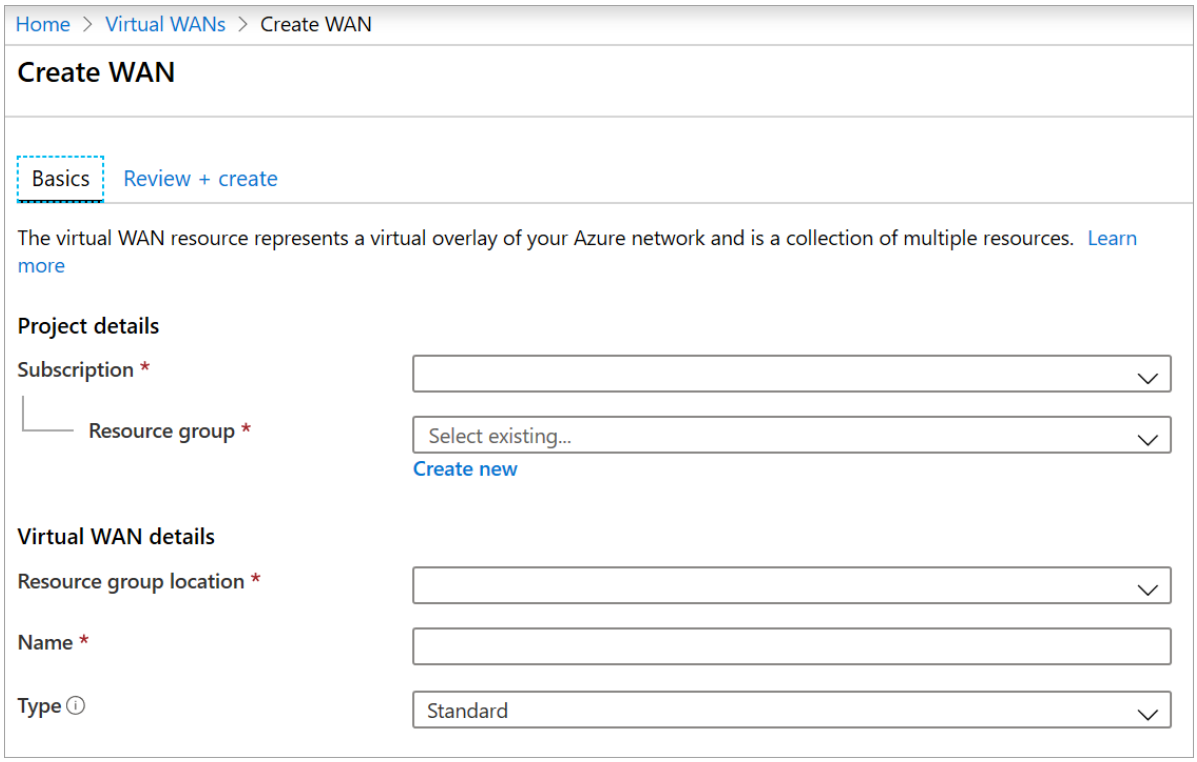
Verify that you have met the following criteria before beginning your configuration:

- You have a virtual network that you want to connect to. Verify that none of the subnets of your on-premises networks overlap with the virtual networks that you want to connect to. To create a virtual network in the Azure portal, see the Quickstart.
- Your virtual network does not have any virtual network gateways. If your virtual network has a gateway (either VPN or ExpressRoute), you must remove all gateways. This configuration requires that virtual networks are connected instead, to the Virtual WAN hub gateway.
- Obtain an IP address range for your hub region. The hub is a virtual network that is created and used by Virtual WAN. The address range that you specify for the hub cannot overlap with any of your existing virtual networks that you connect to. It also cannot overlap with your address ranges that you connect to on premises. If you are unfamiliar with the IP address ranges located in your on-premises network configuration, coordinate with someone who can provide those details for you.
- The ExpressRoute circuit must be a Premium circuit in order to connect to the hub gateway.
- If you don't have an Azure subscription, create a free account.

Create a virtual WAN

From a browser, navigate to the Azure portal and sign in with your Azure account.

1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create** to open the Create WAN page.
3. On the **Create WAN** page, on the **Basics** tab, fill in the following fields:



- **Subscription** - Select the subscription that you want to use.
- **Resource Group** - Create new or use existing.
- **Resource group location** - Choose a resource location from the dropdown. A WAN is a global resource and does not live in a particular region. However, you must select a region in order to more easily manage and locate the WAN resource that you create.
- **Name** - Type the name that you want to call your WAN.
- **Type** - Select **Standard**. You can't create an ExpressRoute gateway using the Basic SKU.

4. After you finish filling out the fields, select **Review +Create**.

5. Once validation passes, select **Create** to create the virtual WAN.

Create a virtual hub and gateway

A virtual hub is a virtual network that is created and used by Virtual WAN. It can contain various gateways, such as VPN and ExpressRoute. In this section, you will create an ExpressRoute gateway for your virtual hub. You can either create the gateway when you create a new virtual hub, or you can create the gateway in an existing hub by editing it.

ExpressRoute gateways are provisioned in units of 2 Gbps. 1 scale unit = 2 Gbps with support up to 10 scale units = 20 Gbps. It takes about 30 minutes for a virtual hub and gateway to fully create.

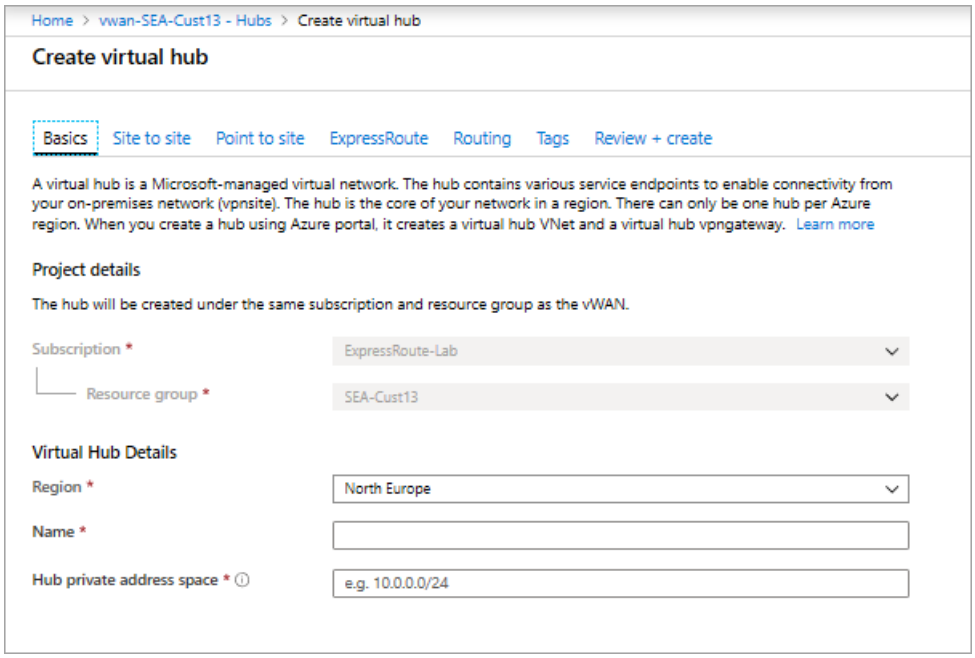
To create a new virtual hub and a gateway

Create a new virtual hub. Once a hub is created, you'll be charged for the hub, even if you don't attach any sites.

1. Locate the Virtual WAN that you created. On the Virtual WAN page, under the **Connectivity** section, select **Hubs**.

2. On the Hubs page, select **+New Hub** to open the **Create virtual hub** page.

3. On the **Create virtual hub** page **Basics** tab, complete the following fields:

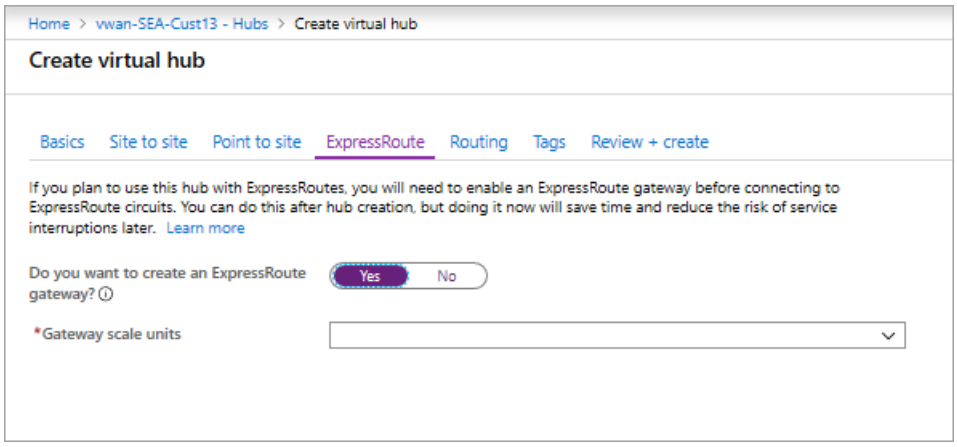


Project details

- Region (previously referred to as Location)
- Name
- Hub private address space. The minimum address space is /24 to create a hub, which implies anything range from /25 to /32 will produce an error during creation.

4. Select the **ExpressRoute tab**.

5. On the **ExpressRoute** tab, complete the following fields:



   - Select **Yes** to create an **ExpressRoute** gateway.
   - Select the **Gateway scale units** value from the dropdown.

6. Select **Review + Create** to validate.

7. Select **Create** to create the hub. After 30 minutes, **Refresh** to view the hub on the **Hubs** page. Select **Go to resource** to navigate to the resource.

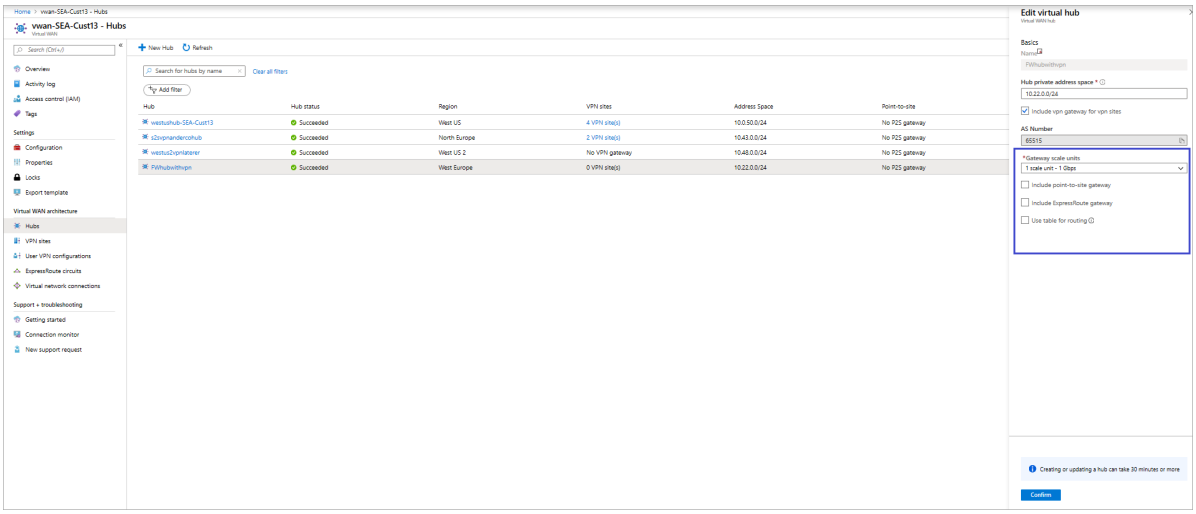
To create a gateway in an existing hub

You can also create a gateway in an existing hub by editing it.

1. Navigate to the virtual hub that you want to edit and select it.

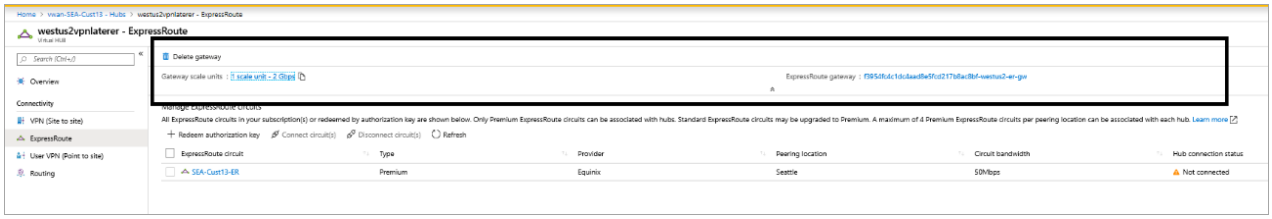
2. On the **Edit virtual hub** page, select the checkbox **Include ExpressRoute gateway**.

3. Select **Confirm** to confirm your changes. It takes about 30 minutes for the hub and hub resources to fully create.



To view a gateway

Once you have created an ExpressRoute gateway, you can view gateway details. Navigate to the hub, select **ExpressRoute**, and view the gateway.



Connect your VNet to the hub

In this section, you create the peering connection between your hub and a VNet. Repeat these steps for each VNet that you want to connect.

1. On the page for your virtual WAN, click **Virtual network connection**.
2. On the virtual network connection page, click **+Add connection**.
3. On the **Add connection** page, fill in the following fields:
   - **Connection name** - Name your connection.
   - **Hubs** - Select the hub you want to associate with this connection.
   - **Subscription** - Verify the subscription.
   - **Virtual network** - Select the virtual network you want to connect to this hub. The virtual network cannot have an already existing virtual network gateway (neither VPN, nor ExpressRoute).

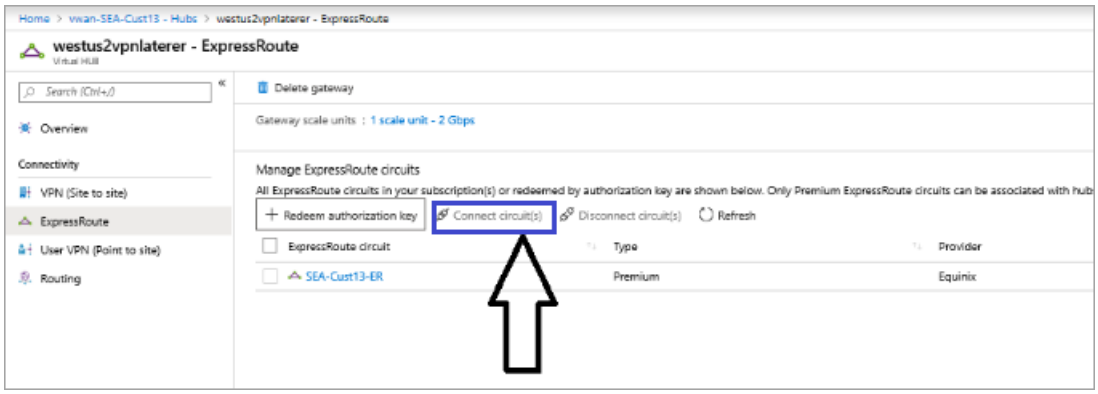
Connect your circuit to the hub gateway

Once the gateway is created, you can connect an ExpressRoute circuit to it. ExpressRoute Premium circuits that are in ExpressRoute Global Reach-supported locations can connect to a Virtual WAN ExpressRoute gateway.

To connect the circuit to the hub gateway

In the portal, go to the **Virtual hub -> Connectivity -> ExpressRoute** page. If you have access in your subscription to an ExpressRoute circuit, you will see the circuit you want to use in the list of circuits. If you don't see any circuits, but have been provided with an authorization key and peer circuit URI, you can redeem and connect a circuit. See To connect by redeeming an authorization key.

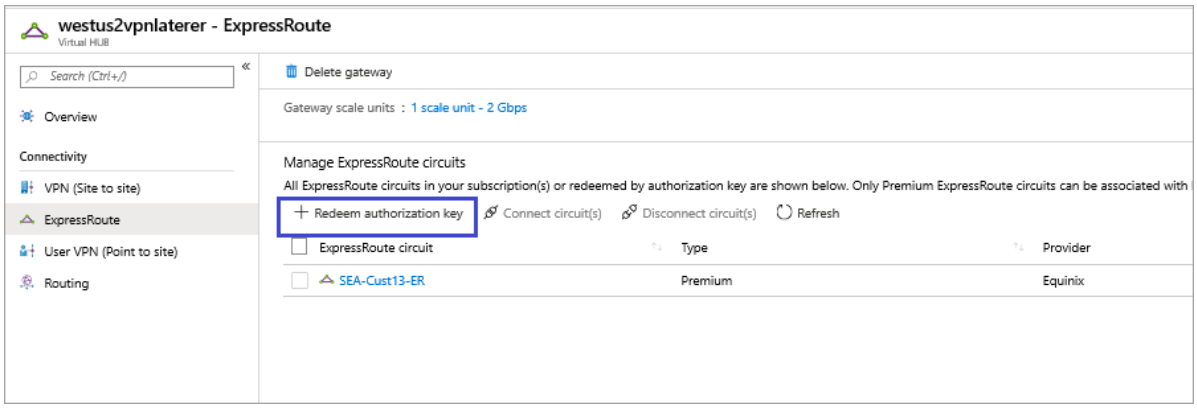
1. Select the circuit.
2. Select **Connect circuit(s)**.



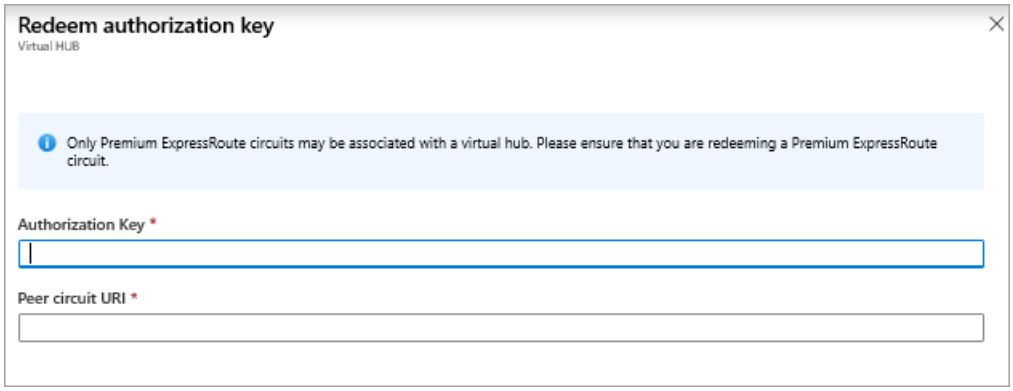
To connect by redeeming an authorization key

Use the authorization key and circuit URI you were provided in order to connect.

1. On the ExpressRoute page, click **+Redeem authorization key**



2. On the Redeem authorization key page, fill in the values.



3. Select **Add** to add the key.

4. View the circuit. A redeemed circuit only shows the name (without the type, provider and other information) because it is in a different subscription than that of the user.

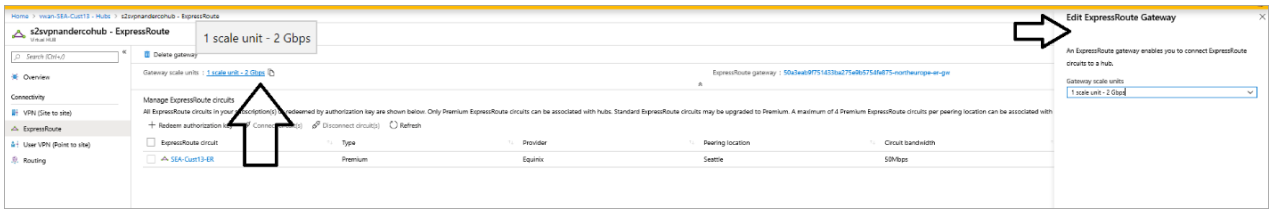
To test connectivity

After the circuit connection is established, the hub connection status will indicate 'this hub', implying the connection is established to the hub ExpressRoute gateway. Wait approximately 5 minutes before you test connectivity from a client behind your ExpressRoute circuit, for example, a VM in the VNet that you created earlier.

If you have sites connected to a Virtual WAN VPN gateway in the same hub as the ExpressRoute gateway, you can have bidirectional connectivity between VPN and ExpressRoute end points. Dynamic routing (BGP) is supported. The ASN of the gateways in the hub is fixed and cannot be edited at this time.

To change the size of a gateway

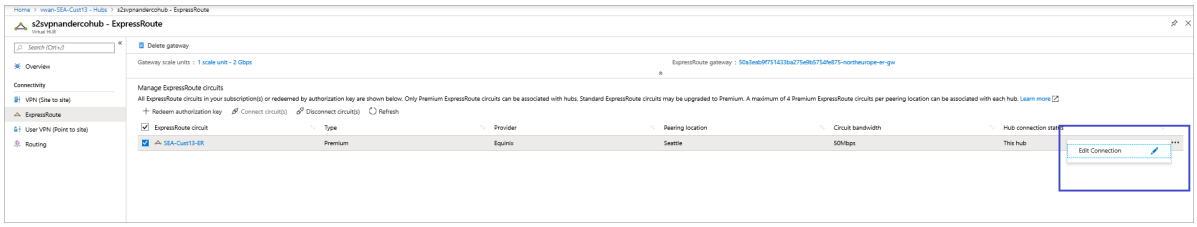
If you want to change the size of your ExpressRoute gateway, locate the ExpressRoute gateway inside the hub, and select the scale units from the dropdown. Save your change. It will take approximately 30 minutes to update the hub gateway.



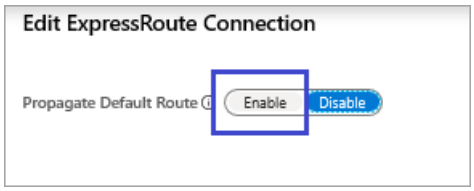
To advertise default route 0.0.0.0/0 to endpoints

If you would like the Azure virtual hub to advertise the default route 0.0.0.0/0 to your ExpressRoute end points, you will need to enable 'Propagate default route'.

1. Select your **Circuit ->...-> Edit connection**.



2. Select **Enable** to propagate the default route.



Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Virtual WAN partners and virtual hub locations

2/12/2020 • 2 minutes to read • Edit Online

This article provides information on Virtual WAN supported regions and partners for connectivity into Virtual Hub.

Azure Virtual WAN is a networking service that provides optimized and automated branch-to-branch connectivity through Azure. Virtual WAN lets you connect and configure branch devices to communicate with Azure. This can be done either manually, or by using provider devices through a Virtual WAN partner. Using partner devices allows you ease of use, simplification of connectivity, and configuration management.

Connectivity from the on-premises device is established in an automated way to the Virtual Hub. A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). You can only have one hub per region.

Automation from connectivity partners

Devices that connect to Azure Virtual WAN have built-in automation to connect. This is typically set up in the device-management UI (or equivalent), which sets up the connectivity and configuration management between the VPN branch device to an Azure Virtual Hub VPN endpoint (VPN gateway).

The following high-level automation is set up in the device console/management center:

- Appropriate permissions for the device to access Azure Virtual WAN Resource Group
- Uploading of Branch Device into Azure Virtual WAN
- Automatic download of Azure connectivity information
- Configuration of on-premises branch device

Some connectivity partners may extend the automation to include creating the Azure Virtual Hub VNet and VPN Gateway. If you want to know more about automation, see Automation guidelines for Virtual WAN partners.

Connectivity through partners

You can check the links in this section for more information about services offered by partners. If your branch device partner is not listed in the section below, have your branch device provider contact us. They can contact us by sending an email to azurevirtualwan@microsoft.com.

PARTNERS
128 Technology
Barracuda Networks
Check Point
Citrix
Cloudgenix
Fortinet

PARTNERS
Netfoundry
Nuage (Nokia)
Palo Alto Networks
Riverbed Technology
Silver-Peak
Versa

The following partners are slated on our roadmap for the near future: Arista, Aruba HPE, Cisco Systems, F5 Networks, Open Systems, Oracle SD-WAN, SharpLink and VMWare Velocloud.

Locations

Azure regions within a geopolitical region

Site-to-site based VPN connectivity and Virtual WAN architecture is available for the following regions:

GEOPOLITICAL REGION	AZURE REGIONS
North America	East US, West US, East US 2, West US 2, Central US, South Central US, North Central US, West Central US, Canada Central, Canada East
South America	Brazil South
Europe	France Central, France South, North Europe, West Europe, UK West, UK South
Asia	East Asia, Southeast Asia
Japan	Japan West, Japan East
Australia	Australia Southeast, Australia East
Australia Government	Australia Central, Australia Central 2
India	India West, India Central, India South
South Korea	Korea Central, Korea South
South Africa	South Africa North, South Africa West

Azure regions and geopolitical boundaries for national clouds

Site-to-site based VPN connectivity and Virtual WAN architecture is available for the following regions:

GEOPOLITICAL REGION	AZURE REGIONS
US Government cloud	US Gov Arizona, US Gov Iowa, US Gov Texas, US Gov Virginia, US DoD Central, US DoD East
China East	China East, China East2
China North	China North, China North2

Next steps

- For more information about Virtual WAN, see the Virtual WAN FAQ.
- For more information about how to automate connectivity to Azure Virtual WAN, see Automation guidelines for Virtual WAN partners.

Automation guidelines for Virtual WAN partners

2/12/2020 • 7 minutes to read • Edit Online

This article helps you understand how to set up the automation environment to connect and configure a branch device (a customer on-premises VPN device or SDWAN CPE) for Azure Virtual WAN. If you are a provider that provides branch devices that can accommodate VPN connectivity over IPsec/IKEv2 or IPsec/IKEv1, this article is for you.

A branch device (a customer on-premises VPN device or SDWAN CPE) typically uses a controller/device dashboard to be provisioned. SD-WAN solution administrators can often use a management console to pre-provision a device before it gets plugged into the network. This VPN capable device gets its control plane logic from a controller. The VPN Device or SD-WAN controller can use Azure APIs to automate connectivity to Azure Virtual WAN. This type of connection requires the on-premises device to have an externally facing public IP address assigned to it.

Before you begin automating

- Verify that your device supports IPsec IKEv1/IKEv2. See default policies.
- View the REST APIs that you use to automate connectivity to Azure Virtual WAN.
- Test out the portal experience of Azure Virtual WAN.
- Then, decide which part of the connectivity steps you would like to automate. At a minimum, we recommend automating:
  - Access Control
  - Upload of branch device information into Azure Virtual WAN
  - Downloading Azure configuration and setting up connectivity from branch device into Azure Virtual WAN

Additional information

- REST API to automate Virtual Hub creation
- REST API to automate Azure VPN gateway for Virtual WAN
- REST API to connect a VPNSite to an Azure VPN Hub
- Default IPsec policies

Customer experience

Understand the expected customer experience in conjunction with Azure Virtual WAN.

1. Typically, a virtual WAN user will start the process by creating a Virtual WAN resource.
2. The user will set up a service principal-based resource group access for the on-premises system (your branch controller or VPN device provisioning software) to write branch info into Azure Virtual WAN.
3. The user may decide at this time to log into your UI and set up the service principal credentials. Once that is complete, your controller should be able to upload branch information with the automation you will provide. The manual equivalent of this on the Azure side is 'Create Site'.
4. Once the Site (branch device) information is available in Azure, the user will connect the site to a hub. A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). The hub is the core of your network in a region. There can only be one hub per Azure region and the vpn endpoint (vpngateway) inside it is created during this

process. The VPN gateway is a scalable gateway which sizes appropriately based on bandwidth and connection needs. You may choose to automate virtual hub and vpngateway creation from your branch device controller dashboard.

5. Once the virtual Hub is associated to the site, a configuration file is generated for the user to manually download. This is where your automation comes in and makes the user experience seamless. Instead of the user having to manually download and configure the branch device, you can set the automation and provide minimal click-through experience on your UI, thereby alleviating typical connectivity issues such as shared key mismatch, IPSec parameter mismatch, configuration file readability etc.
6. At the end of this step in your solution, the user will have a seamless site-to-site connection between the branch device and virtual hub. You can also set up additional connections across other hubs. Each connection is an active-active tunnel. Your customer may choose to use a different ISP for each of the links for the tunnel.
7. Consider providing troubleshooting and monitoring capabilities in the CPE management interface. Typical scenarios include "Customer not able to access Azure resources due to a CPE issue", "Show IPsec parameters at the CPE side" etc.

Automation details

Access control

Customers must be able to set up appropriate access control for Virtual WAN in the device UI. This is recommended using an Azure Service Principal. Service principal-based access provides the device controller appropriate authentication to upload branch information. For more information, see Create service principal. While this functionality is outside of the Azure Virtual WAN offering, we list below the typical steps taken to set up access in Azure after which the relevant details are inputted into the device management dashboard

- Create an Azure Active Directory application for your on-premises device controller.
- Get application ID and authentication key
- Get tenant ID
- Assign application to role "Contributor"

Upload branch device information

You should design the user experience to upload branch (on-premises site) information to Azure. You can use REST APIs for VPNSite to create the site information in Virtual WAN. You can provide all branch SDWAN/VPN devices or select device customizations as appropriate.

Device configuration download and connectivity

This step involves downloading Azure configuration and setting up connectivity from the branch device into Azure Virtual WAN. In this step, a customer that is not using a provider would manually download the Azure configuration and apply it to their on-premises SDWAN/VPN device. As a provider, you should automate this step. View the download REST APIs for additional information. The device controller can call 'GetVpnConfiguration' REST API to download the Azure configuration.

Configuration notes

- If Azure VNets are attached to the virtual hub, they will appear as ConnectedSubnets.
- VPN connectivity uses route-based configuration and supports both IKEv1, and IKEv2 protocols.

Device configuration file

The device configuration file contains the settings to use when configuring your on-premises VPN device. When you view this file, notice the following information:

- **vpnSiteConfiguration -** This section denotes the device details set up as a site connecting to the virtual WAN. It includes the name and public ip address of the branch device.

- **vpnSiteConnections -** This section provides information about the following:
  - **Address space** of the virtual hub(s) VNet.
    Example:

    ```
    "AddressSpace":"10.1.0.0/24"
    ```

  - **Address space** of the VNets that are connected to the hub.
    Example:

    ```
    "ConnectedSubnets":["10.2.0.0/16","10.3.0.0/16"]
    ```

  - **IP addresses** of the virtual hub vpngateway. Because the vpngateway has each connection comprising of 2 tunnels in active-active configuration, you will see both IP addresses listed in this file. In this example, you see "Instance0" and "Instance1" for each site.
    Example:

    ```
    "Instance0":"104.45.18.186"
    "Instance1":"104.45.13.195"
    ```

  - **Vpngateway connection configuration details** such as BGP, pre-shared key etc. The PSK is the pre-shared key that is automatically generated for you. You can always edit the connection in the Overview page for a custom PSK.

Example device configuration file

```
{
    "configurationVersion":{
       "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
       "Version":"r403583d-9c82-4cb8-8570-1cbbcd9983b5"
    },
    "vpnSiteConfiguration":{
       "Name":"testsite1",
       "IPAddress":"73.239.3.208"
    },
    "vpnSiteConnections":[
       {
          "hubConfiguration":{
             "AddressSpace":"10.1.0.0/24",
             "Region":"West Europe",
             "ConnectedSubnets":[
                "10.2.0.0/16",
                "10.3.0.0/16"
             ]
          },
          "gatewayConfiguration":{
             "IpAddresses":{
                "Instance0":"104.45.18.186",
                "Instance1":"104.45.13.195"
             }
          },
          "connectionConfiguration":{
             "IsBgpEnabled":false,
             "PSK":"bkOWe5dPPqkx0DfFE3tyuP7y3oYqAEbI",
             "IPsecParameters":{
                "SADataSizeInKilobytes":102400000,
                "SALifeTimeInSeconds":3600
             }
          }
       }
```

```
    ]
  },
  {
    "configurationVersion":{
       "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
       "Version":"1f33f891-e1ab-42b8-8d8c-c024d337bcac"
    },
    "vpnSiteConfiguration":{
       "Name":" testsite2",
       "IPAddress":"66.193.205.122"
    },
    "vpnSiteConnections":[
       {
          "hubConfiguration":{
             "AddressSpace":"10.1.0.0/24",
             "Region":"West Europe"
          },
          "gatewayConfiguration":{
             "IpAddresses":{
                "Instance0":"104.45.18.187",
                "Instance1":"104.45.13.195"
             }
          },
          "connectionConfiguration":{
             "IsBgpEnabled":false,
             "PSK":"XzODPyAYQqFs4ai9WzrJour0qLzeg7Qg",
             "IPsecParameters":{
                "SADataSizeInKilobytes":102400000,
                "SALifeTimeInSeconds":3600
             }
          }
       }
    ]
  },
  {
    "configurationVersion":{
       "LastUpdatedTime":"2018-07-03T18:29:49.8405161Z",
       "Version":"cd1e4a23-96bd-43a9-93b5-b51c2a945c7"
    },
    "vpnSiteConfiguration":{
       "Name":" testsite3",
       "IPAddress":"182.71.123.228"
    },
    "vpnSiteConnections":[
       {
          "hubConfiguration":{
             "AddressSpace":"10.1.0.0/24",
             "Region":"West Europe"
          },
          "gatewayConfiguration":{
             "IpAddresses":{
                "Instance0":"104.45.18.187",
                "Instance1":"104.45.13.195"
             }
          },
          "connectionConfiguration":{
             "IsBgpEnabled":false,
             "PSK":"YLkSdSYd4wjjEThR3aIxaXaqNdxUwSo9",
             "IPsecParameters":{
                "SADataSizeInKilobytes":102400000,
                "SALifeTimeInSeconds":3600
             }
          }
       }
    ]
  }
```

Connectivity details

Your on-premises SDWAN/VPN device or SD-WAN configuration must match or contain the following algorithms and parameters, which you specify in the Azure IPsec/IKE policy.

- IKE encryption algorithm
- IKE integrity algorithm
- DH Group
- IPsec encryption algorithm
- IPsec integrity algorithm
- PFS Group

Default policies for IPsec connectivity

> **NOTE**
> When working with Default policies, Azure can act as both initiator and responder during an IPsec tunnel setup. There is no support for Azure as a responder only.

Initiator

The following sections list the supported policy combinations when Azure is the initiator for the tunnel.

Phase-1

- AES_256, SHA1, DH_GROUP_2
- AES_256, SHA_256, DH_GROUP_2
- AES_128, SHA1, DH_GROUP_2
- AES_128, SHA_256, DH_GROUP_2

Phase-2

- GCM_AES_256, GCM_AES_256, PFS_NONE
- AES_256, SHA_1, PFS_NONE
- AES_256, SHA_256, PFS_NONE
- AES_128, SHA_1, PFS_NONE

Responder

The following sections list the supported policy combinations when Azure is the responder for the tunnel.

Phase-1

- AES_256, SHA1, DH_GROUP_2
- AES_256, SHA_256, DH_GROUP_2
- AES_128, SHA1, DH_GROUP_2
- AES_128, SHA_256, DH_GROUP_2

Phase-2

- GCM_AES_256, GCM_AES_256, PFS_NONE
- AES_256, SHA_1, PFS_NONE
- AES_256, SHA_256, PFS_NONE
- AES_128, SHA_1, PFS_NONE
- AES_256, SHA_1, PFS_1
- AES_256, SHA_1, PFS_2

- AES_256, SHA_1, PFS_14
- AES_128, SHA_1, PFS_1
- AES_128, SHA_1, PFS_2
- AES_128, SHA_1, PFS_14
- AES_256, SHA_256, PFS_1
- AES_256, SHA_256, PFS_2
- AES_256, SHA_256, PFS_14
- AES_256, SHA_1, PFS_24
- AES_256, SHA_256, PFS_24
- AES_128, SHA_256, PFS_NONE
- AES_128, SHA_256, PFS_1
- AES_128, SHA_256, PFS_2
- AES_128, SHA_256, PFS_14

Custom policies for IPsec connectivity

When working with custom IPsec policies, keep in mind the following requirements:

- **IKE** - For IKE, you can select any parameter from IKE Encryption, plus any parameter from IKE Integrity, plus any parameter from DH Group.
- **IPsec** - For IPsec, you can select any parameter from IPsec Encryption, plus any parameter from IPsec Integrity, plus PFS. If any of the parameters for IPsec Encryption or IPsec Integrity is GCM, then the parameters for both settings must be GCM.

> **NOTE**
> With Custom IPsec policies, there is no concept of responder and initiator (unlike Default IPsec policies). Both sides (on-premises and Azure VPN gateway) will use the same settings for IKE Phase 1 and IKE Phase 2. Both IKEv1 and IKEv2 protocols are supported. There is no support for Azure as a responder only.

Available settings and parameters

SETTING	PARAMETERS
IKE Encryption	AES256, AES192, AES128
IKE Integrity	SHA384, SHA256, SHA1
DH Group	DHGroup24, ECP384, ECP256, DHGroup14, DHGroup2048, DHGroup2
IPsec Encryption	GCMAES256, GCMAES192, GCMAES128, AES256, AES192, AES128
IPsec Integrity	GCMASE256, GCMAES192, GCMAES128, SHA256, SHA1
PFS Group	PFS24, ECP384, ECP256, PFS2048, PFS2

Next steps

For more information about Virtual WAN, see About Azure Virtual WAN and the Azure Virtual WAN FAQ.

For any additional information, please send an email to azurevirtualwan@microsoft.com. Include your company

name in “[ ]” in the subject line.

Virtual WAN default policies for IPsec connectivity

11/4/2019 • 2 minutes to read • Edit Online

This article shows the supported IPsec policy combinations.

Default IPsec policies

> **NOTE**
> When working with Default policies, Azure can act as both initiator and responder during an IPsec tunnel setup. There is no support for Azure as a responder only.

Initiator

The following sections list the supported policy combinations when Azure is the initiator for the tunnel.

Phase-1

- AES_256, SHA1, DH_GROUP_2
- AES_256, SHA_256, DH_GROUP_2
- AES_128, SHA1, DH_GROUP_2
- AES_128, SHA_256, DH_GROUP_2

Phase-2

- GCM_AES_256, GCM_AES_256, PFS_NONE
- AES_256, SHA_1, PFS_NONE
- AES_256, SHA_256, PFS_NONE
- AES_128, SHA_1, PFS_NONE

Responder

The following sections list the supported policy combinations when Azure is the responder for the tunnel.

Phase-1

- AES_256, SHA1, DH_GROUP_2
- AES_256, SHA_256, DH_GROUP_2
- AES_128, SHA1, DH_GROUP_2
- AES_128, SHA_256, DH_GROUP_2

Phase-2

- GCM_AES_256, GCM_AES_256, PFS_NONE
- AES_256, SHA_1, PFS_NONE
- AES_256, SHA_256, PFS_NONE
- AES_128, SHA_1, PFS_NONE
- AES_256, SHA_1, PFS_1
- AES_256, SHA_1, PFS_2
- AES_256, SHA_1, PFS_14
- AES_128, SHA_1, PFS_1
- AES_128, SHA_1, PFS_2

- AES_128, SHA_1, PFS_14
- AES_256, SHA_256, PFS_1
- AES_256, SHA_256, PFS_2
- AES_256, SHA_256, PFS_14
- AES_256, SHA_1, PFS_24
- AES_256, SHA_256, PFS_24
- AES_128, SHA_256, PFS_NONE
- AES_128, SHA_256, PFS_1
- AES_128, SHA_256, PFS_2
- AES_128, SHA_256, PFS_14

Custom IPsec policies

When working with custom IPsec policies, keep in mind the following requirements:

- **IKE** - For IKE, you can select any parameter from IKE Encryption, plus any parameter from IKE Integrity, plus any parameter from DH Group.
- **IPsec** - For IPsec, you can select any parameter from IPsec Encryption, plus any parameter from IPsec Integrity, plus PFS. If any of the parameters for IPsec Encryption or IPsec Integrity is GCM, then the parameters for both settings must be GCM.

> **NOTE**
> With Custom IPsec policies, there is no concept of responder and initiator (unlike Default IPsec policies). Both sides (on-premises and Azure VPN gateway) will use the same settings for IKE Phase 1 and IKE Phase 2. Both IKEv1 and IKEv2 protocols are supported. There is no support for Azure as a responder only.

Available settings and parameters

SETTING	PARAMETERS
IKE Encryption	AES256, AES192, AES128
IKE Integrity	SHA384, SHA256, SHA1
DH Group	DHGroup24, ECP384, ECP256, DHGroup14, DHGroup2048, DHGroup2
IPsec Encryption	GCMAES256, GCMAES192, GCMAES128, AES256, AES192, AES128
IPsec Integrity	GCMASE256, GCMAES192, GCMAES128, SHA256, SHA1
PFS Group	PFS24, ECP384, ECP256, PFS2048, PFS2

Next steps

For steps to configure a custom IPsec policy, see Configure a custom IPsec policy for Virtual WAN. For more information about Virtual WAN, see About Azure Virtual WAN and the Azure Virtual WAN FAQ.

Connect a VPN Gateway (virtual network gateway) to Virtual WAN

11/4/2019 • 6 minutes to read • Edit Online

This article helps you set up connectivity from an Azure VPN Gateway (virtual network gateway) to an Azure Virtual WAN (VPN gateway). Creating a connection from a VPN Gateway (virtual network gateway) to a Virtual WAN (VPN gateway) is similar to setting up connectivity to a virtual WAN from branch VPN sites.

In order to minimize possible confusion between two features, we will preface the gateway with the name of the feature that we are referring to. For example, VPN Gateway virtual network gateway, and Virtual WAN VPN gateway.

Before you begin

Before you begin, create the following resources:

Azure Virtual WAN

- Create a virtual WAN.
- Create a hub. The virtual hub contains the Virtual WAN VPN gateway.

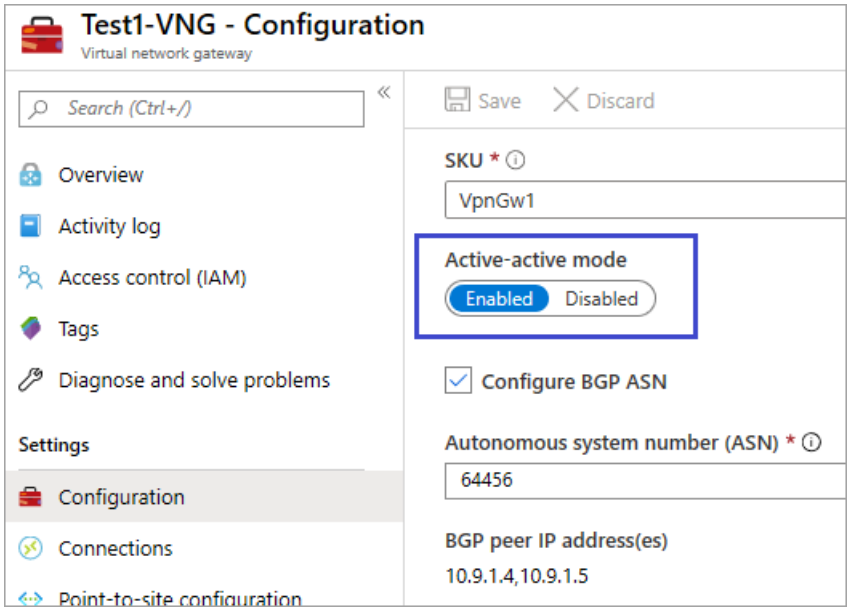
Azure Virtual Network

- Create a virtual network without any virtual network gateways. Verify that none of the subnets of your on-premises networks overlap with the virtual networks that you want to connect to. To create a virtual network in the Azure portal, see the Quickstart.

1. Create an Azure virtual network gateway

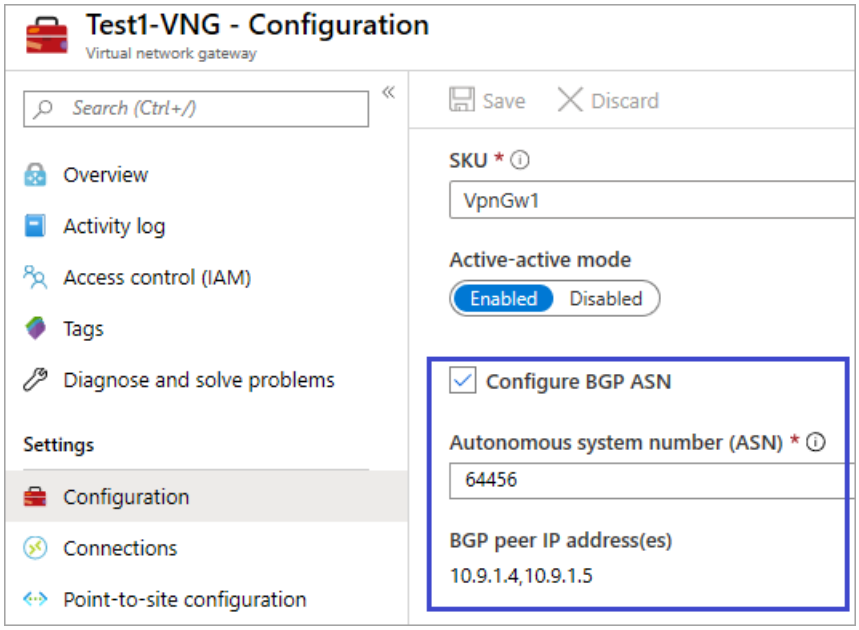
Create a VPN Gateway virtual network gateway for your virtual network in active-active mode for your virtual network. When you create the gateway, you can either use existing public IP addresses for the two instances of the gateway, or you can create new public IPs. You use these public IPs when setting up the Virtual WAN sites. For more information about active-active mode, see Configure active-active connections.

Active-active mode setting



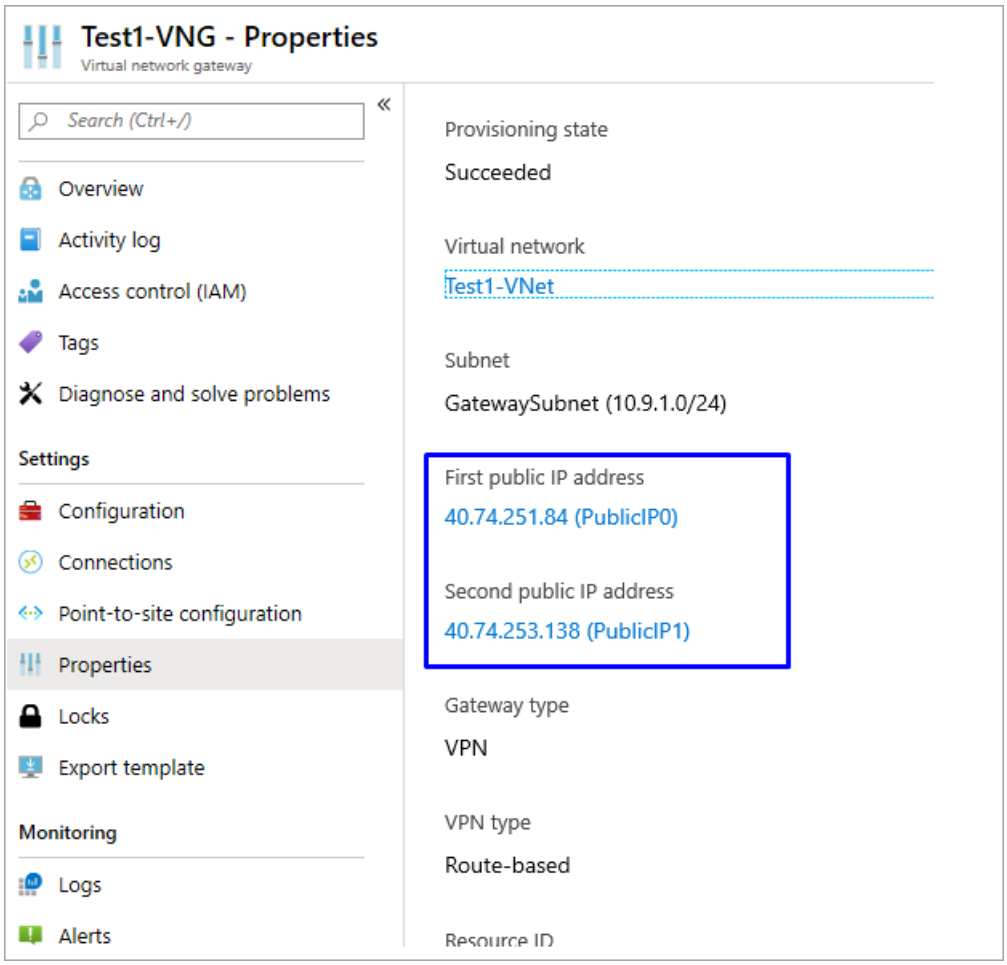
BGP setting

The BGP ASN cannot be 65515. 66515 will be used by Azure Virtual WAN.



Public IP addresses

When the gateway is created, navigate to the **Properties** page. The properties and configuration settings will be similar to the following example. Notice the two public IP addresses that are used for the gateway.



2. Create Virtual WAN VPN sites

To create Virtual WAN VPN sites, navigate your to your virtual WAN and, under **Connectivity**, select **VPN sites**. In this section, you will create two Virtual WAN VPN sites that correspond to the virtual network gateways you

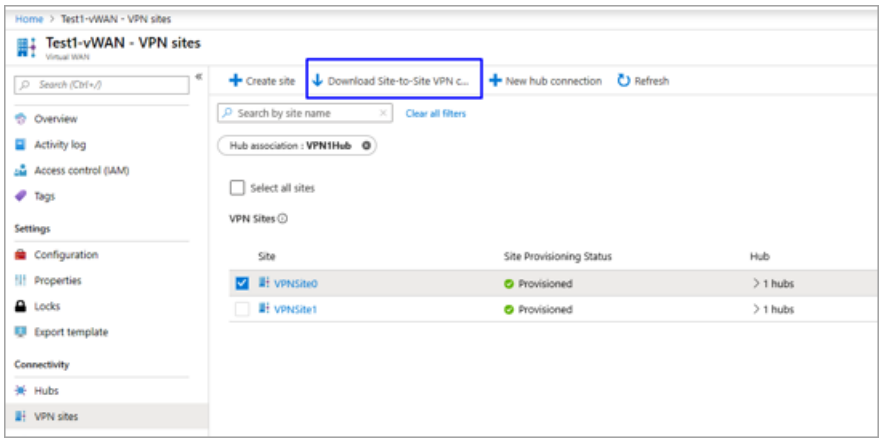
created in the previous section.

1. Select **+Create site**.
2. On the **Create VPN sites** page, type the following values:
   - **Region** - (The same region as the Azure VPN Gateway virtual network gateway)
   - **Device vendor** - Enter the device vendor (any name)
   - **Private address space** - (Enter a value, or leave blank when BGP is enabled)
   - **Border Gateway Protocol** - (Set to **Enable** if the Azure VPN Gateway virtual network gateway has BGP enabled)
   - **Connect to Hubs** (Select hub you created in the prerequisites from the dropdown)
3. Under **Links**, enter the following values:
   - **Provider Name** - Enter a Link name and a Provider name (any name)
   - **Speed** - Speed (any number)
   - **IP Address** - Enter IP address (same as the first public IP address shown under the (VPN Gateway) virtual network gateway properties)
   - **BGP Address** and **ASN** - BGP address and ASN. These must be the same as one of the BGP peer IP addresses, and ASN from the VPN Gateway virtual network gateway that you configured in Step 1.
4. Review and select **Confirm** to create the site.
5. Repeat the previous steps to create the second site to match with the second instance of the VPN Gateway virtual network gateway. You'll keep the same settings, except using second public IP address and second BGP peer IP address from VPN Gateway configuration.
6. You now have two sites successfully provisioned and can proceed to the next section to download configuration files.

3. Download the VPN configuration files

In this section, you download the VPN configuration file for each of the sites that you created in the previous section.

1. At the top of the Virtual WAN **VPN sites** page, select the **Site**, then select **Download Site-to-site VPN configuration**. Azure creates a configuration file with the settings.



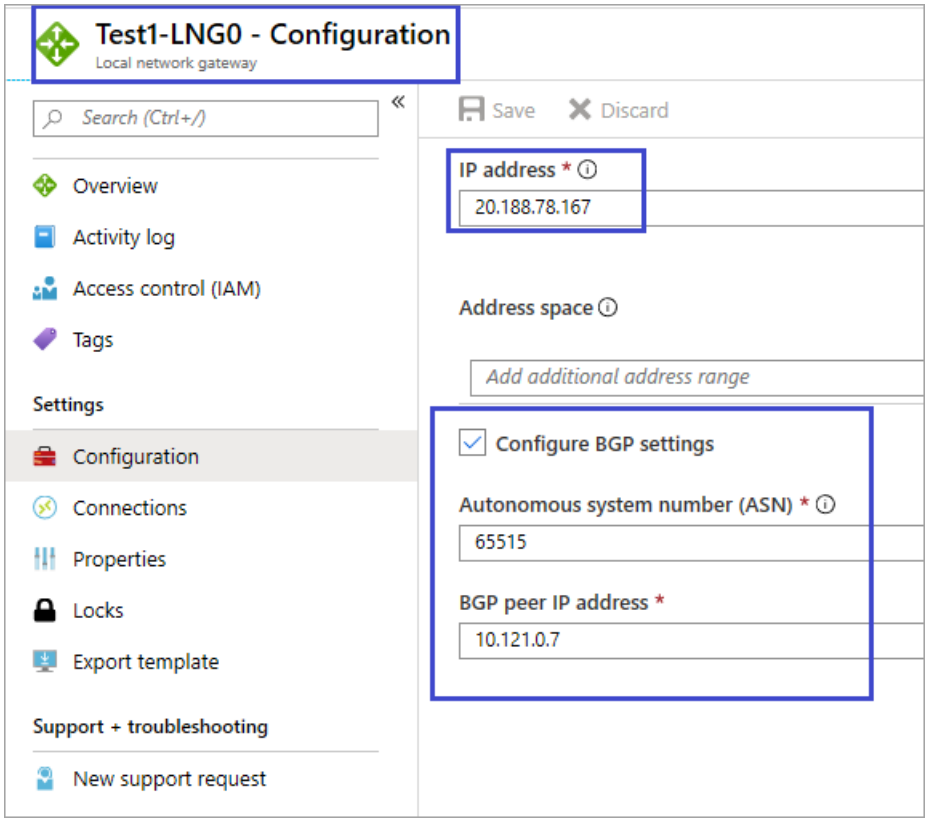
2. Download and open the configuration file.
3. Repeat these steps for the second site. Once you have both configuration files open, you can proceed to the next section.

4. Create the local network gateways

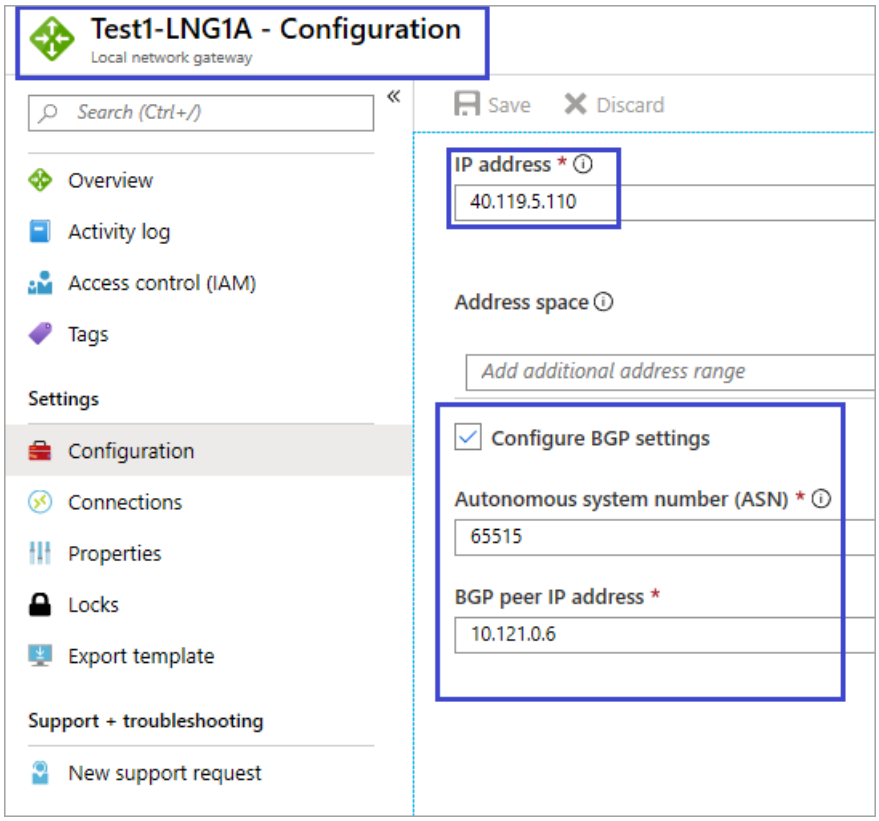
In this section, you create two Azure VPN Gateway local network gateways. The configuration files from the previous step contain the gateway configuration settings. Use these settings to create and configure the Azure VPN Gateway local network gateways.

1. Create the local network gateway using these settings. For information about how to create a VPN Gateway local network gateway, see the VPN Gateway article Create a local network gateway.

   - **IP address** - Use the Instance0 IP Address shown for *gatewayconfiguration* from the configuration file.
   - **BGP** - If the connection is over BGP, select **Configure BGP settings** and enter the ASN '65515'. Enter the BGP peer IP address. Use 'Instance0 BgpPeeringAddresses' for *gatewayconfiguration* from the configuration file.
   - **Subscription, Resource Group, and Location** are same as for the Virtual WAN hub.
2. Review and create the local network gateway. Your local network gateway should look similar to this example.



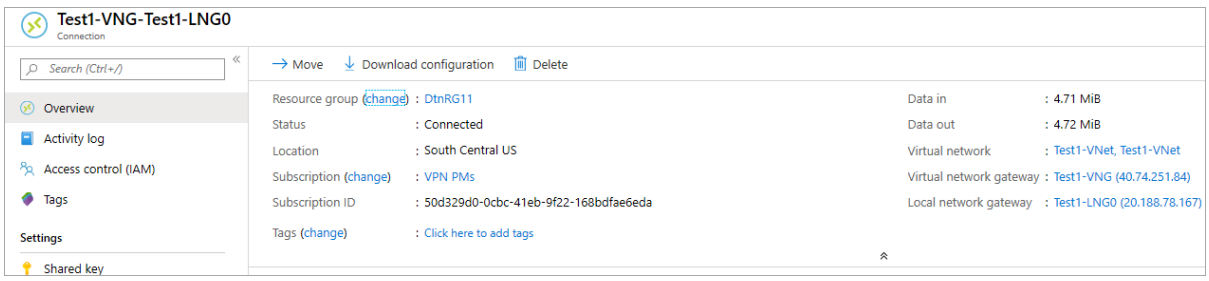
3. Repeat these steps to create another local network gateway, but this time, use the 'Instance1' values instead of 'Instance0' values from the configuration file.



5. Create connections

In this section, you create a connection between the VPN Gateway local network gateways and virtual network gateway. For steps on how to create a VPN Gateway connection, see Configure a connection.

1. In the portal, navigate to your virtual network gateway and click **Connections**. At the top of the Connections page, click **+Add** to open the **Add connection** page.
2. On the **Add connection** page, configure the following values for your connection:
   - **Name:** Name your connection.
   - **Connection type:** Select **Site-to-site(IPSec)**
   - **Virtual network gateway:** The value is fixed because you are connecting from this gateway.
   - **Local network gateway:** This connection will connect the virtual network gateway to the local network gateway. Choose one of the local network gateways that you created earlier.
   - **Shared Key:** Enter a shared key.
   - **IKE Protocol:** Choose the IKE protocol.
   - **BGP:** Choose **Enable BGP** if the connection is over BGP.
3. Click **OK** to create your connection.
4. You can view the connection in the **Connections** page of the virtual network gateway.



5. Repeat the preceding steps to create a second connection. For the second connection, select the other local network gateway that you created.

6. Test connections

You can test the connectivity by creating two virtual machines, one on the side of the VPN Gateway virtual network gateway, and one in a virtual network for the Virtual WAN, and then ping the two virtual machines.

1. Create a virtual machine in the virtual network (Test1-VNet) for Azure VPN Gateway (Test1-VNG). Do not create the virtual machine in the GatewaySubnet.
2. Create another virtual network to connect to the virtual WAN. Create a virtual machine in a subnet of this virtual network. This virtual network cannot contain any virtual network gateways. You can quickly create a virtual network using the PowerShell steps in the site-to-site connection article. Be sure to change the values before running the cmdlets.
3. Connect the VNet to the Virtual WAN hub. On the page for your virtual WAN, select **Virtual network connections**, then **+Add connection**. On the **Add connection** page, fill in the following fields:
   - **Connection name** - Name your connection.
   - **Hubs** - Select the hub you want to associate with this connection.
   - **Subscription** - Verify the subscription.
   - **Virtual network** - Select the virtual network you want to connect to this hub. The virtual network cannot have an already existing virtual network gateway.
4. Click **OK** to create the virtual network connection.
5. Connectivity is now set between the VMs. You should be able to ping one VM from the other, unless there are any firewalls or other policies blocking the communication.

Next steps

For steps to configure a custom IPsec policy, see Configure a custom IPsec policy for Virtual WAN. For more information about Virtual WAN, see About Azure Virtual WAN and the Azure Virtual WAN FAQ.

Configure Global VNet peering (cross-region VNet) for Virtual WAN

11/4/2019 • 2 minutes to read • Edit Online

You can connect a VNet in a different region to your Virtual WAN hub.

Before you begin

Verify that you have met the following criteria:

- The cross-region VNet (spoke) is not connected to another Virtual WAN hub. A spoke can only be connected to one virtual hub.
- The VNet (spoke) does not contain a virtual network gateway (for example, an Azure VPN Gateway or ExpressRoute virtual network gateway). If the VNet contains a virtual network gateway, you must remove the gateway before connecting the spoke VNet to the hub.

Register this feature

You can register for this feature using PowerShell. If you select "Try It" from the example below, Azure Cloud-Shell opens and you won't need to install the PowerShell cmdlets locally to your computer. If necessary, you can change subscriptions using the 'Select-AzSubscription -SubscriptionId ' cmdlet.

```
Register-AzProviderFeature -FeatureName AllowCortexGlobalVnetPeering -ProviderNamespace Microsoft.Network
Register-AzResourceProvider -ProviderNamespace 'Microsoft.Network'
```

Verify registration

```
Get-AzProviderFeature -FeatureName AllowCortexGlobalVnetPeering -ProviderNamespace Microsoft.Network
```

Connect a VNet to the hub

In this step, you create the peering connection between your hub and the cross-region VNet. Repeat these steps for each VNet that you want to connect.

1. On the page for your virtual WAN, click **Virtual network connections**.
2. On the virtual network connection page, click **+Add connection**.
3. On the **Add connection** page, fill in the following fields:
   - **Connection name** - Name your connection.
   - **Hubs** - Select the hub you want to associate with this connection.
   - **Subscription** - Verify the subscription.
   - **Virtual network** - Select the virtual network you want to connect to this hub. The virtual network cannot have an already existing virtual network gateway.
4. Click **OK** to create the peering connection.

Next steps

To learn more about Virtual WAN, see Virtual WAN Overview.

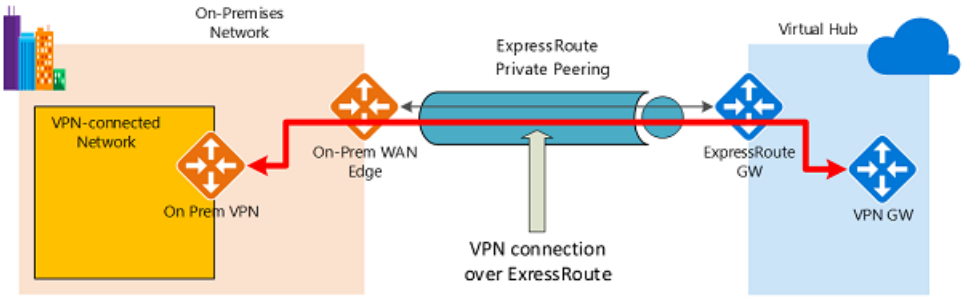
ExpressRoute encryption: IPsec over ExpressRoute for Virtual WAN

2/18/2020 • 9 minutes to read • Edit Online

This article shows you how to use Azure Virtual WAN to establish an IPsec/IKE VPN connection from your on-premises network to Azure over the private peering of an Azure ExpressRoute circuit. This technique can provide an encrypted transit between the on-premises networks and Azure virtual networks over ExpressRoute, without going over the public internet or using public IP addresses.

Topology and routing

The following diagram shows an example of VPN connectivity over ExpressRoute private peering:



The diagram shows a network within the on-premises network connected to the Azure hub VPN gateway over ExpressRoute private peering. The connectivity establishment is straightforward:

1. Establish ExpressRoute connectivity with an ExpressRoute circuit and private peering.
2. Establish the VPN connectivity as described in this article.

An important aspect of this configuration is routing between the on-premises networks and Azure over both the ExpressRoute and VPN paths.

Traffic from on-premises networks to Azure

For traffic from on-premises networks to Azure, the Azure prefixes (including the virtual hub and all the spoke virtual networks connected to the hub) are advertised via both the ExpressRoute private peering BGP and the VPN BGP. This results in two network routes (paths) toward Azure from the on-premises networks:

- One over the IPsec-protected path
- One directly over ExpressRoute *without* IPsec protection

To apply encryption to the communication, you must make sure that for the VPN-connected network in the diagram, the Azure routes via on-premises VPN gateway are preferred over the direct ExpressRoute path.

Traffic from Azure to on-premises networks

The same requirement applies to the traffic from Azure to on-premises networks. To ensure that the IPsec path is preferred over the direct ExpressRoute path (without IPsec), you have two options:

- Advertise more specific prefixes on the VPN BGP session for the VPN-connected network. You can advertise a larger range that encompasses the VPN-connected network over ExpressRoute private peering, then more specific ranges in the VPN BGP session. For example, advertise 10.0.0.0/16 over ExpressRoute, and 10.0.1.0/24 over VPN.
- Advertise disjoint prefixes for VPN and ExpressRoute. If the VPN-connected network ranges are disjoint

from other ExpressRoute connected networks, you can advertise the prefixes in the VPN and ExpressRoute BGP sessions respectively. For example, advertise 10.0.0.0/24 over ExpressRoute, and 10.0.1.0/24 over VPN.

In both of these examples, Azure will send traffic to 10.0.1.0/24 over the VPN connection rather than directly over ExpressRoute without VPN protection.

> **WARNING**
> If you advertise the *same* prefixes over both ExpressRoute and VPN connections, Azure will use the ExpressRoute path directly without VPN protection.

Before you begin

Before you start your configuration, verify that you meet the following criteria:

- If you already have virtual network that you want to connect to, verify that none of the subnets of your on-premises network overlap with it. Your virtual network doesn't require a gateway subnet and can't have any virtual network gateways. If you don't have a virtual network, you can create one by using the steps in this article.
- Obtain an IP address range for your hub region. The hub is a virtual network, and the address range that you specify for the hub region can't overlap with an existing virtual network that you connect to. It also can't overlap with the address ranges that you connect to on-premises. If you're unfamiliar with the IP address ranges located in your on-premises network configuration, coordinate with someone who can provide those details for you.
- If you don't have an Azure subscription, create a free account before you begin.

1. Create a virtual WAN and hub with gateways

The following Azure resources and the corresponding on-premises configurations must be in place before you proceed:

- An Azure virtual WAN
- A virtual WAN hub with an ExpressRoute gateway and a VPN gateway

For the steps to create an Azure virtual WAN and a hub with an ExpressRoute association, see Create an ExpressRoute association using Azure Virtual WAN. For the steps to create a VPN gateway in the virtual WAN, see Create a site-to-site connection using Azure Virtual WAN.

2. Create a site for the on-premises network

The site resource is the same as the non-ExpressRoute VPN sites for a virtual WAN. The IP address of the on-premises VPN device can now be either a private IP address, or a public IP address in the on-premises network reachable via ExpressRoute private peering created in step 1.

> **NOTE**
> The IP address for the on-premises VPN device *must* be part of the address prefixes advertised to the virtual WAN hub via Azure ExpressRoute private peering.

1. Go to the Azure portal in your browser.
2. Select the WAN that you created. On the WAN page, under **Connectivity**, select **VPN sites**.
3. On the **VPN sites** page, select **+Create site**.
4. On the **Create site** page, fill in the following fields:

- **Subscription**: Verify the subscription.
- **Resource Group**: Select or create the resource group that you want to use.
- **Region**: Enter the Azure region for the VPN site resource.
- **Name**: Enter the name by which you want to refer to your on-premises site.
- **Device vendor**: Enter the vendor of the on-premises VPN device.
- **Border Gateway Protocol**: Select "Enable" if your on-premises network uses BGP.
- **Private address space**: Enter the IP address space that's located on your on-premises site. Traffic destined for this address space is routed to the on-premises network via the VPN gateway.
- **Hubs**: Select one or more hubs to connect this VPN site. The selected hubs must have VPN gateways already created.

5. Select **Next: Links >** for the VPN link settings:

   - **Link Name**: The name by which you want to refer to this connection.
   - **Provider Name**: The name of the internet service provider for this site. For an ExpressRoute on-premises network, it's the name of the ExpressRoute service provider.
   - **Speed**: The speed of the internet service link or ExpressRoute circuit.
   - **IP address**: The public IP address of the VPN device that resides on your on-premises site. Or, for ExpressRoute on-premises, it's the private IP address of the VPN device via ExpressRoute.

   If BGP is enabled, it will apply to all connections created for this site in Azure. Configuring BGP on a virtual WAN is equivalent to configuring BGP on an Azure VPN gateway.

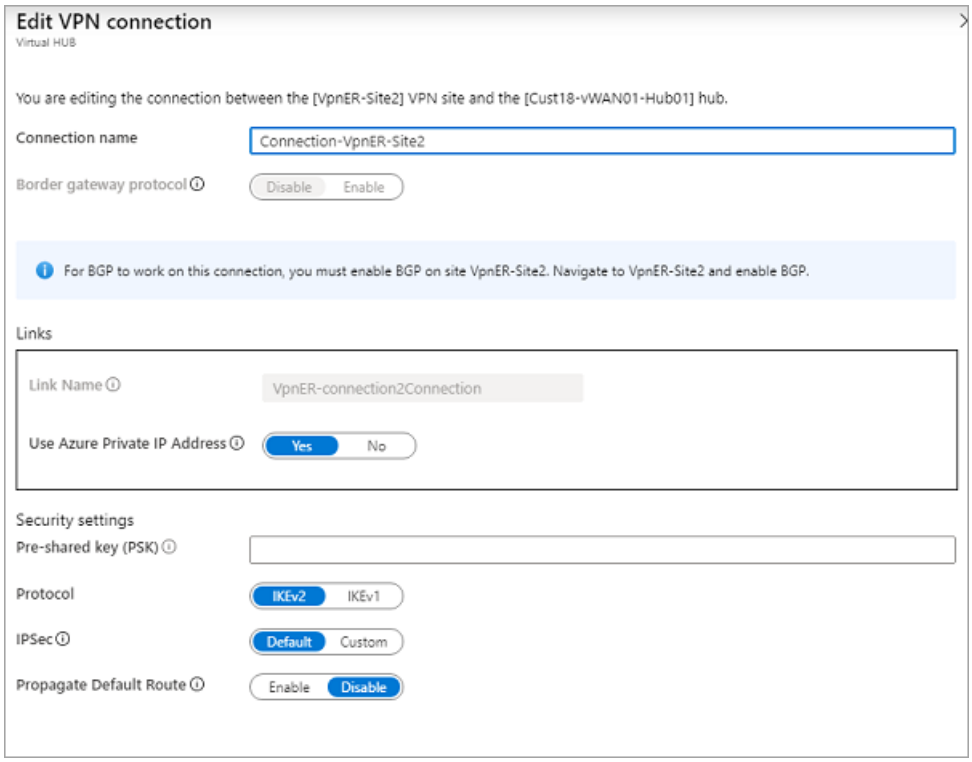
   Your on-premises BGP peer address *must not* be the same as the IP address of your VPN to the device or the virtual network address space of the VPN site. Use a different IP address on the VPN device for your BGP peer IP. It can be an address assigned to the loopback interface on the device. However, it *can't* be an APIPA (169.254.*x.x*) address. Specify this address in the corresponding local network gateway that represents the location. For BGP prerequisites, see About BGP with Azure VPN Gateway.

6. Select **Next: Review + create >** to check the setting values and create the VPN site. If you selected **Hubs** to connect, the connection will be established between the on-premises network and the hub VPN gateway.

3. Update the VPN connection setting to use ExpressRoute

After you create the VPN site and connect to the hub, use the following steps to configure the connection to use ExpressRoute private peering:

1. Go back to the virtual WAN resource page, and select the hub resource. Or navigate from the VPN site to the connected hub.
2. Under **Connectivity**, select **VPN (Site-to-Site)**.
3. Select the ellipsis (**...**) on the VPN site over ExpressRoute, and select **Edit VPN connection to this hub**.
4. For **Use Azure Private IP Address**, select **Yes**. The setting configures the hub VPN gateway to use private IP addresses within the hub address range on the gateway for this connection, instead of the public IP addresses. This will ensure that the traffic from the on-premises network traverses the ExpressRoute private peering paths rather than using the public internet for this VPN connection. The following screenshot shows the setting.



5. Select **Save**.

After you save your changes, the hub VPN gateway will use the private IP addresses on the VPN gateway to establish the IPsec/IKE connections with the on-premises VPN device over ExpressRoute.

4. Get the private IP addresses for the hub VPN gateway

Download the VPN device configuration to get the private IP addresses of the hub VPN gateway. You need these addresses to configure the on-premises VPN device.

1. On the page for your hub, select **VPN (Site-to-Site)** under **Connectivity**.
2. At the top of the **Overview** page, select **Download VPN Config**.

   Azure creates a storage account in the resource group "microsoft-network-[location]," where *location* is the location of the WAN. After you apply the configuration to your VPN devices, you can delete this storage account.
3. After the file is created, select the link to download it.
4. Apply the configuration to your VPN device.

VPN device configuration file

The device configuration file contains the settings to use when you're configuring your on-premises VPN device. When you view this file, notice the following information:

- **vpnSiteConfiguration**: This section denotes the device details set up as a site that's connecting to the virtual WAN. It includes the name and public IP address of the branch device.
- **vpnSiteConnections**: This section provides information about the following settings:
  - Address space of the virtual hub's virtual network.
    Example: `"AddressSpace":"10.51.230.0/24"`
  - Address space of the virtual networks that are connected to the hub.
    Example: `"ConnectedSubnets":["10.51.231.0/24"]`
  - IP addresses of the virtual hub's VPN gateway. Because each connection of the VPN gateway is

composed of two tunnels in active-active configuration, you'll see both IP addresses listed in this file. In this example, you see `Instance0` and `Instance1` for each site, and they're private IP addresses instead of public IP addresses.
Example: `"Instance0":"10.51.230.4" "Instance1":"10.51.230.5"`

- Configuration details for the VPN gateway connection, such as BGP and pre-shared key. The pre-shared key is automatically generated for you. You can always edit the connection on the **Overview** page for a custom pre-shared key.

Example device configuration file

```
[{
      "configurationVersion":{
        "LastUpdatedTime":"2019-10-11T05:57:35.1803187Z",
        "Version":"5b096293-edc3-42f1-8f73-68c14a7c4db3"
      },
      "vpnSiteConfiguration":{
        "Name":"VPN-over-ER-site",
        "IPAddress":"172.24.127.211",
        "LinkName":"VPN-over-ER"
      },
      "vpnSiteConnections":[{
        "hubConfiguration":{
          "AddressSpace":"10.51.230.0/24",
          "Region":"West US 2",
          "ConnectedSubnets":["10.51.231.0/24"]
        },
        "gatewayConfiguration":{
          "IpAddresses":{
            "Instance0":"10.51.230.4",
            "Instance1":"10.51.230.5"
          }
        },
        "connectionConfiguration":{
          "IsBgpEnabled":false,
          "PSK":"abc123",
          "IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}
        }
      }]
    },
    {
      "configurationVersion":{
        "LastUpdatedTime":"2019-10-11T05:57:35.1803187Z",
        "Version":"fbdb34ea-45f8-425b-9bc2-4751c2c4fee0"
      },
      "vpnSiteConfiguration":{
        "Name":"VPN-over-INet-site",
        "IPAddress":"13.75.195.234",
        "LinkName":"VPN-over-INet"
      },
      "vpnSiteConnections":[{
        "hubConfiguration":{
          "AddressSpace":"10.51.230.0/24",
          "Region":"West US 2",
          "ConnectedSubnets":["10.51.231.0/24"]
        },
        "gatewayConfiguration":{
          "IpAddresses":{
            "Instance0":"51.143.63.104",
            "Instance1":"52.137.90.89"
          }
        },
        "connectionConfiguration":{
          "IsBgpEnabled":false,
          "PSK":"abc123",
          "IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}
        }
      }]
}]
```


Configuring your VPN device

If you need instructions to configure your device, you can use the instructions on the VPN device configuration scripts page with the following caveats:

- The instructions on the VPN device page are not written for a virtual WAN. But you can use the virtual WAN values from the configuration file to manually configure your VPN device.

- The downloadable device configuration scripts that are for the VPN gateway don't work for the virtual WAN, because the configuration is different.
- A new virtual WAN can support both IKEv1 and IKEv2.
- A virtual WAN can use only route-based VPN devices and device instructions.

5. View your virtual WAN

1. Go to the virtual WAN.
2. On the **Overview** page, each point on the map represents a hub. Hover over any point to view the hub's health summary.
3. In the **Hubs and connections** section, you can view hub, site, region, and VPN connection status. You can also view bytes in and out.

6. View your resource health

1. Go to your WAN.
2. In the **SUPPORT + Troubleshooting** section, select **Health** and view your resource.

7. Monitor a connection

Create a connection to monitor communication between an Azure virtual machine (VM) and a remote site. For information about how to set up a connection monitor, see Monitor network communication. The source field is the VM IP in Azure, and the destination IP is the site IP.

8. Clean up resources

When you no longer need these resources, you can use Remove-AzResourceGroup to remove the resource group and all of the resources that it contains. Run the following PowerShell command, and replace `myResourceGroup` with the name of your resource group:

```
Remove-AzResourceGroup -Name myResourceGroup -Force
```

Next steps

This article helps you create a VPN connection over ExpressRoute private peering by using Virtual WAN. To learn more about Virtual WAN and related features, see the Virtual WAN overview.

Upgrade a virtual WAN from Basic to Standard

11/4/2019 • 2 minutes to read • Edit Online

This article helps you upgrade a Basic WAN to a Standard WAN. A 'Basic' WAN type creates all hubs inside of it as Basic SKU hubs. In a Basic hub, you are limited to site-to-site VPN functionality only. A 'Standard' WAN type creates all the hubs inside of it as Standard SKU hubs. When you use Standard hubs, you can enable ExpressRoute, User (Point-to-site) VPN, a full mesh hub, and VNet-to-VNet transit through the Azure hubs.

The following table shows the configurations available for each WAN type:

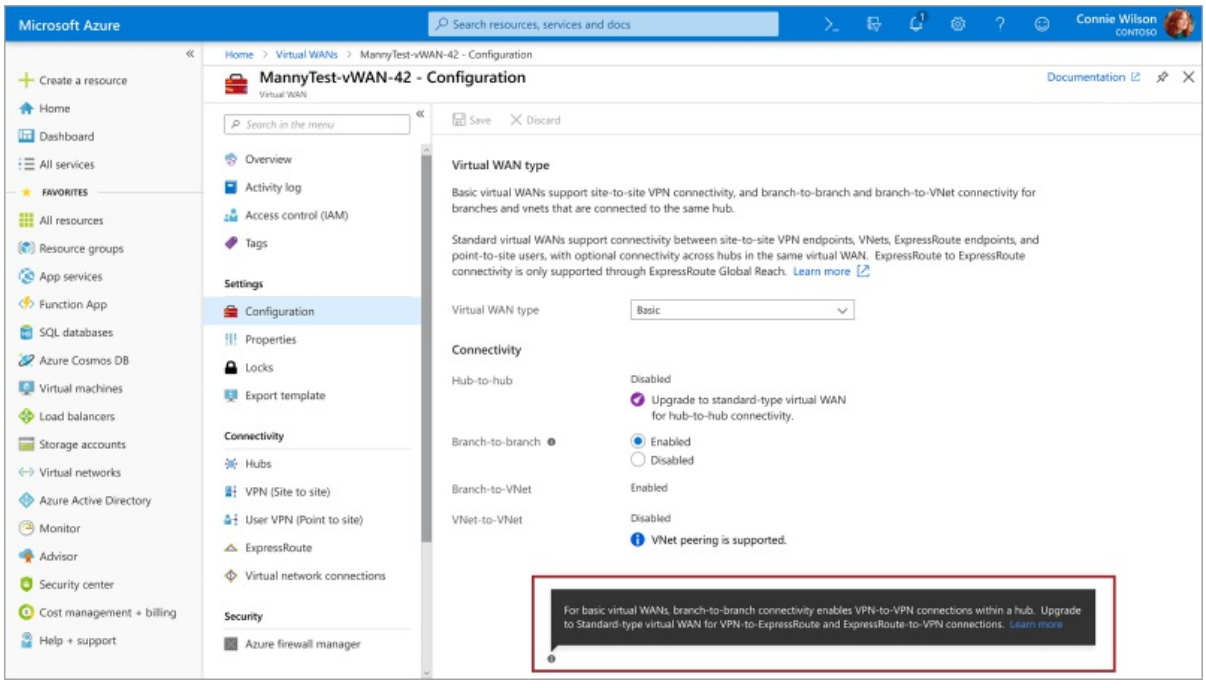
VIRTUAL WAN TYPE	HUB TYPE	AVAILABLE CONFIGURATIONS
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub

NOTE

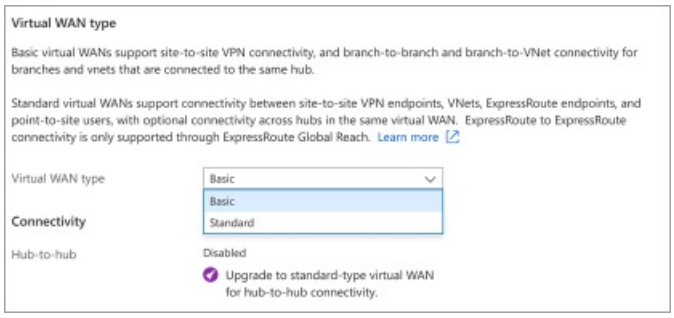
You can upgrade from Basic to Standard, but cannot revert from Standard back to Basic.

To change the virtual WAN type

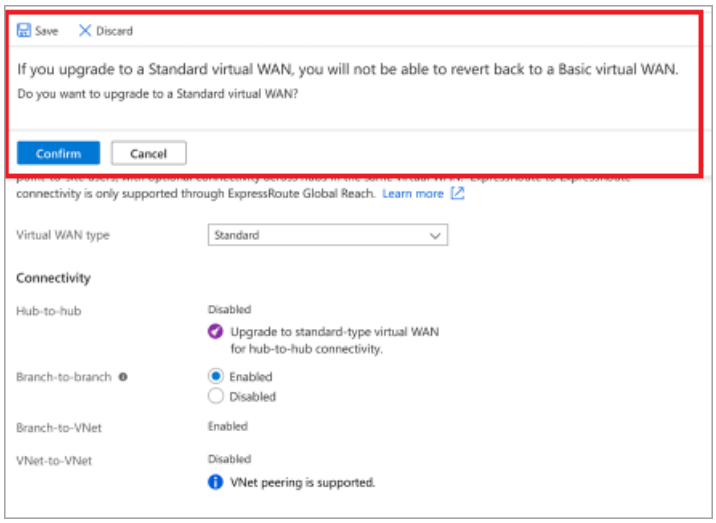
1. On the page for your virtual WAN, select **Configuration** to open the Configuration page.



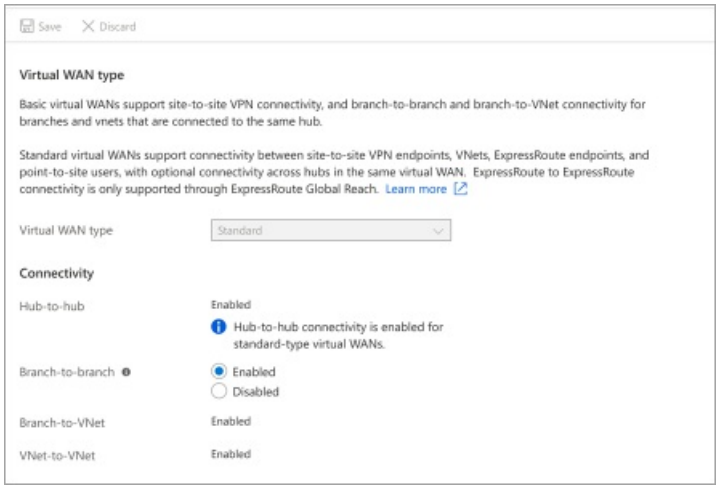
2. For the Virtual WAN type, select **Standard** from the dropdown.



3. Understand that if you upgrade to a Standard virtual WAN, you cannot revert back to a Basic virtual WAN. Select **Confirm** if you want to upgrade.



4. Once the change has been saved, your virtual WAN page looks similar to this example.



Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Configure a custom IPsec policy for Virtual WAN using the portal

11/4/2019 • 2 minutes to read • Edit Online

You can configure custom IPsec policy for Virtual WAN in the Azure portal. Custom policies are helpful when you want both sides (on-premises and Azure VPN gateway) to use the same settings for IKE Phase 1 and IKE Phase 2.

Working with custom policies

When working with custom IPsec policies, keep in mind the following requirements:

- **IKE** - For IKE, you can select any parameter from IKE Encryption, plus any parameter from IKE Integrity, plus any parameter from DH Group.
- **IPsec** - For IPsec, you can select any parameter from IPsec Encryption, plus any parameter from IPsec Integrity, plus PFS. If any of the parameters for IPsec Encryption or IPsec Integrity is GCM, then the parameters for both settings must be GCM.

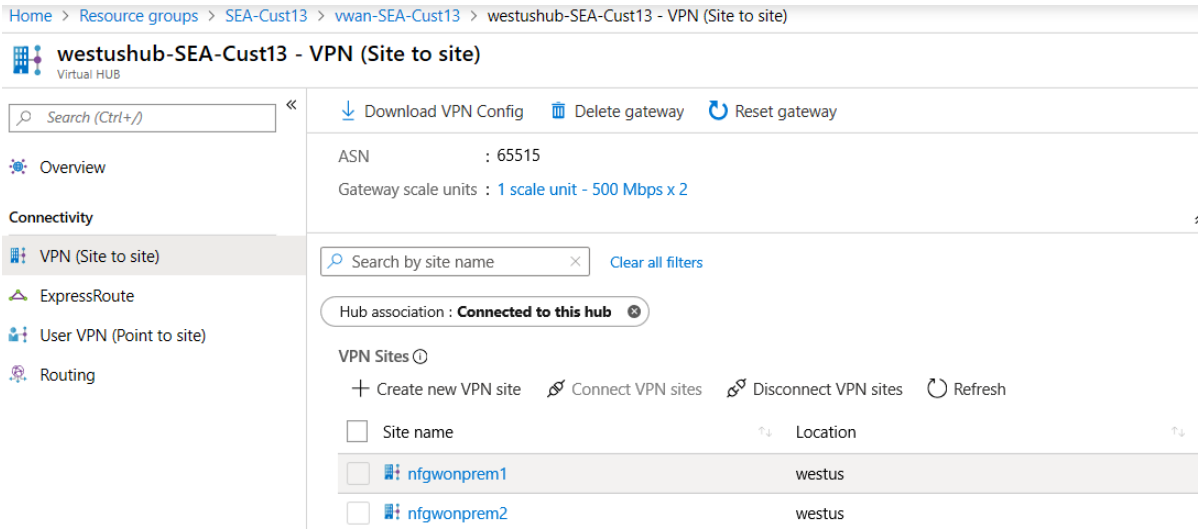
> **NOTE**
> With Custom IPsec policies, there is no concept of responder and initiator (unlike Default IPsec policies). Both sides (on-premises and Azure VPN gateway) will use the same settings for IKE Phase 1 and IKE Phase 2. Both IKEv1 and IKEv2 protocols are supported. There is no support for Azure as a responder only.

Available settings and parameters

SETTING	PARAMETERS
IKE Encryption	AES256, AES192, AES128
IKE Integrity	SHA384, SHA256, SHA1
DH Group	DHGroup24, ECP384, ECP256, DHGroup14, DHGroup2048, DHGroup2
IPsec Encryption	GCMAES256, GCMAES192, GCMAES128, AES256, AES192, AES128
IPsec Integrity	GCMASE256, GCMAES192, GCMAES128, SHA256, SHA1
PFS Group	PFS24, ECP384, ECP256, PFS2048, PFS2

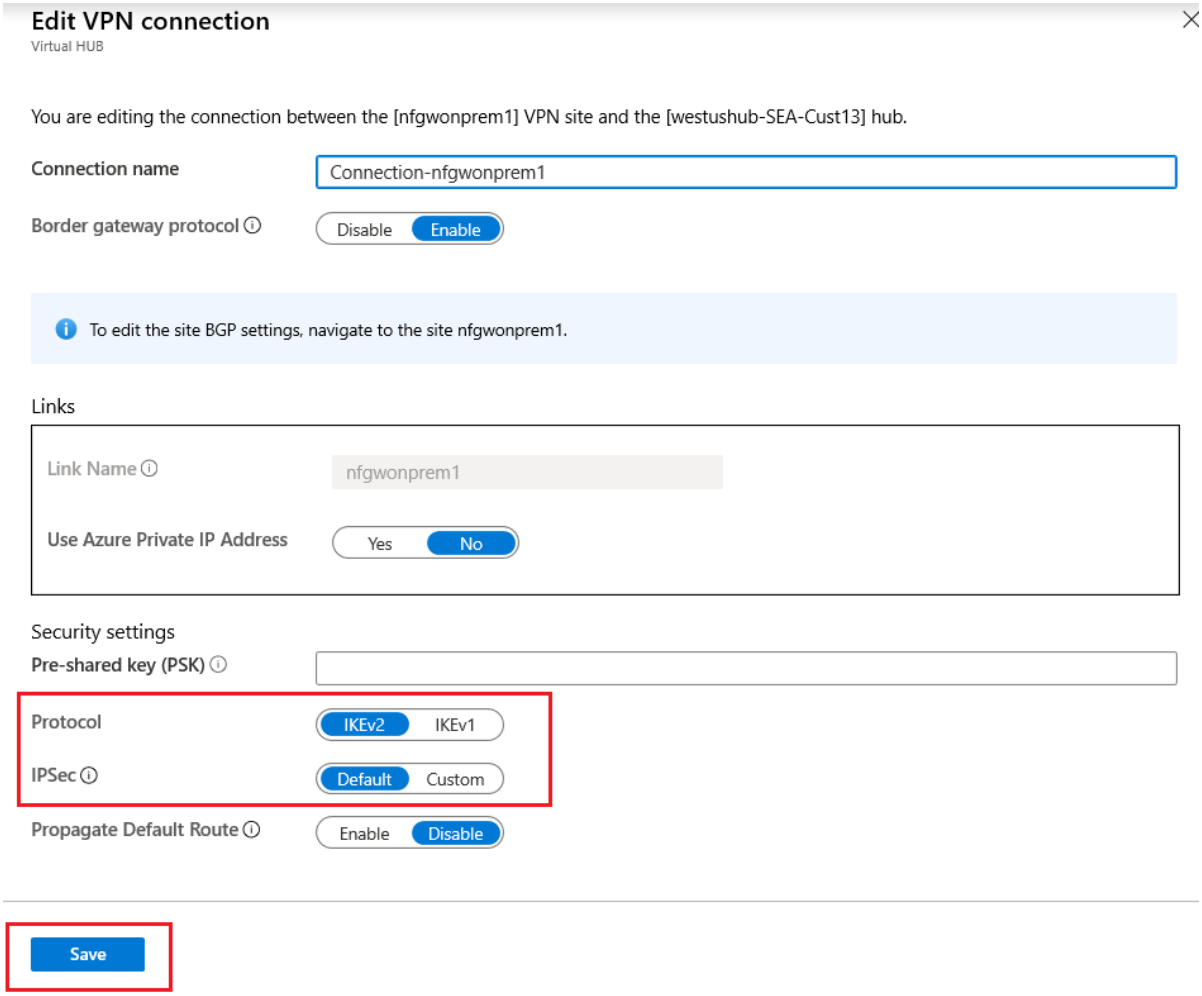
Configure a policy

1. **Locate the virtual hub**. From a browser, navigate to the Azure portal and sign in with your Azure account. Locate the virtual hub for your site.
2. **Select the VPN site**. From the hub page, select the VPN Site for which you want to set up a custom policy.



3. **Edit the VPN connection**. From the **Context menu ...**, select **Edit VPN Connection**.

4. **Configure the settings**. On the **Edit VPN connection** page, configure the settings the settings. Select **Save** to save your settings.



Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Generate and export certificates for Virtual WAN user VPN connections

11/4/2019 • 7 minutes to read • Edit Online

User VPN connections use certificates to authenticate. This article shows you how to create a self-signed root certificate and generate client certificates using PowerShell on Windows 10 or Windows Server 2016.

You must perform the steps in this article on a computer running Windows 10 or Windows Server 2016. The PowerShell cmdlets that you use to generate certificates are part of the operating system and do not work on other versions of Windows. The Windows 10 or Windows Server 2016 computer is only needed to generate the certificates. Once the certificates are generated, you can upload them, or install them on any supported client operating system.

Create a self-signed root certificate

Use the New-SelfSignedCertificate cmdlet to create a self-signed root certificate. For additional parameter information, see New-SelfSignedCertificate.

1. From a computer running Windows 10 or Windows Server 2016, open a Windows PowerShell console with elevated privileges. These examples do not work in the Azure Cloud Shell "Try It". You must run these examples locally.
2. Use the following example to create the self-signed root certificate. The following example creates a self-signed root certificate named 'P2SRootCert' that is automatically installed in 'Certificates-Current User\Personal\Certificates'. You can view the certificate by opening *certmgr.msc*, or *Manage User Certificates*.

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

Generate a client certificate

Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

The following steps walk you through generating a client certificate from a self-signed root certificate. You may generate multiple client certificates from the same root certificate. When you generate client certificates using the steps below, the client certificate is automatically installed on the computer that you used to generate the certificate. If you want to install a client certificate on another client computer, you can export the certificate.

The examples use the New-SelfSignedCertificate cmdlet to generate a client certificate that expires in one year. For additional parameter information, such as setting a different expiration value for the client certificate, see New-SelfSignedCertificate.

Example 1

Use this example if you have not closed your PowerShell console after creating the self-signed root certificate. This example continues from the previous section and uses the declared '$cert' variable. If you closed the PowerShell

console after creating the self-signed root certificate, or are creating additional client certificates in a new PowerShell console session, use the steps in Example 2.

Modify and run the example to generate a client certificate. If you run the following example without modifying it, the result is a client certificate named 'P2SChildCert'. If you want to name the child certificate something else, modify the CN value. Do not change the TextExtension when running this example. The client certificate that you generate is automatically installed in 'Certificates - Current User\Personal\Certificates' on your computer.

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Example 2

If you are creating additional client certificates, or are not using the same PowerShell session that you used to create your self-signed root certificate, use the following steps:

1. Identify the self-signed root certificate that is installed on the computer. This cmdlet returns a list of certificates that are installed on your computer.

   ```
   Get-ChildItem -Path "Cert:\CurrentUser\My"
   ```

2. Locate the subject name from the returned list, then copy the thumbprint that is located next to it to a text file. In the following example, there are two certificates. The CN name is the name of the self-signed root certificate from which you want to generate a child certificate. In this case, 'P2SRootCert'.

   ```
   Thumbprint                                Subject

   AED812AD883826FF76B4D1D5A77B3C08EFA79F3F  CN=P2SChildCert4
   7181AA8C1B4D34EEDB2F3D3BEC5839F3FE52D655  CN=P2SRootCert
   ```

3. Declare a variable for the root certificate using the thumbprint from the previous step. Replace THUMBPRINT with the thumbprint of the root certificate from which you want to generate a child certificate.

   ```
   $cert = Get-ChildItem -Path "Cert:\CurrentUser\My\THUMBPRINT"
   ```

   For example, using the thumbprint for P2SRootCert in the previous step, the variable looks like this:

   ```
   $cert = Get-ChildItem -Path "Cert:\CurrentUser\My\7181AA8C1B4D34EEDB2F3D3BEC5839F3FE52D655"
   ```

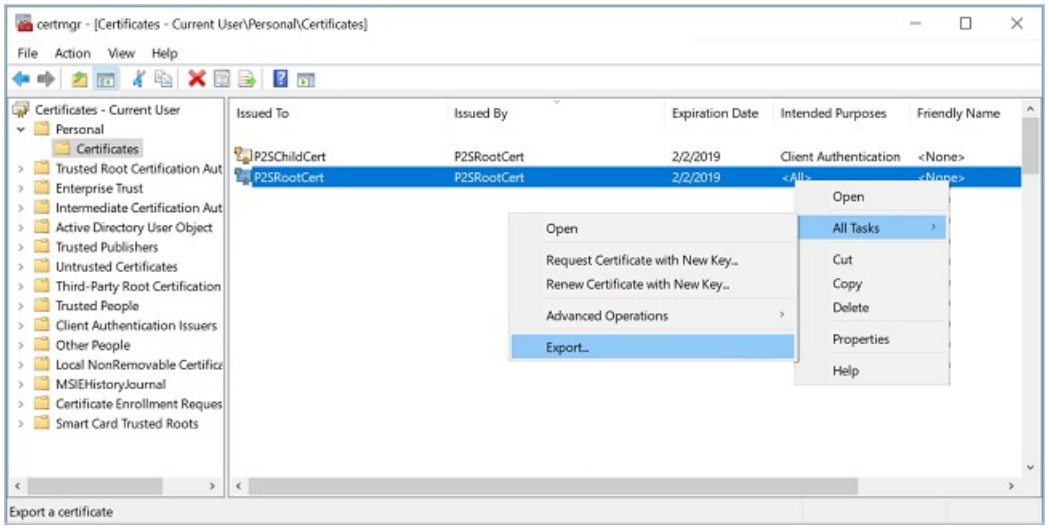
4. Modify and run the example to generate a client certificate. If you run the following example without modifying it, the result is a client certificate named 'P2SChildCert'. If you want to name the child certificate something else, modify the CN value. Do not change the TextExtension when running this example. The client certificate that you generate is automatically installed in 'Certificates - Current User\Personal\Certificates' on your computer.

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

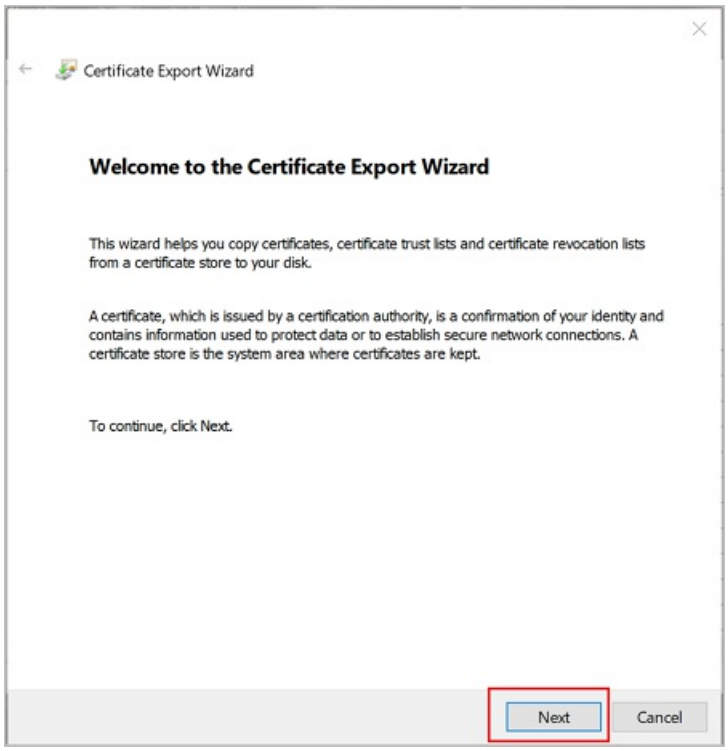
Export the root certificate public key (.cer)

After creating a self-signed root certificate, export the root certificate public key .cer file (not the private key). You will later upload this file to Azure. The following steps help you export the .cer file for your self-signed root certificate:

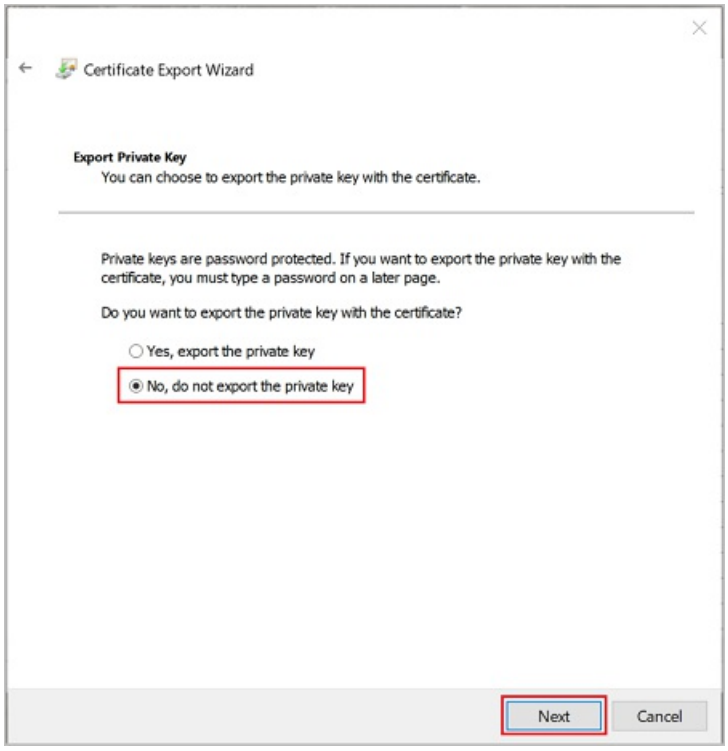
1. To obtain a .cer file from the certificate, open **Manage user certificates**. Locate the self-signed root certificate, typically in 'Certificates - Current User\Personal\Certificates', and right-click. Click **All Tasks**, and then click **Export**. This opens the **Certificate Export Wizard**. If you can't find the certificate under Current User\Personal\Certificates, you may have accidentally opened "Certificates - Local Computer", rather than "Certificates - Current User"). If you want to open Certificate Manager in current user scope using PowerShell, you type *certmgr* in the console window.



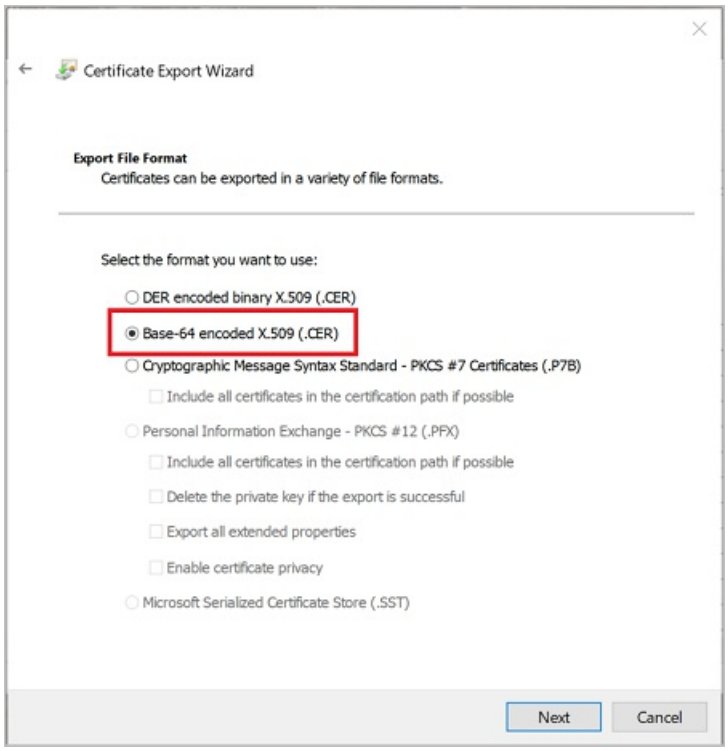
2. In the Wizard, click **Next**.



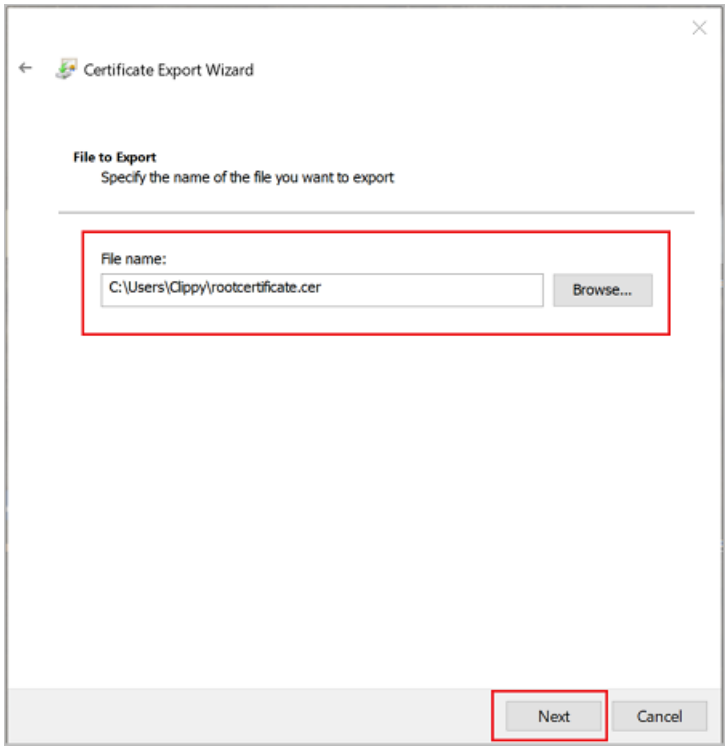
3. Select **No, do not export the private key**, and then click **Next**.



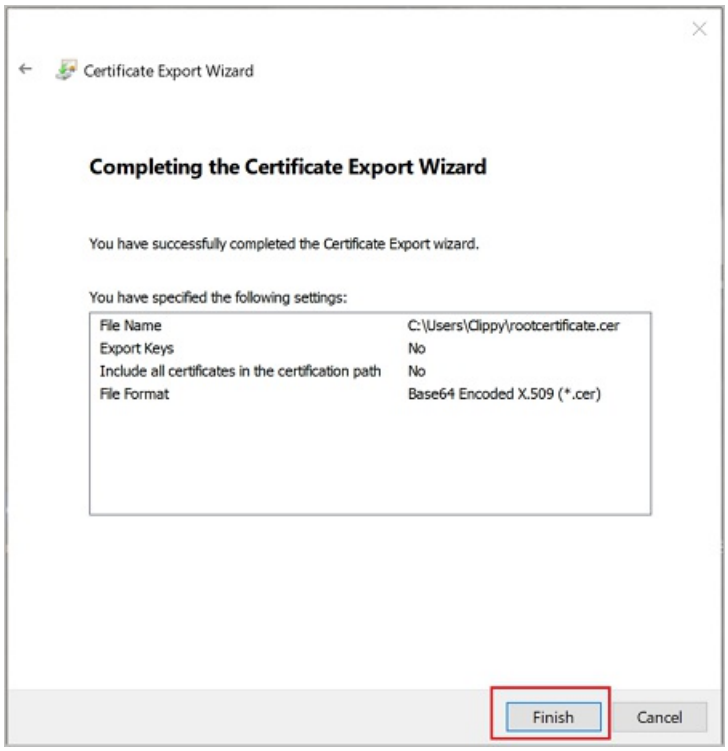
4. On the **Export File Format** page, select **Base-64 encoded X.509 (.CER).**, and then click **Next**.



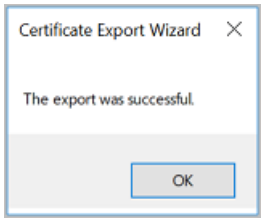
5. For **File to Export**, **Browse** to the location to which you want to export the certificate. For **File name**, name the certificate file. Then, click **Next**.



6. Click **Finish** to export the certificate.

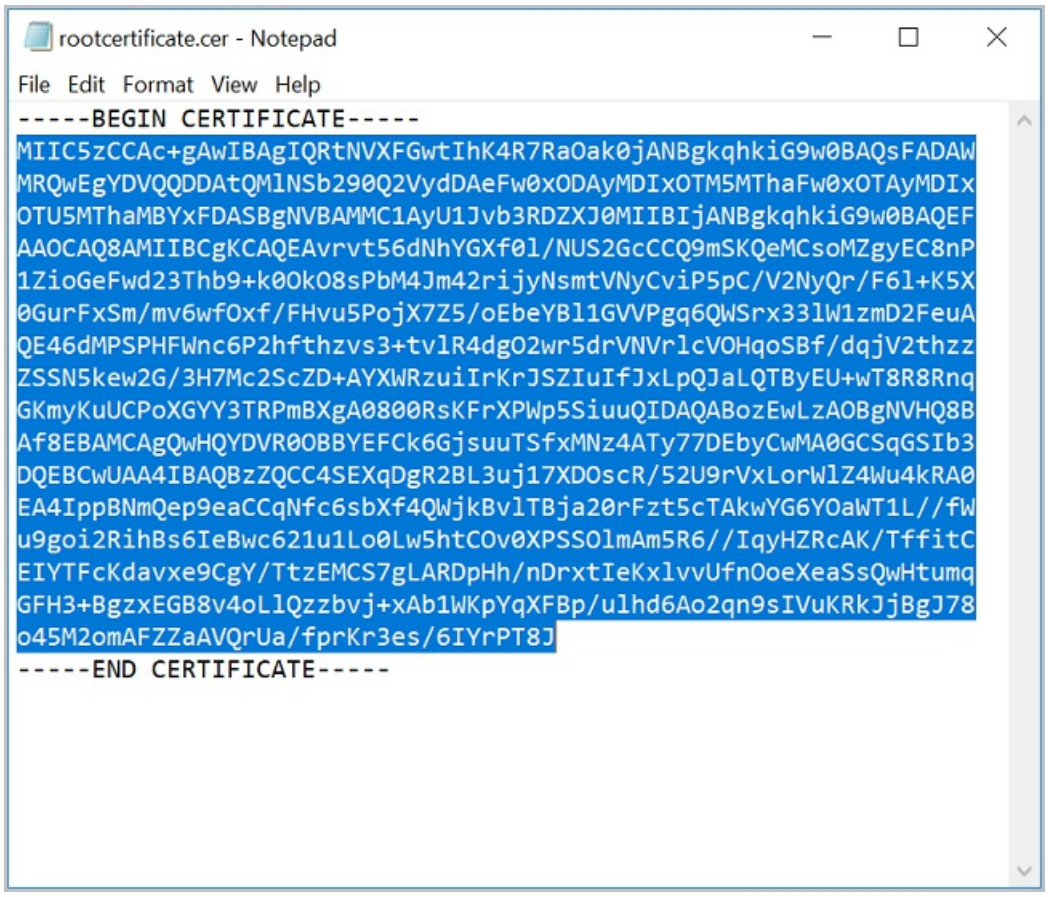


7. Your certificate is successfully exported.



8. The exported certificate looks similar to this:

9. If you open the exported certificate using Notepad, you see something similar to this example. The section in blue contains the information that is uploaded to Azure. If you open your certificate with Notepad and it does not look similar to this, typically this means you did not export it using the Base-64 encoded X.509(.CER) format. Additionally, if you want to use a different text editor, understand that some editors can introduce unintended formatting in the background. This can create problems when uploaded the text from this certificate to Azure.



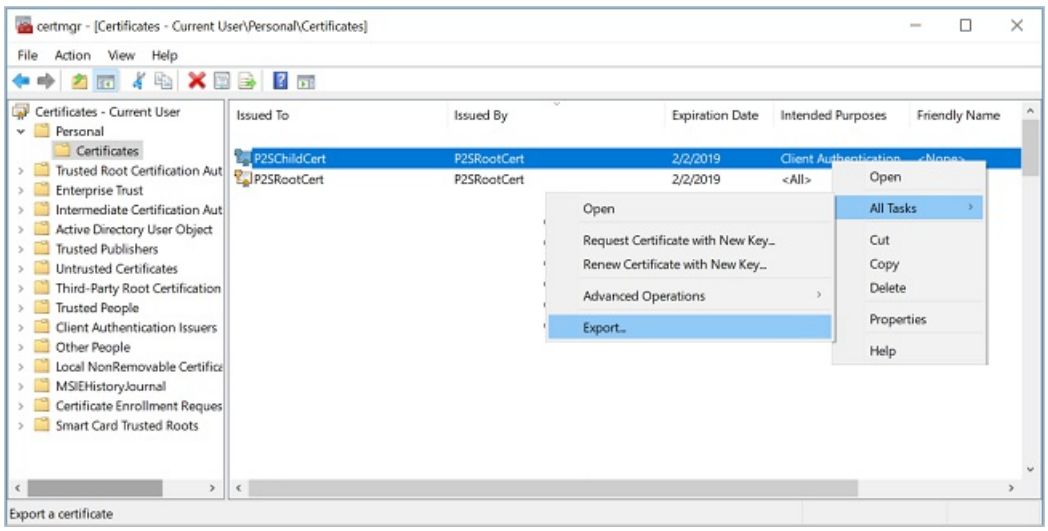
Export the self-signed root certificate and private key to store it (optional)

You may want to export the self-signed root certificate and store it safely as backup. If need be, you can later install it on another computer and generate more client certificates. To export the self-signed root certificate as a .pfx, select the root certificate and use the same steps as described in Export a client certificate.

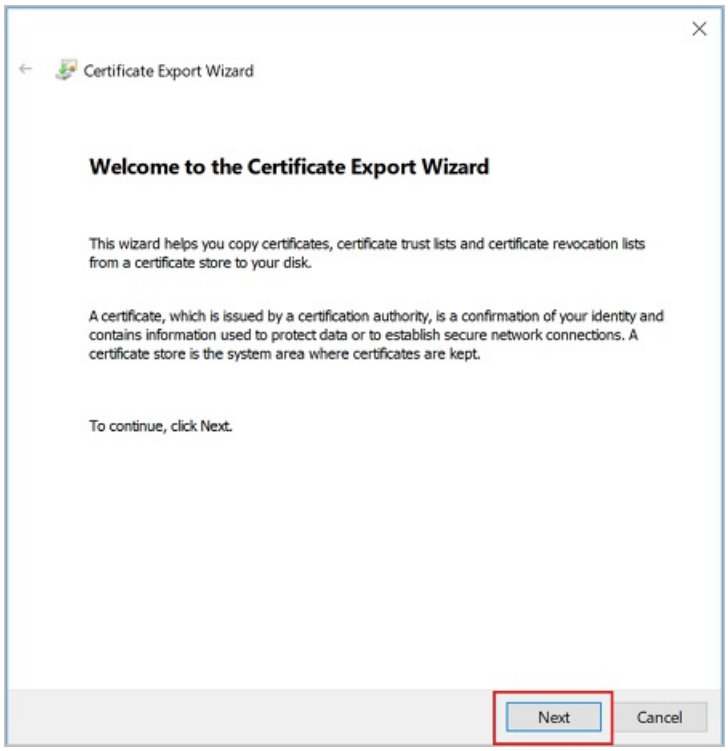
Export the client certificate

When you generate a client certificate, it's automatically installed on the computer that you used to generate it. If you want to install the client certificate on another client computer, you need to export the client certificate that you generated.

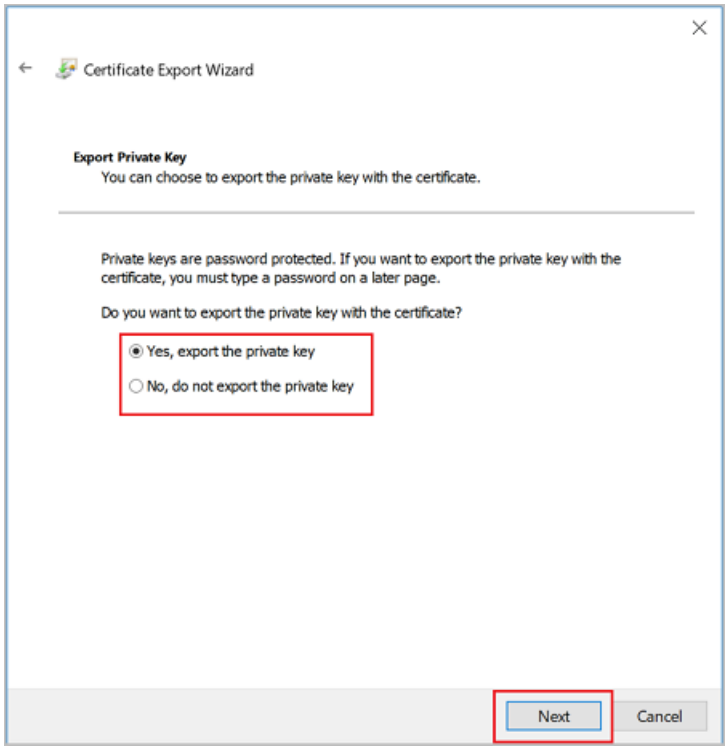
1. To export a client certificate, open **Manage user certificates**. The client certificates that you generated are, by default, located in 'Certificates - Current User\Personal\Certificates'. Right-click the client certificate that you want to export, click **all tasks**, and then click **Export** to open the **Certificate Export Wizard**.



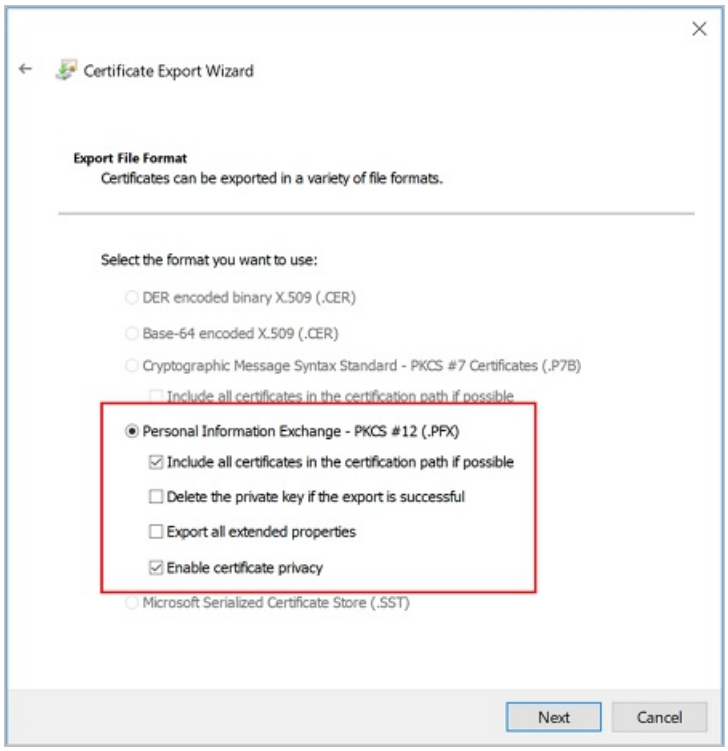
2. In the Certificate Export Wizard, click **Next** to continue.



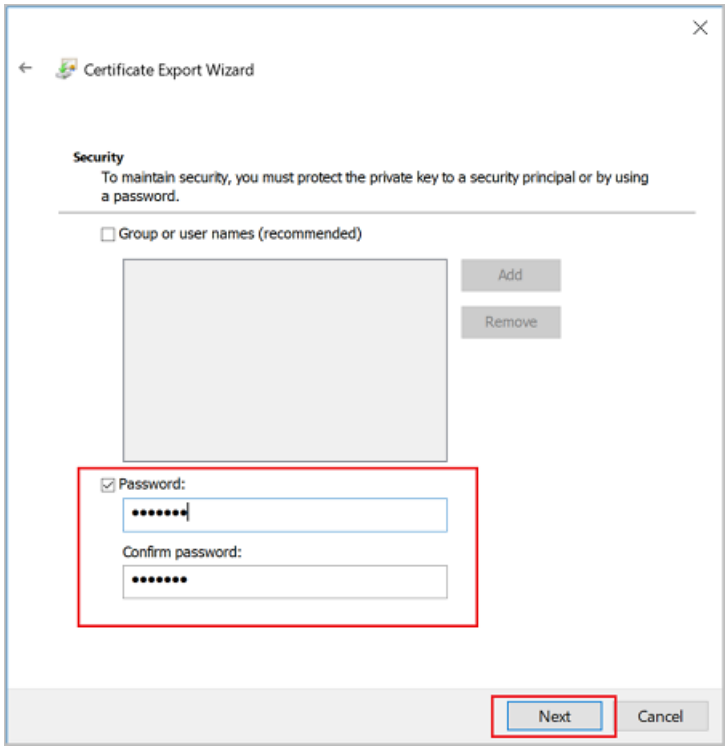
3. Select **Yes, export the private key**, and then click **Next**.



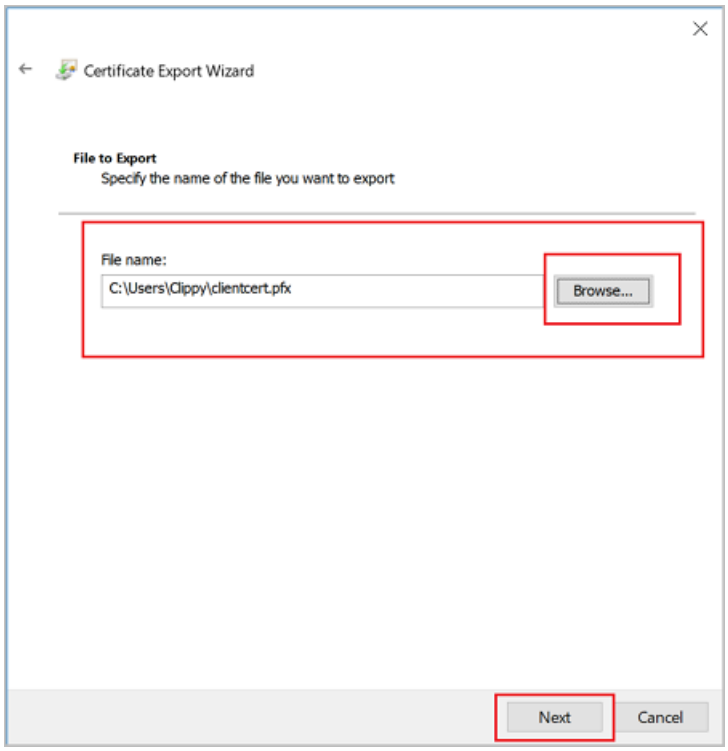
4. On the **Export File Format** page, leave the defaults selected. Make sure that **Include all certificates in the certification path if possible** is selected. This setting additionally exports the root certificate information that is required for successful client authentication. Without it, client authentication fails because the client doesn't have the trusted root certificate. Then, click **Next**.



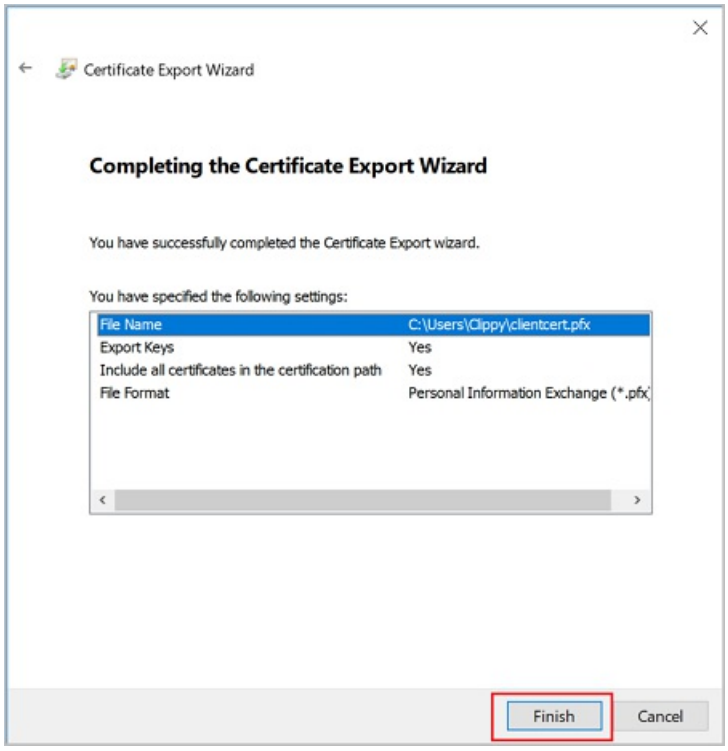
5. On the **Security** page, you must protect the private key. If you select to use a password, make sure to record or remember the password that you set for this certificate. Then, click **Next**.



6. On the **File to Export**, **Browse** to the location to which you want to export the certificate. For **File name**, name the certificate file. Then, click **Next**.



7. Click **Finish** to export the certificate.



Next steps

Continue with the Virtual WAN steps for user VPN connection

Create an Azure Active Directory tenant for P2S OpenVPN protocol connections

1/13/2020 • 2 minutes to read • Edit Online

When connecting to your VNet, you can use certificate-based authentication or RADIUS authentication. However, when you use the Open VPN protocol, you can also use Azure Active Directory authentication. This article helps you set up an Azure AD tenant for P2S Open VPN authentication.

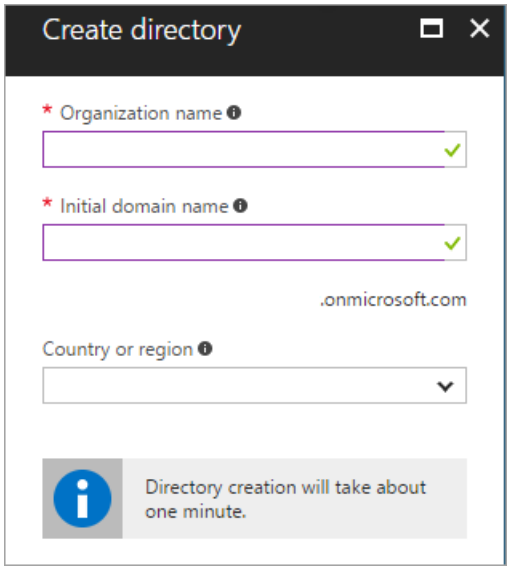
> **NOTE**
> Azure AD authentication is supported only for OpenVPN® protocol connections.

1. Create the Azure AD tenant

Create an Azure AD tenant using the steps in the Create a new tenant article:

- Organizational name
- Initial domain name

Example:



2. Create Azure AD tenant users

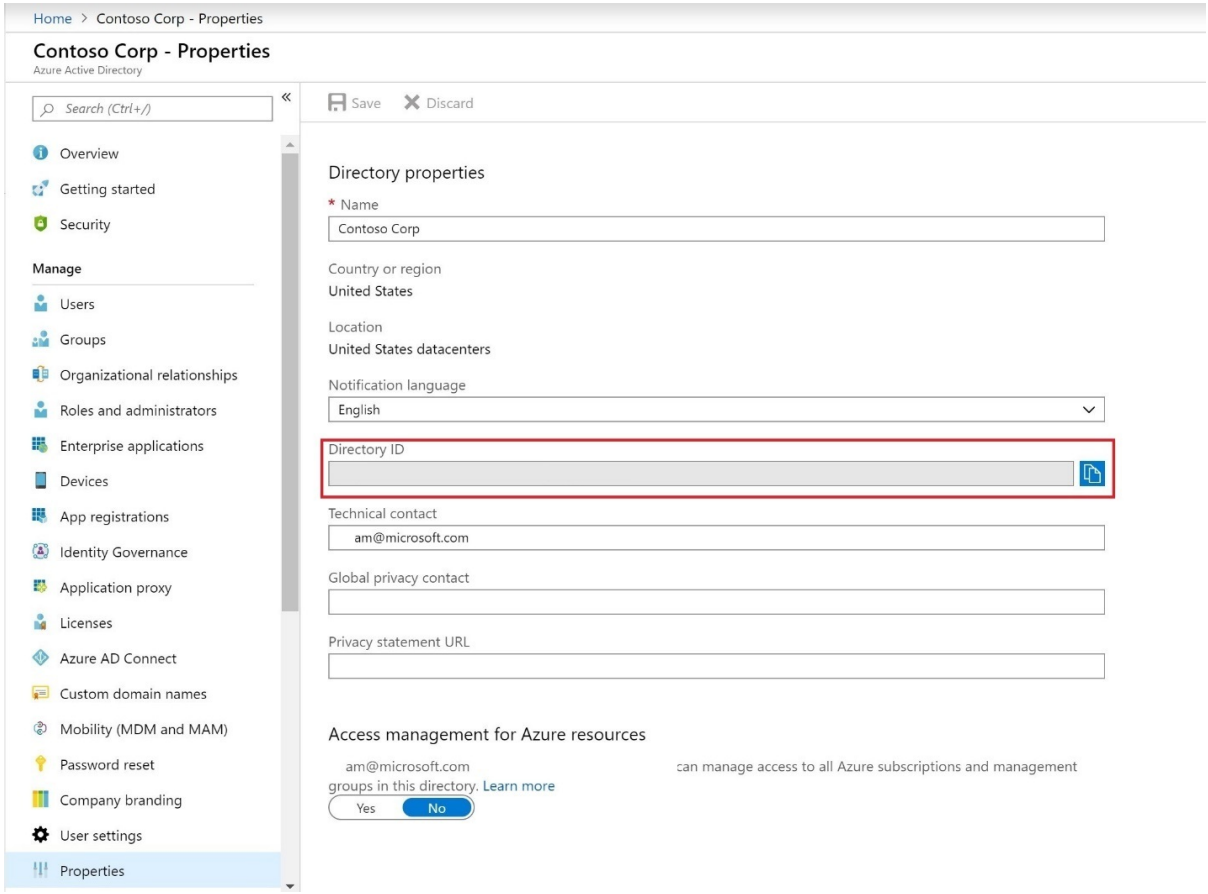
Next, create two user accounts. Create one Global Admin account and one master user account. The master user account is used as your master embedding account (service account). When you create an Azure AD tenant user account, you adjust the Directory role for the type of user that you want to create.

Use the steps in this article to create at least two users for your Azure AD tenant. Be sure to change the **Directory Role** to create the account types:

- Global Admin
- User

3. Enable Azure AD authentication on the VPN gateway

1. Locate the Directory ID of the directory that you want to use for authentication. It is listed in the properties section of the Active Directory page.



2. Copy the Directory ID.
3. Sign in to the Azure portal as a user that is assigned the **Global administrator** role.
4. Next, give admin consent. Copy and paste the URL that pertains to your deployment location in the address bar of your browser:

   Public

   ```
   https://login.microsoftonline.com/common/oauth2/authorize?client_id=41b23e61-6c1e-4545-b367-cd054e0ed4b4&response_type=code&redirect_uri=https://portal.azure.com&nonce=1234&prompt=admin_consent
   ```

   Azure Government

   ```
   https://login-us.microsoftonline.com/common/oauth2/authorize?client_id=51bb15d4-3a4f-4ebf-9dca-40096fe32426&response_type=code&redirect_uri=https://portal.azure.us&nonce=1234&prompt=admin_consent
   ```

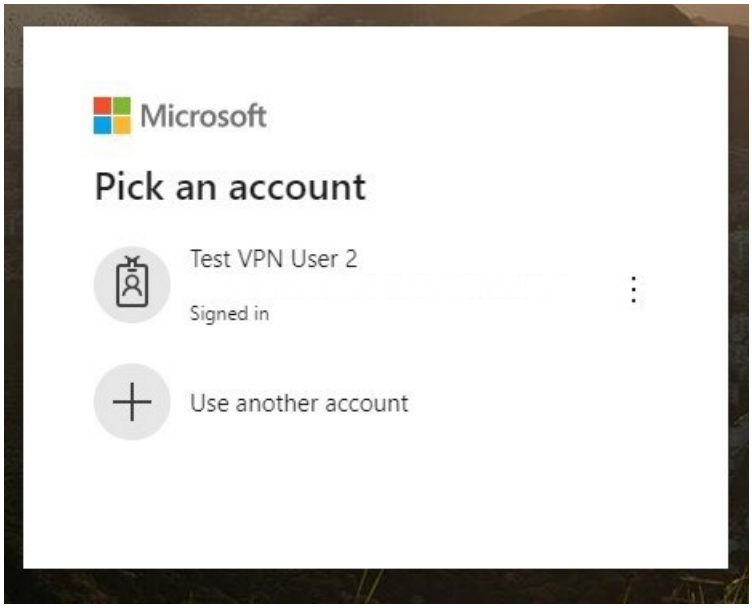
   Microsoft Cloud Germany

   ```
   https://login-us.microsoftonline.de/common/oauth2/authorize?client_id=538ee9e6-310a-468d-afef-ea97365856a9&response_type=code&redirect_uri=https://portal.microsoftazure.de&nonce=1234&prompt=admin_consent
   ```

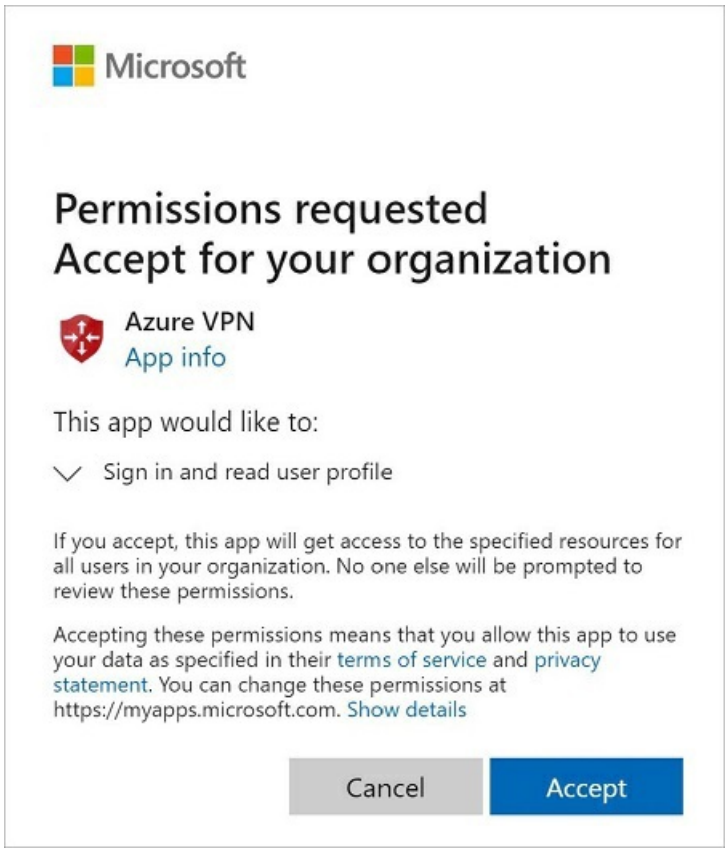
   Azure China 21Vianet

   ```
   https://https://login.chinacloudapi.cn/common/oauth2/authorize?client_id=49f817b6-84ae-4cc0-928c-73f27289b3aa&response_type=code&redirect_uri=https://portal.azure.cn&nonce=1234&prompt=admin_consent
   ```

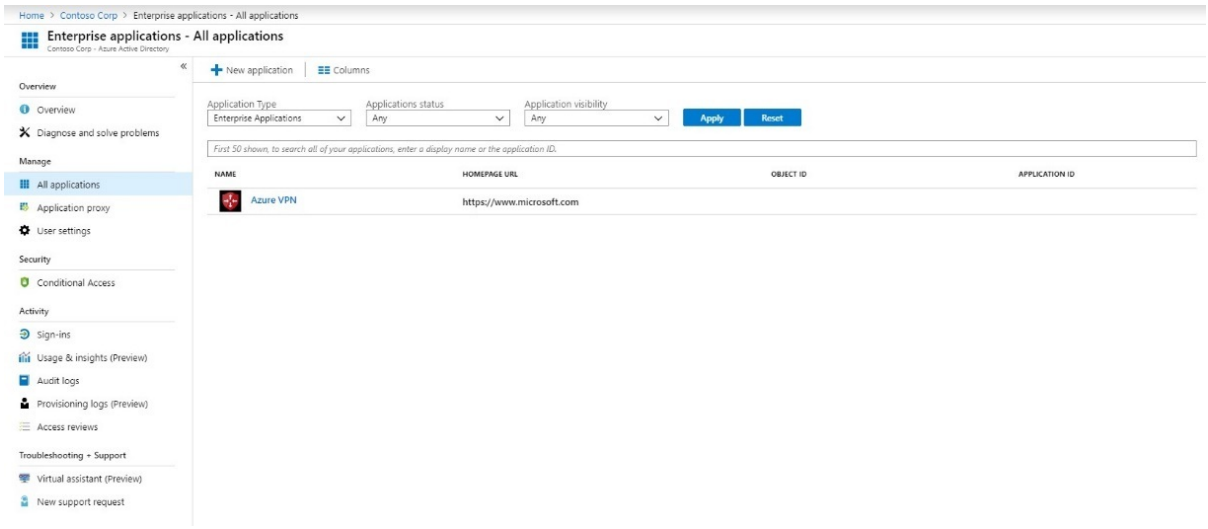
5. Select the **Global Admin** account if prompted.



6. Select **Accept** when prompted.



7. Under your Azure AD, in **Enterprise applications**, you see **Azure VPN** listed.



8. Configure Azure AD authentication for User VPN and assign it to a Virtual Hub by following the steps in Configure Azure AD authentication for Point-to-Site connection to Azure

Next steps

In order to connect to your virtual network, you must create and configure a VPN client profile and associate it to a Virtual Hub. See Configure Azure AD authentication for Point-to-Site connection to Azure.

Enable Azure Multi-Factor Authentication (MFA) for VPN users

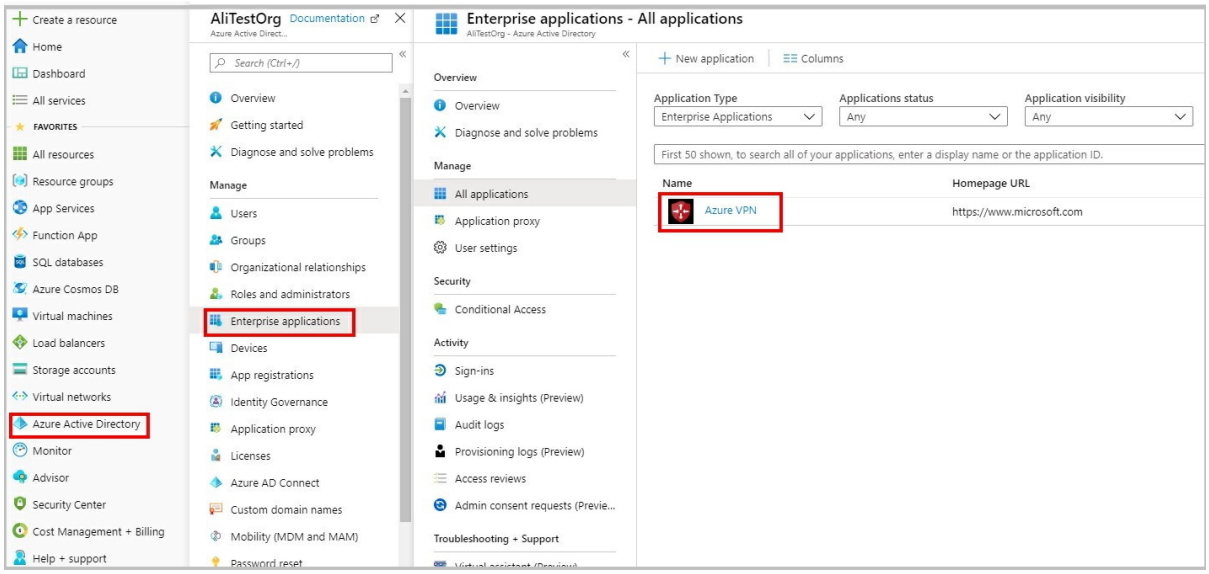
2/19/2020 • 2 minutes to read • Edit Online

If you want users to be prompted for a second factor of authentication before granting access, you can configure Azure Multi-Factor Authentication (MFA). You can configure MFA on a per user basis, or you can leverage MFA via Conditional Access.

- MFA per user can be enabled at no-additional cost. When enabling MFA per user, the user will be prompted for second factor authentication against all applications tied to the Azure AD tenant. See Option 1 for steps.
- Conditional Access allows for finer-grained control over how a second factor should be promoted. It can allow assignment of MFA to only VPN, and exclude other applications tied to the Azure AD tenant. See Option 2 for steps.

Enable authentication

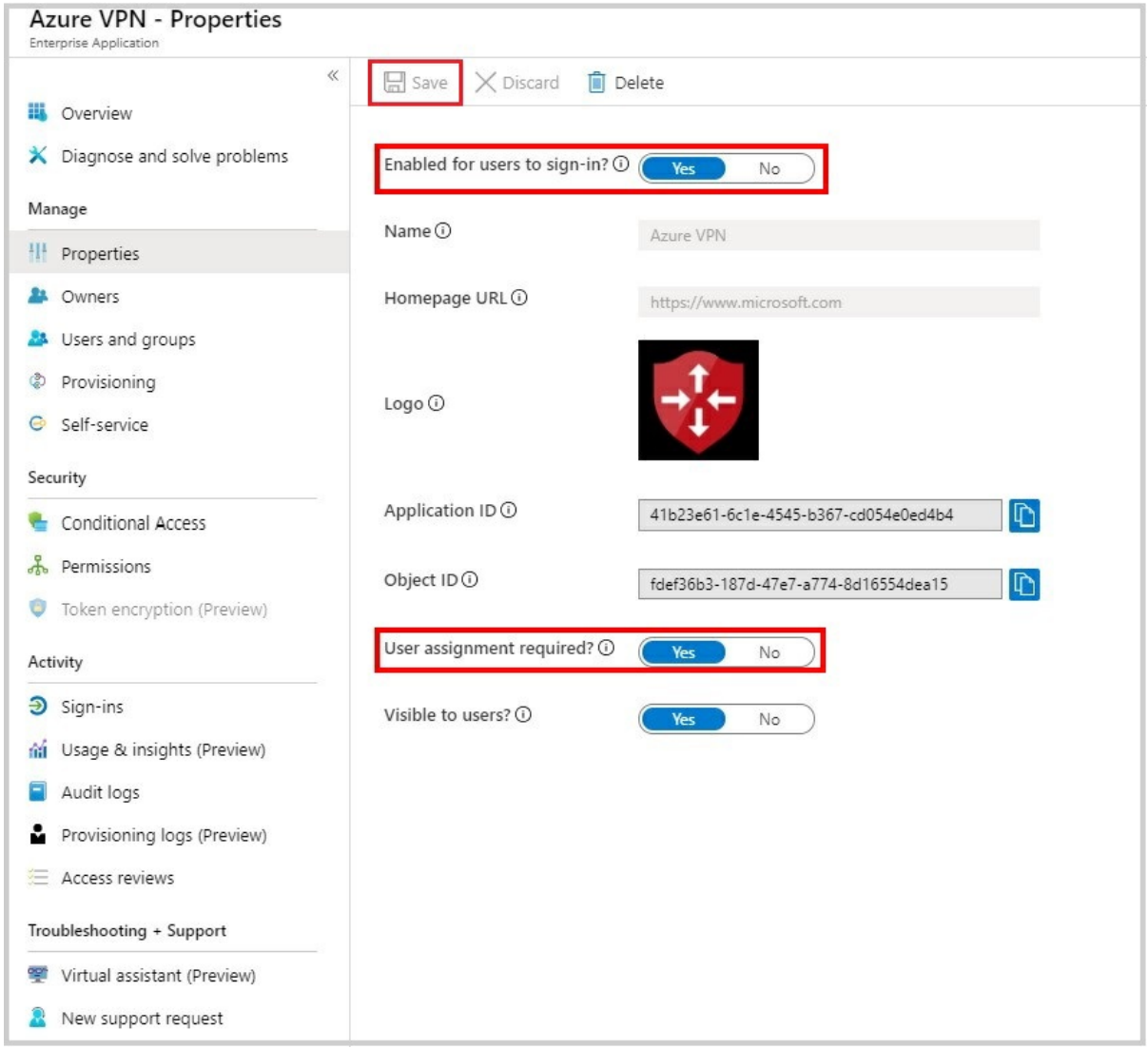
1. Navigate to **Azure Active Directory -> Enterprise applications -> All applications**.
2. On the **Enterprise applications - All applications** page, select **Azure VPN**.



Configure sign-in settings

On the **Azure VPN - Properties** page, configure sign-in settings.

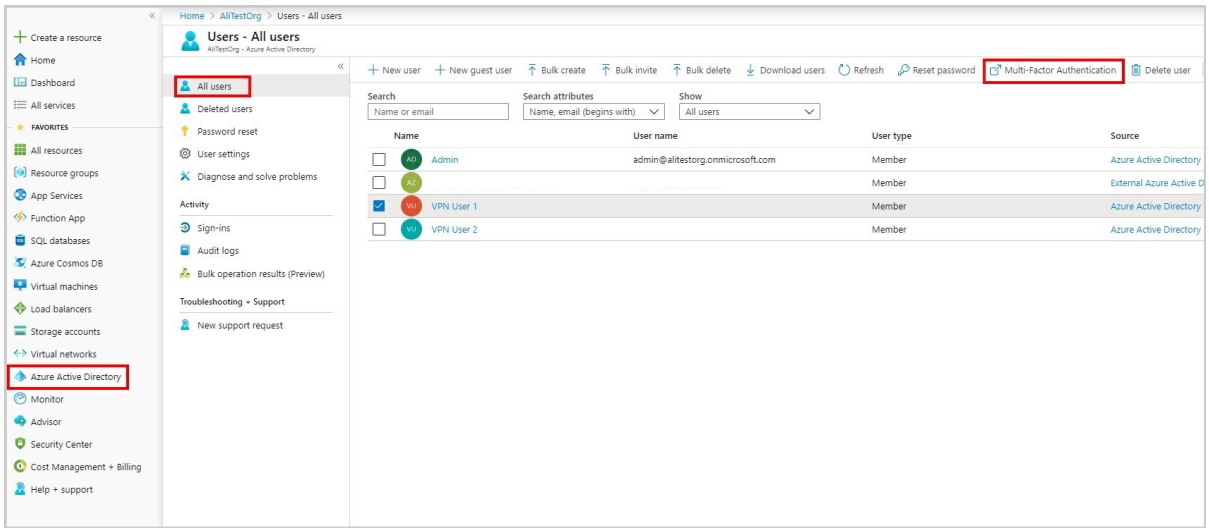
1. Set **Enabled for users to sign-in?** to **Yes**. This setting allows all users in the AD tenant to connect to the VPN successfully.
2. Set **User assignment required?** to **Yes** if you want to limit sign-in to only users that have permissions to the Azure VPN.
3. Save your changes.



Option 1 - Per User access

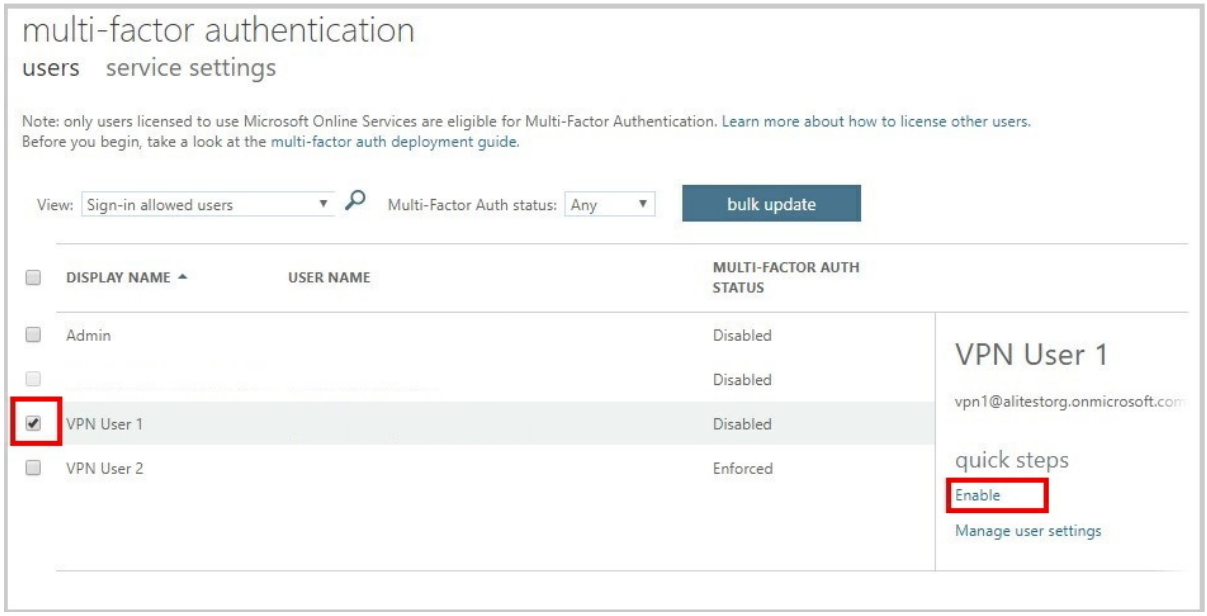
Open the MFA page

1. Sign in to the Azure portal.
2. Navigate to **Azure Active Directory -> All users**.
3. Select **Multi-Factor Authentication** to open the multi-factor authentication page.



Select users

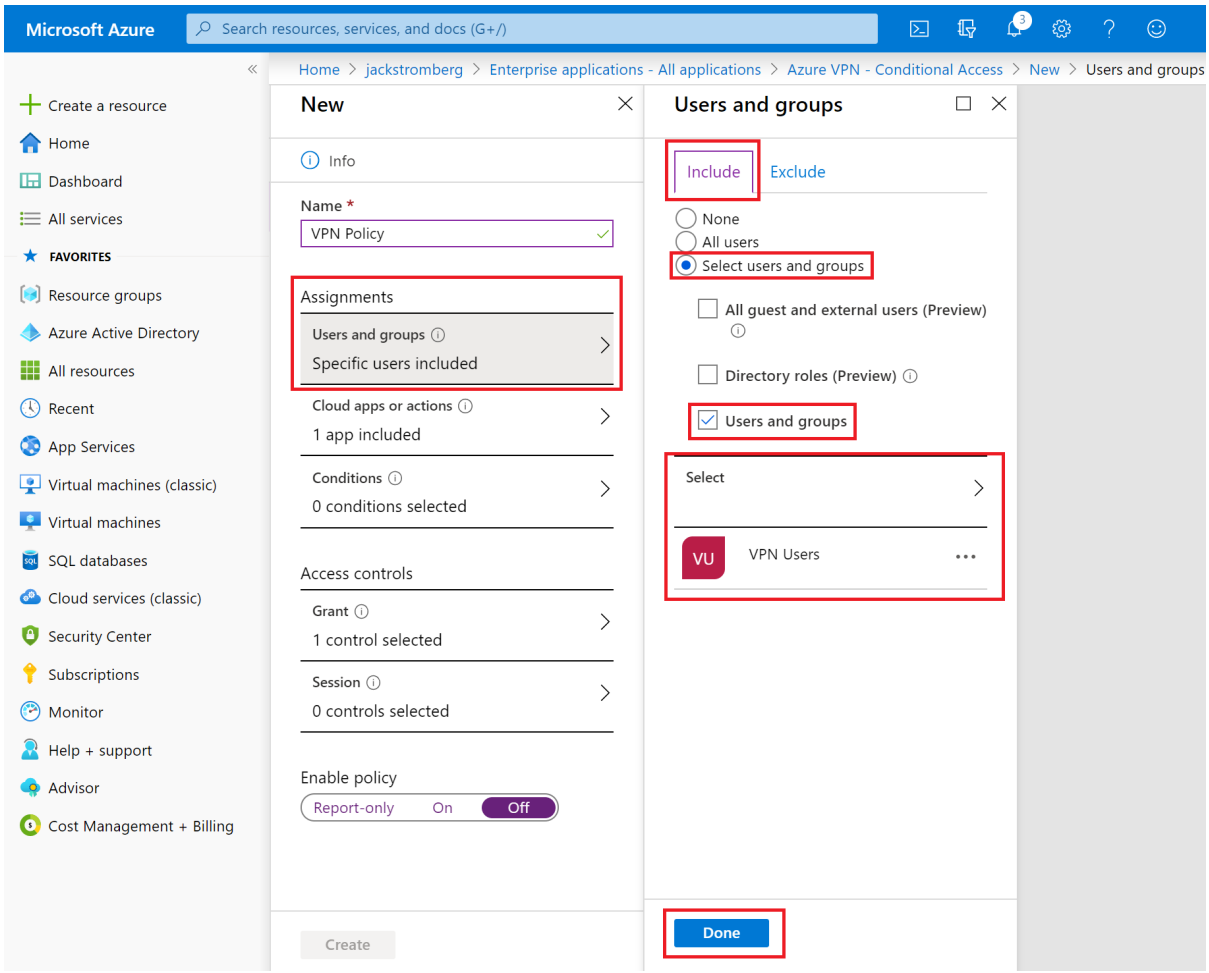
1. On the **multi-factor authentication** page, select the user(s) for whom you want to enable MFA.
2. Select **Enable**.



Option 2 - Conditional Access

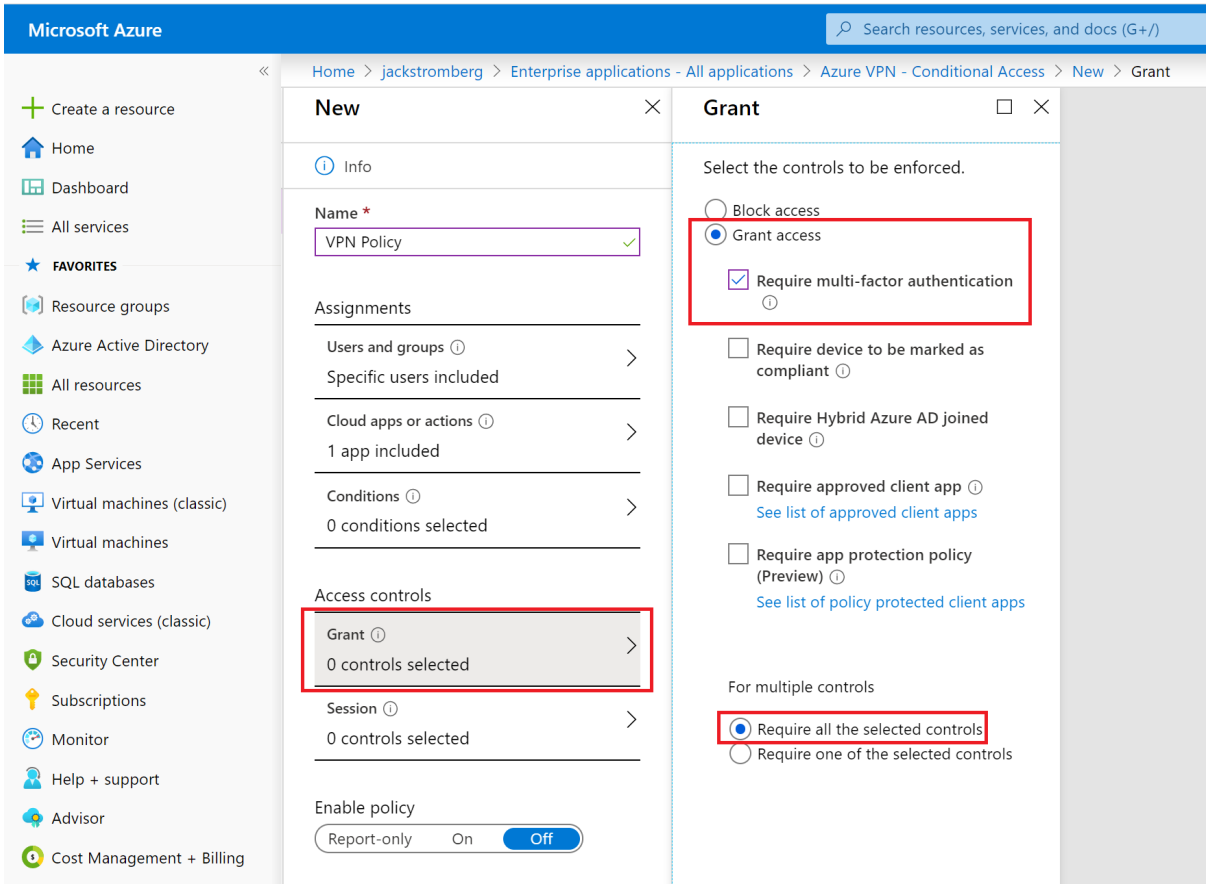
Conditional Access allows for fine-grained access control on a per-application basis. In order to use Conditional Access, you should have Azure AD Premium 1 or greater licensing applied to the users that will be subject to the Conditional Access rules.

1. Navigate to the **Enterprise applications - All applications** page and click **Azure VPN**.
   - Click **Conditional Access**.
   - Click **New policy** to open the **New** pane.
2. On the **New** pane, navigate to **Assignments -> Users and groups**. On the **Users and groups -> Include** tab:
   - Click **Select users and groups**.
   - Check **Users and groups**.
   - Click **Select** to select a group or set of users to be affected by MFA.
   - Click **Done**.

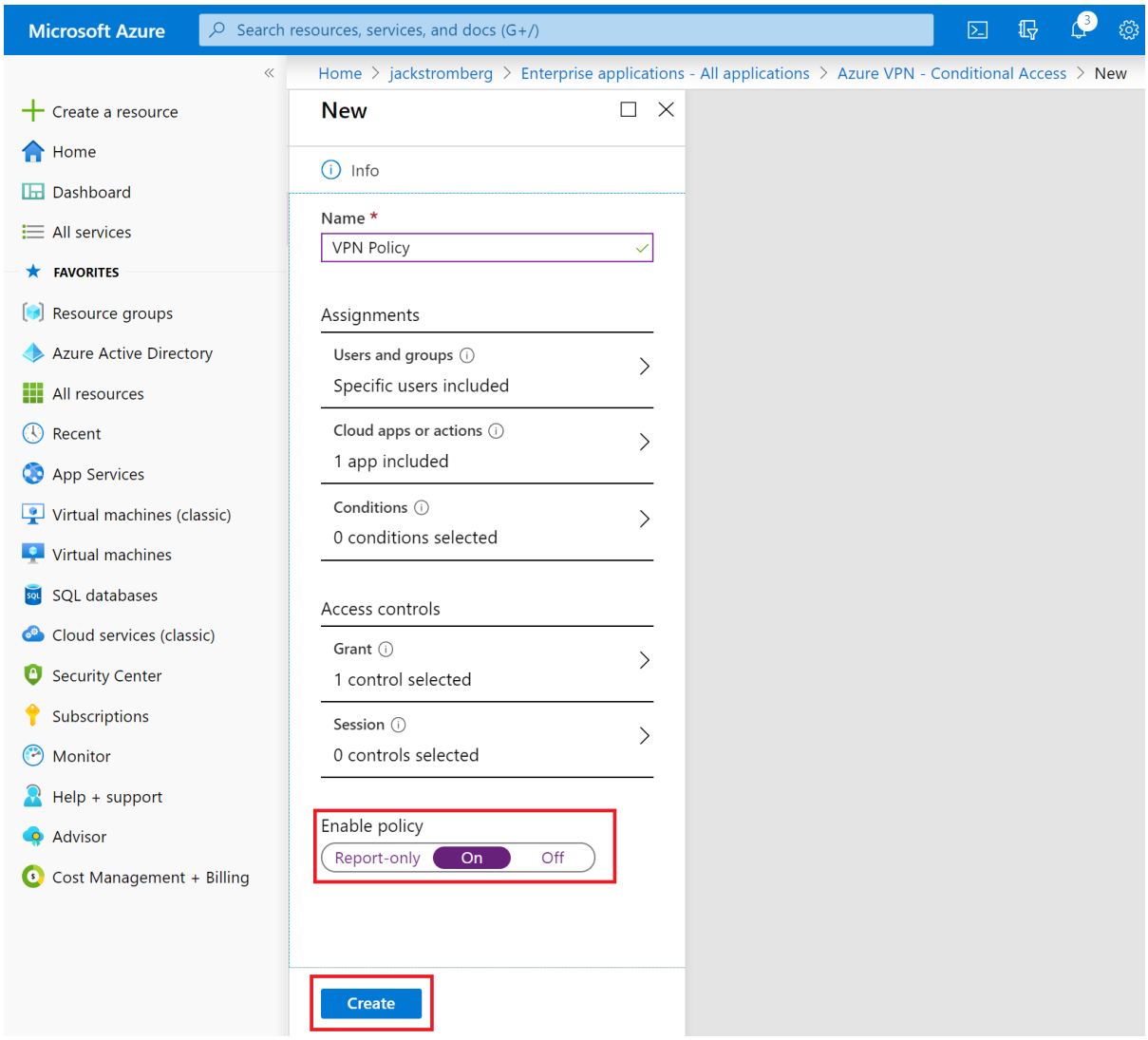


3. On the **New** pane, navigate to the **Access controls -> Grant** pane:

   - Click **Grant access**.
   - Click **Require multi-factor authentication**.
   - Click **Require all the selected controls**.
   - Click **Select**.



4. In the **Enable policy** section:
   - Select **On**.
   - Click **Create**.



Next steps

To connect to your virtual network, you must create and configure a VPN client profile. See Configure Azure AD authentication for Point-to-Site connection to Azure.

Tutorial: Create a User VPN connection by using Azure Virtual WAN

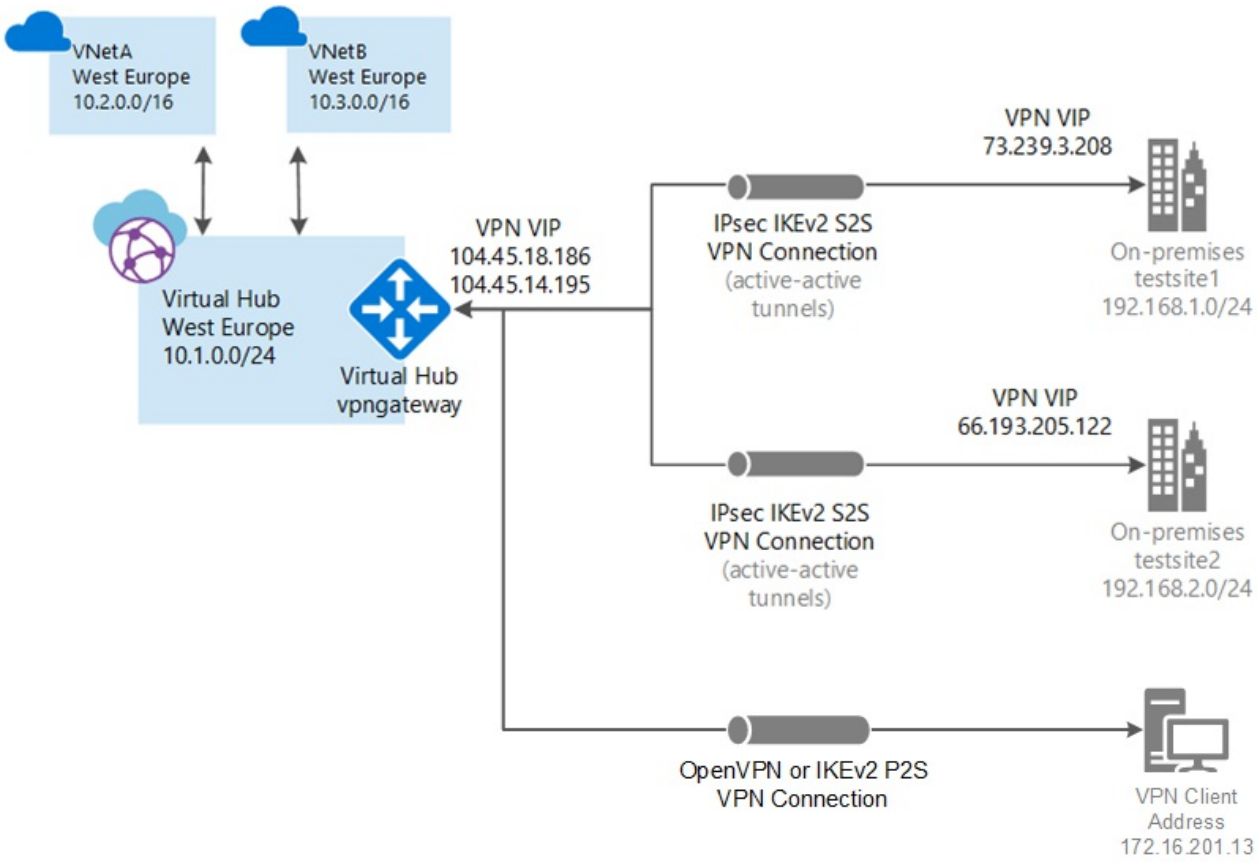
2/10/2020 • 5 minutes to read • Edit Online

This tutorial shows you how to configure Azure AD authentication for User VPN in Virtual WAN to connect to your resources in Azure over an OpenVPN VPN connection. Azure Active Directory authentication is only available for gateways using OpenVPN protocol and clients running Windows.

This type of connection requires a client to be configured on the client computer. For more information about Virtual WAN, see the Virtual WAN Overview.

In this tutorial, you learn how to:

- Create a WAN
- Create a hub
- Create a P2S configuration
- Download a VPN client profile
- Apply P2S configuration to a hub
- Connect a VNet to a hub
- Download and apply the VPN client configuration
- View your virtual WAN
- View resource health



Before you begin

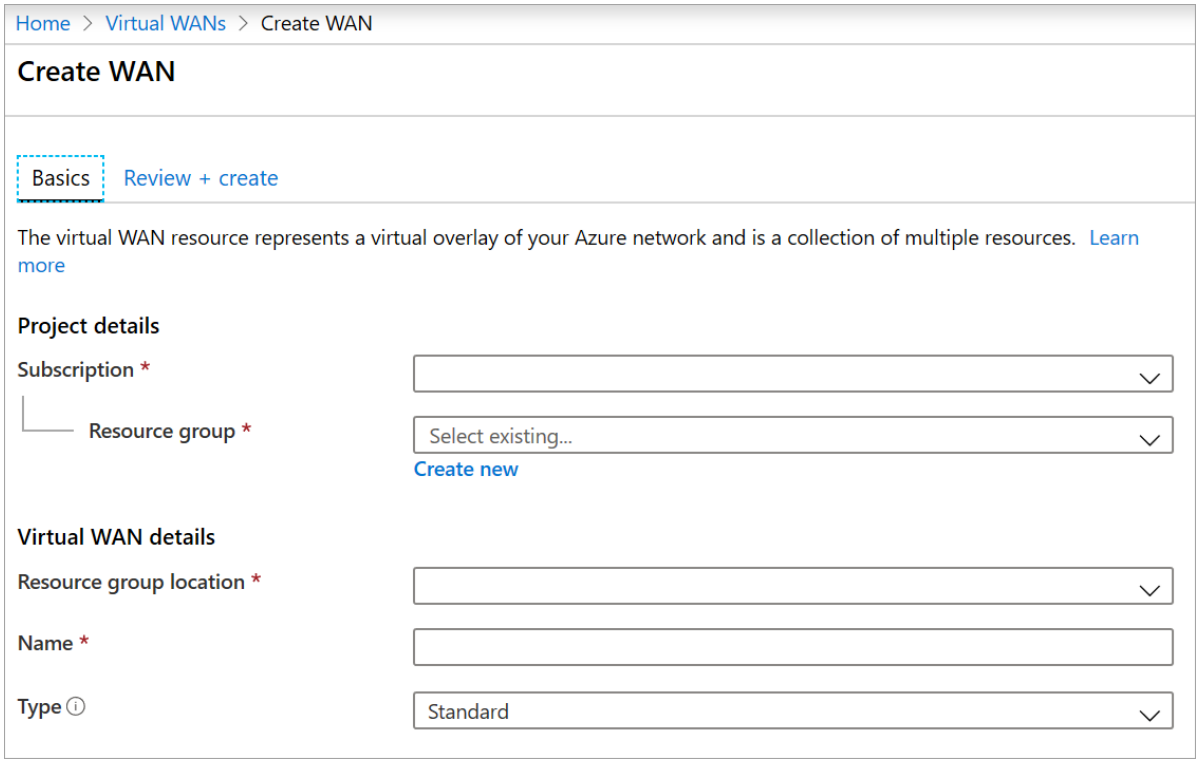
Verify that you have met the following criteria before beginning your configuration:

- You have a virtual network that you want to connect to. Verify that none of the subnets of your on-premises networks overlap with the virtual networks that you want to connect to. To create a virtual network in the Azure portal, see the Quickstart.
- Your virtual network does not have any virtual network gateways. If your virtual network has a gateway (either VPN or ExpressRoute), you must remove all gateways. This configuration requires that virtual networks are connected instead, to the Virtual WAN hub gateway.
- Obtain an IP address range for your hub region. The hub is a virtual network that is created and used by Virtual WAN. The address range that you specify for the hub cannot overlap with any of your existing virtual networks that you connect to. It also cannot overlap with your address ranges that you connect to on premises. If you are unfamiliar with the IP address ranges located in your on-premises network configuration, coordinate with someone who can provide those details for you.
- If you don't have an Azure subscription, create a free account.

Create a virtual WAN

From a browser, navigate to the Azure portal and sign in with your Azure account.

1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create** to open the Create WAN page.
3. On the **Create WAN** page, on the **Basics** tab, fill in the following fields:



- **Subscription** - Select the subscription that you want to use.
- **Resource group** - Create new or use existing.
- **Resource group location** - Choose a resource location from the dropdown. A WAN is a global resource and does not live in a particular region. However, you must select a region in order to more easily manage and locate the WAN resource that you create.
- **Name** - Type the Name that you want to call your WAN.
- **Type:** Standard. If you create a Basic WAN, you can create only a Basic hub. Basic hubs are capable of

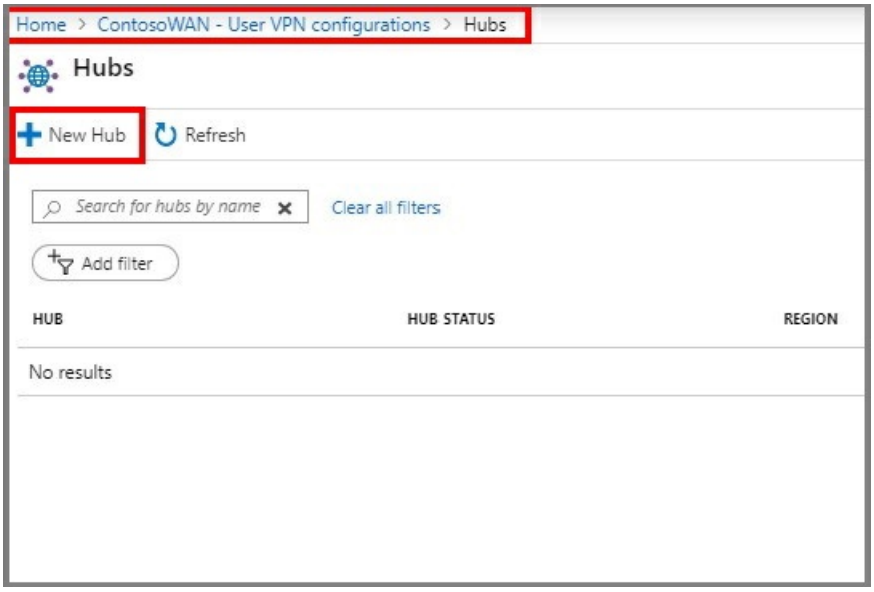
VPN site-to-site connectivity only.

4. After you finish filling out the fields, select **Review +Create**.

5. After validation passes, select **Create** to create the virtual WAN.

Create an empty virtual hub

1. Under your virtual WAN, select Hubs and click **+New Hub**.

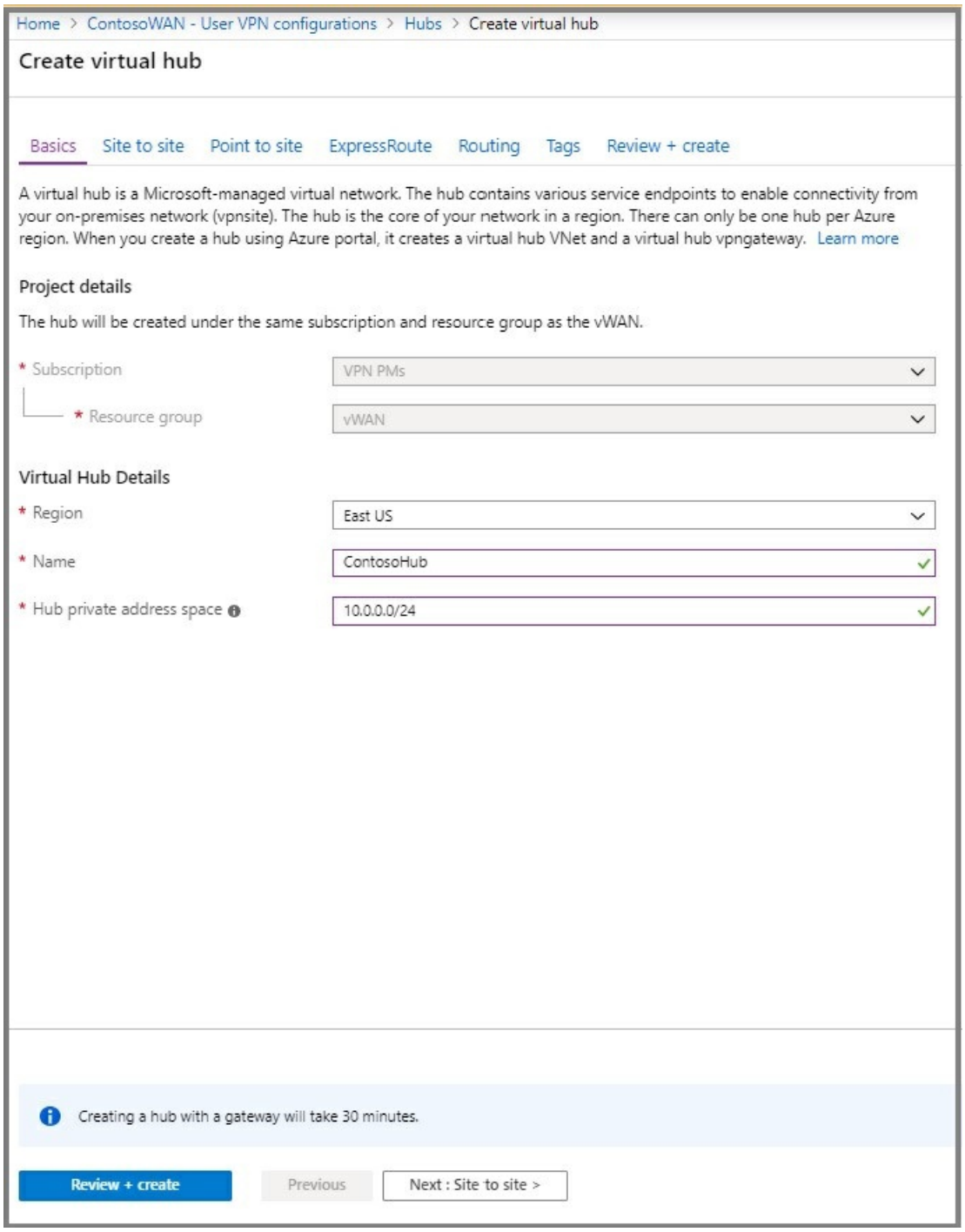


2. On the create virtual hub page, fill in the following fields.

   Region - Select the region that you want to deploy the virtual hub in.

   Name - Enter the name that you want to call your virtual hub.

   Hub private address space - The hub's address range in CIDR notation.

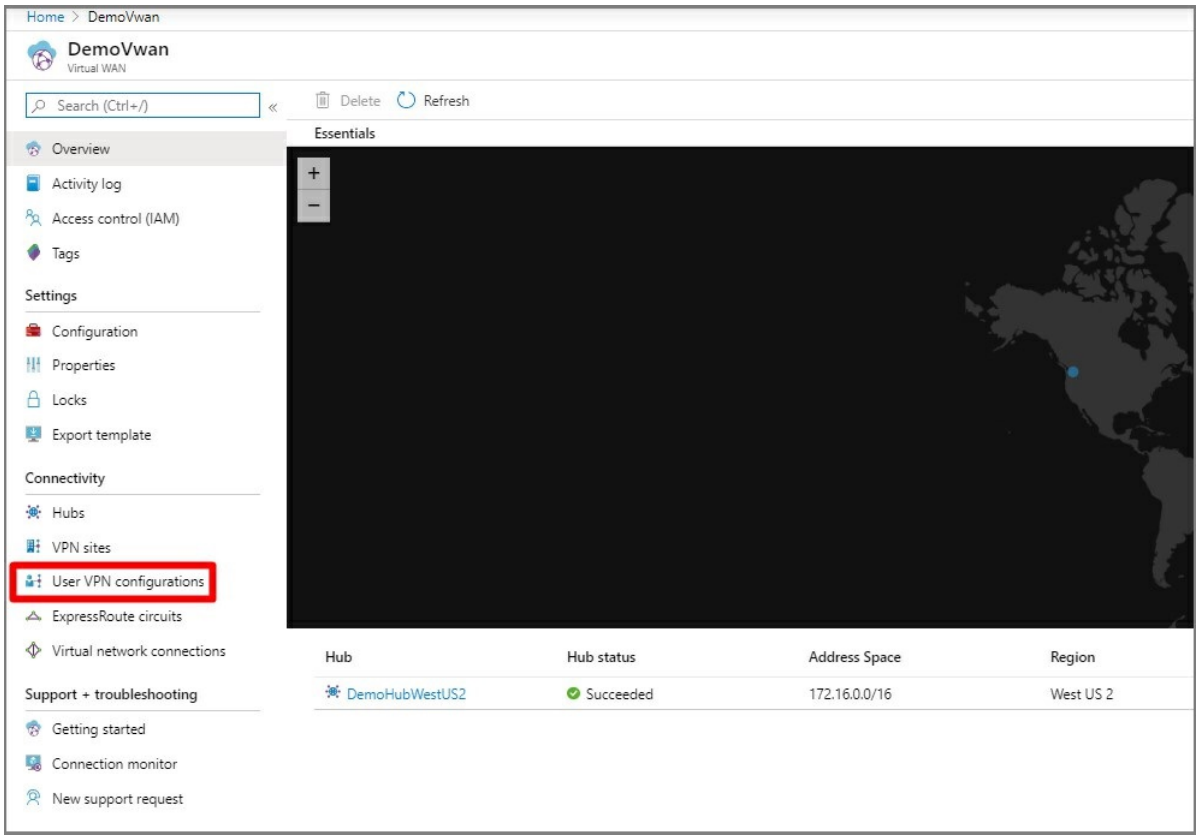


3. Click **Review + create**.
4. On the **validation passed** page, click **create**.

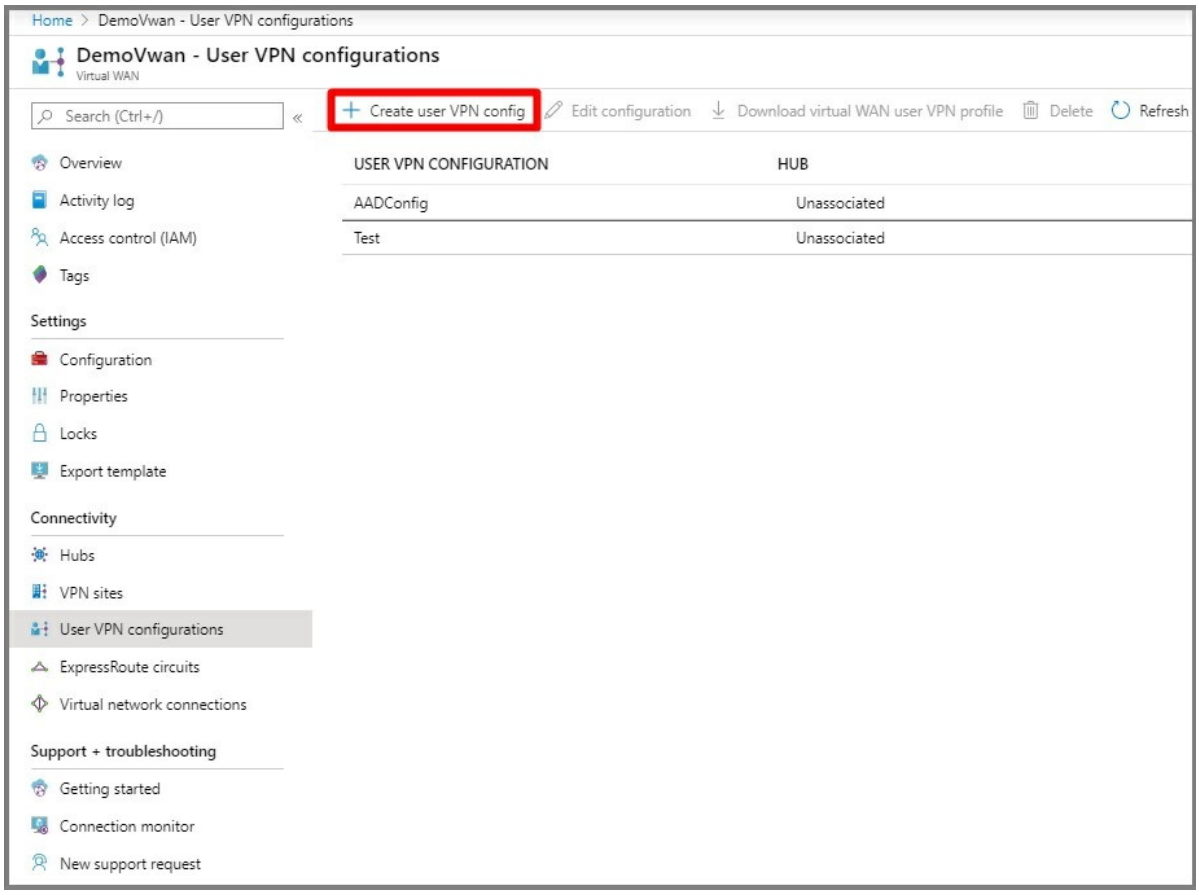
Create a new P2S configuration

A P2S configuration defines the parameters for connecting remote clients.

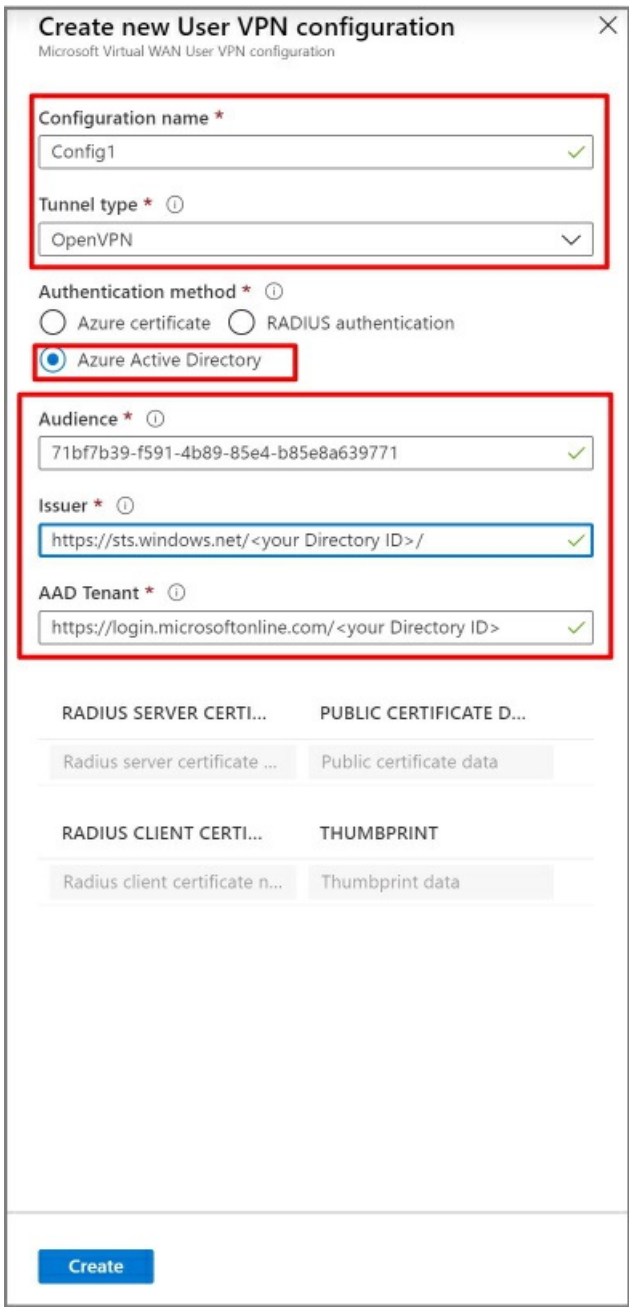
1. Under your virtual WAN, select **User VPN configurations**.



2. click **+Create user VPN config**.



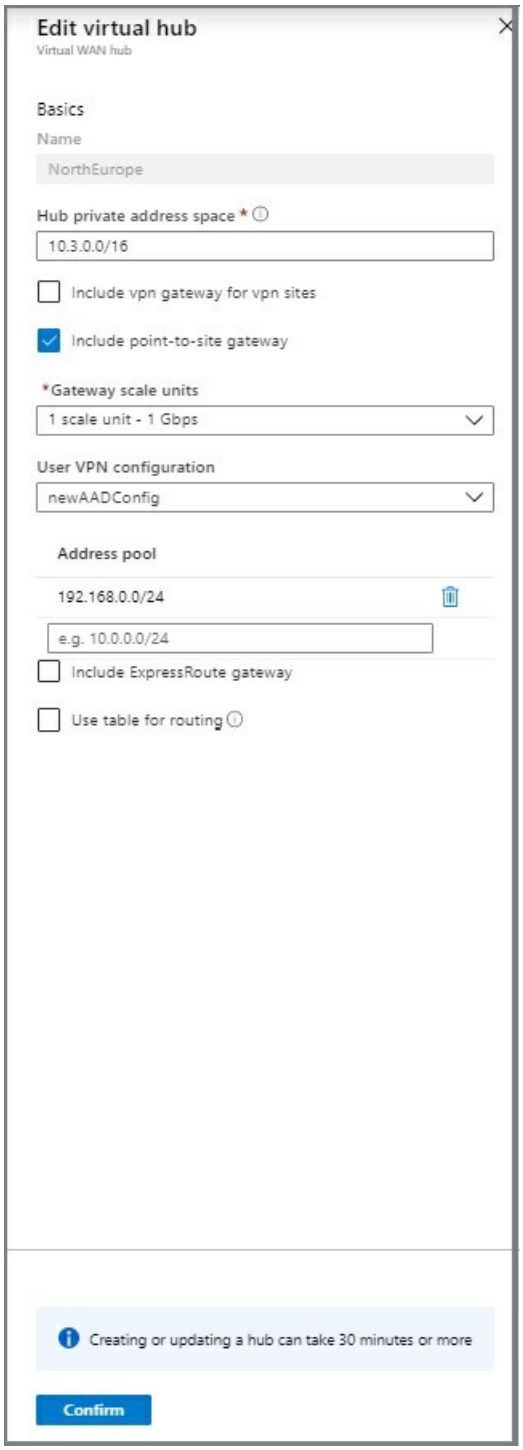
3. Enter the information and click **Create**



Edit hub assignment

1. Navigate to the **Hubs** blade under the virtual WAN.
2. Select the hub that you want to associate the vpn server configuration to and click the ellipsis (...).

3. Click **Edit virtual hub**.
4. Check the **Include point-to-site gateway** check box and pick the **Gateway scale unit** that you want.



5. Enter the **Address pool** from which the VPN clients will be assigned IP addresses.
6. Click **Confirm**.
7. The operation will can take up to 30 minutes to complete.

Download VPN profile

Use the VPN profile to configure your clients.

1. On the page for your virtual WAN, click **User VPN configurations**.
2. At the top of the page, click **Download user VPN config**.
3. Once the file has finished creating, you can click the link to download it.
4. Use the profile file to configure the VPN clients.

Configure user VPN clients

To connect, you need to download the Azure VPN Client and import the VPN client profile that was downloaded in the previous steps on every computer that wants to connect to the VNet.

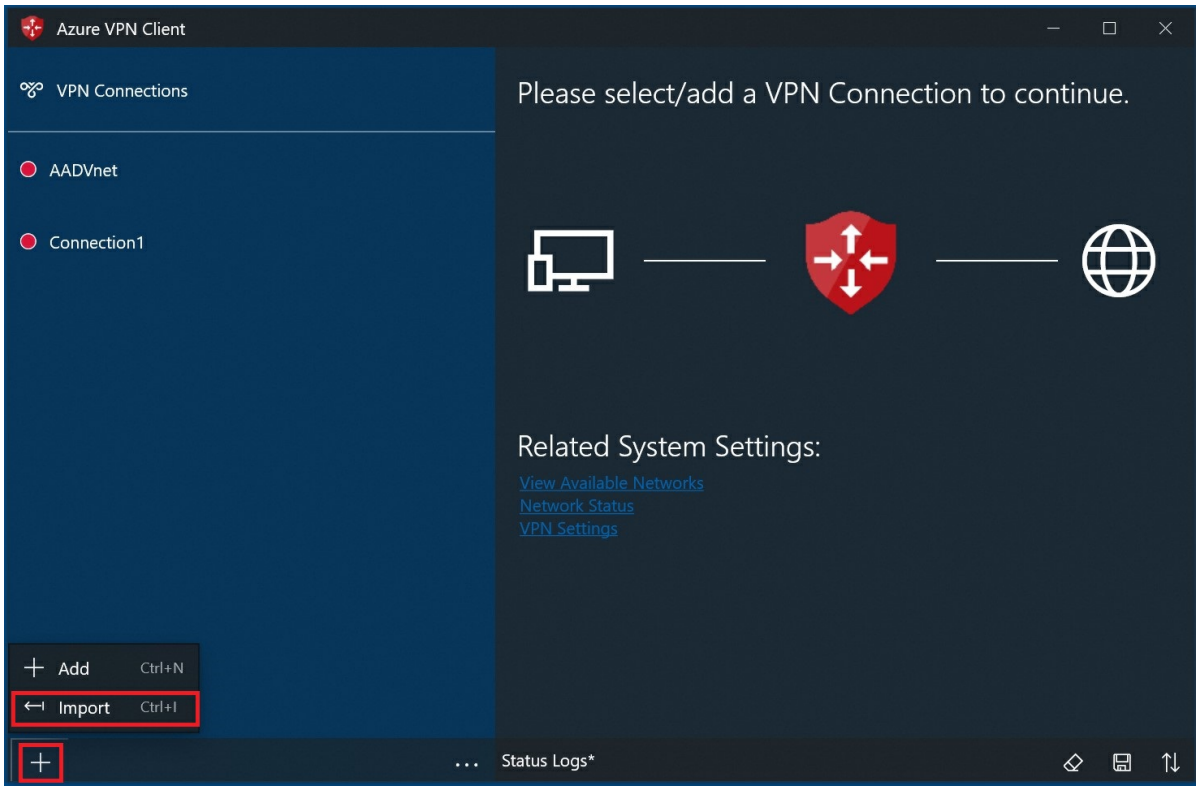
> **NOTE**
> Azure AD authentication is supported only for OpenVPN® protocol connections.

To download the Azure VPN client

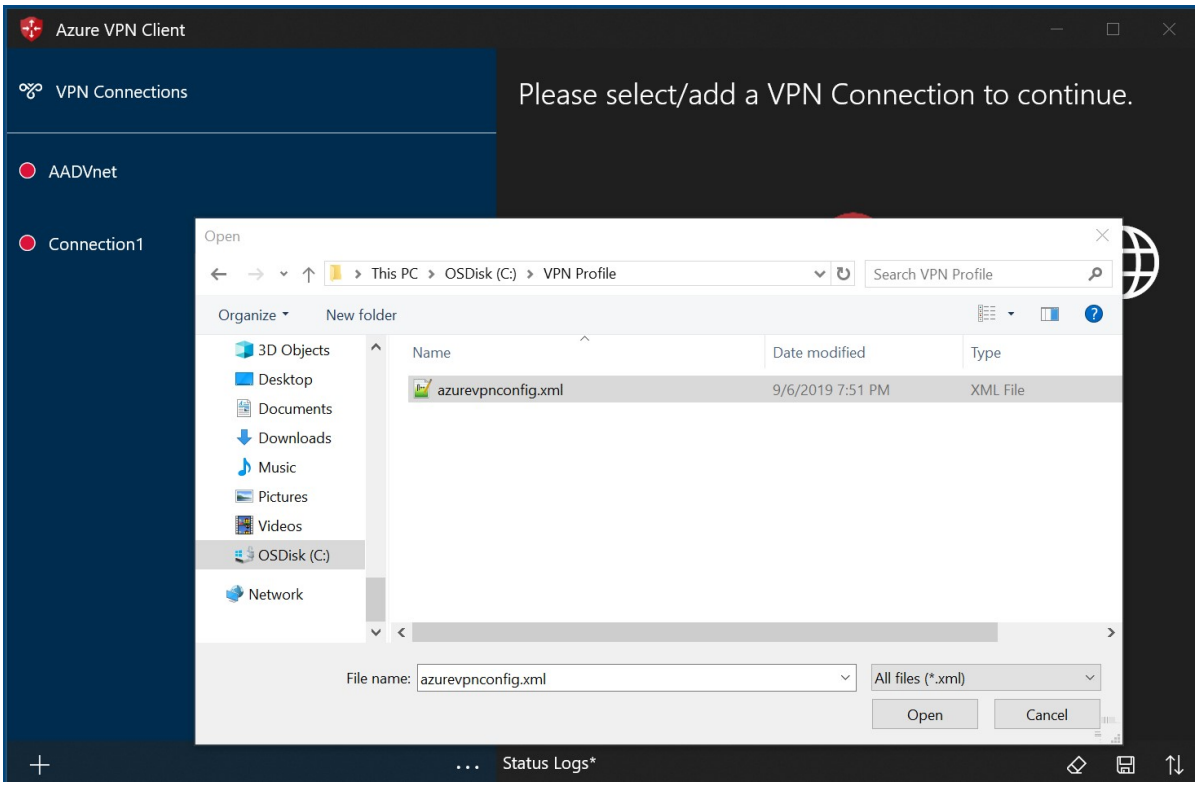
Use this link to download the Azure VPN Client.

To import a client profile

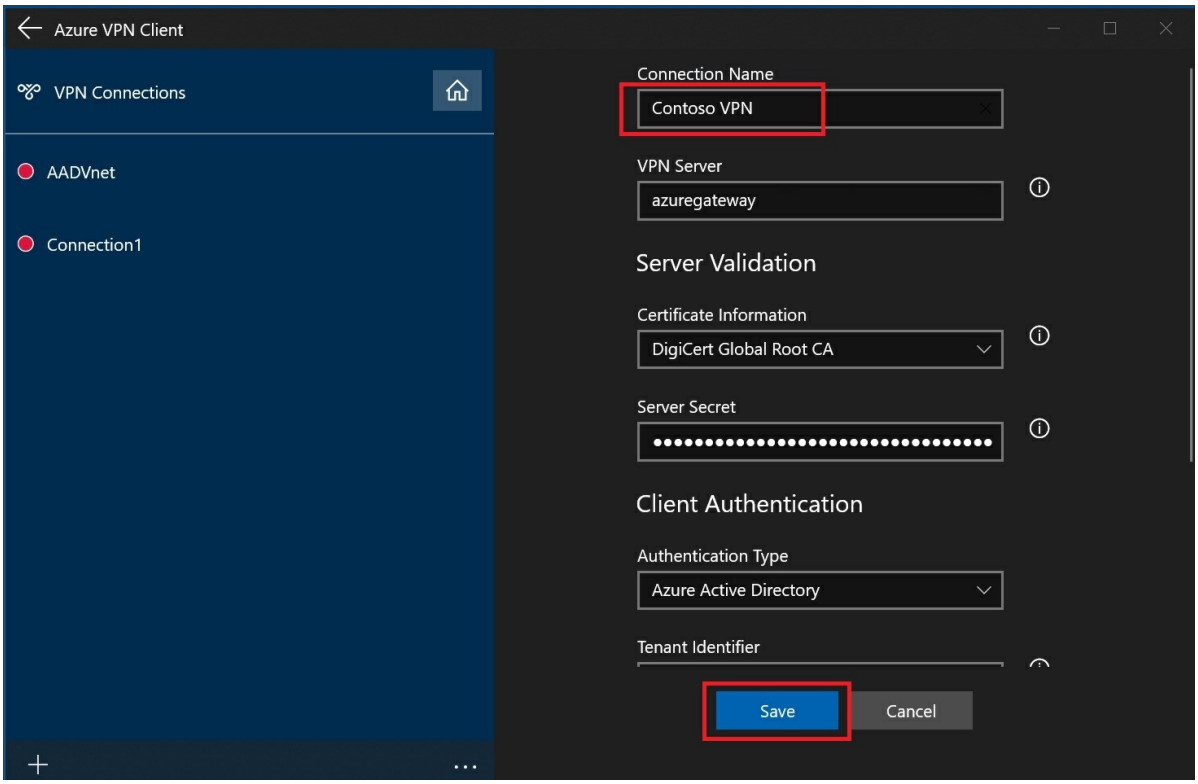
1. On the page, select **Import**.



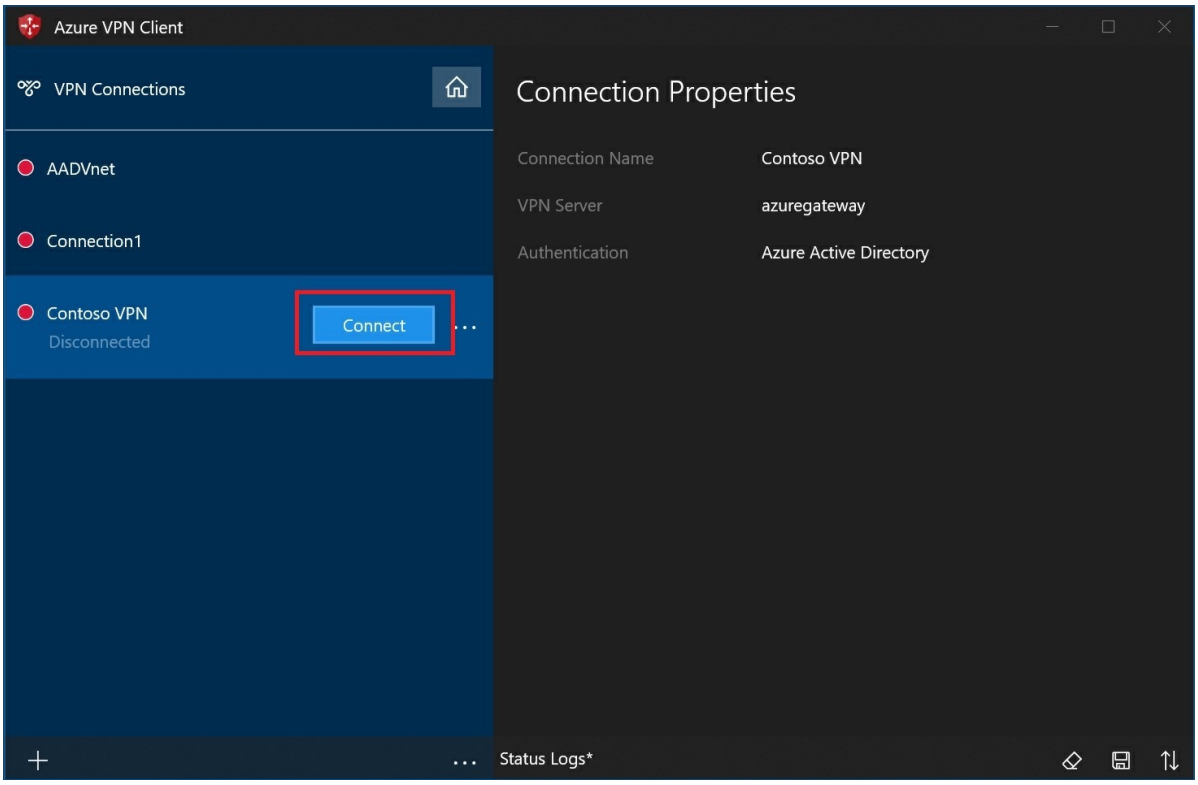
2. Browse to the profile xml file and select it. With the file selected, select **Open**.



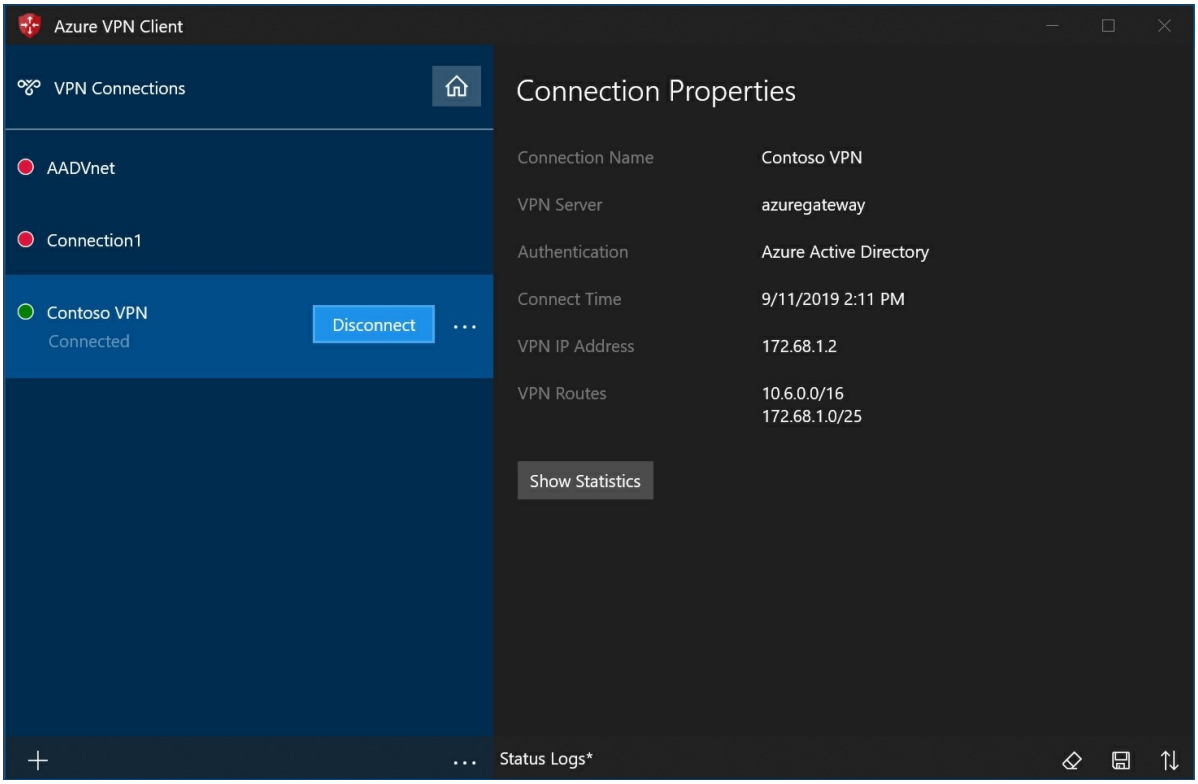
3. Specify the name of the profile and select **Save**.



4. Select **Connect** to connect to the VPN.

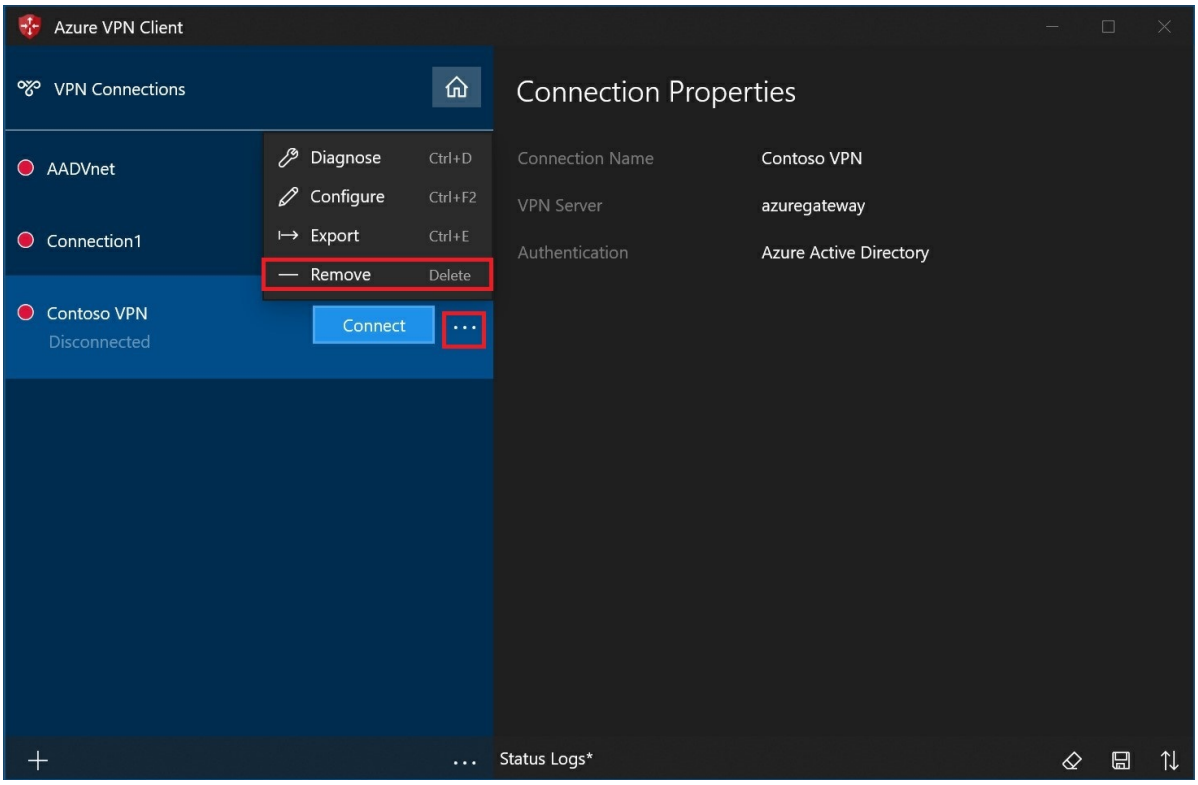


5. Once connected, the icon will turn green and say **Connected**.

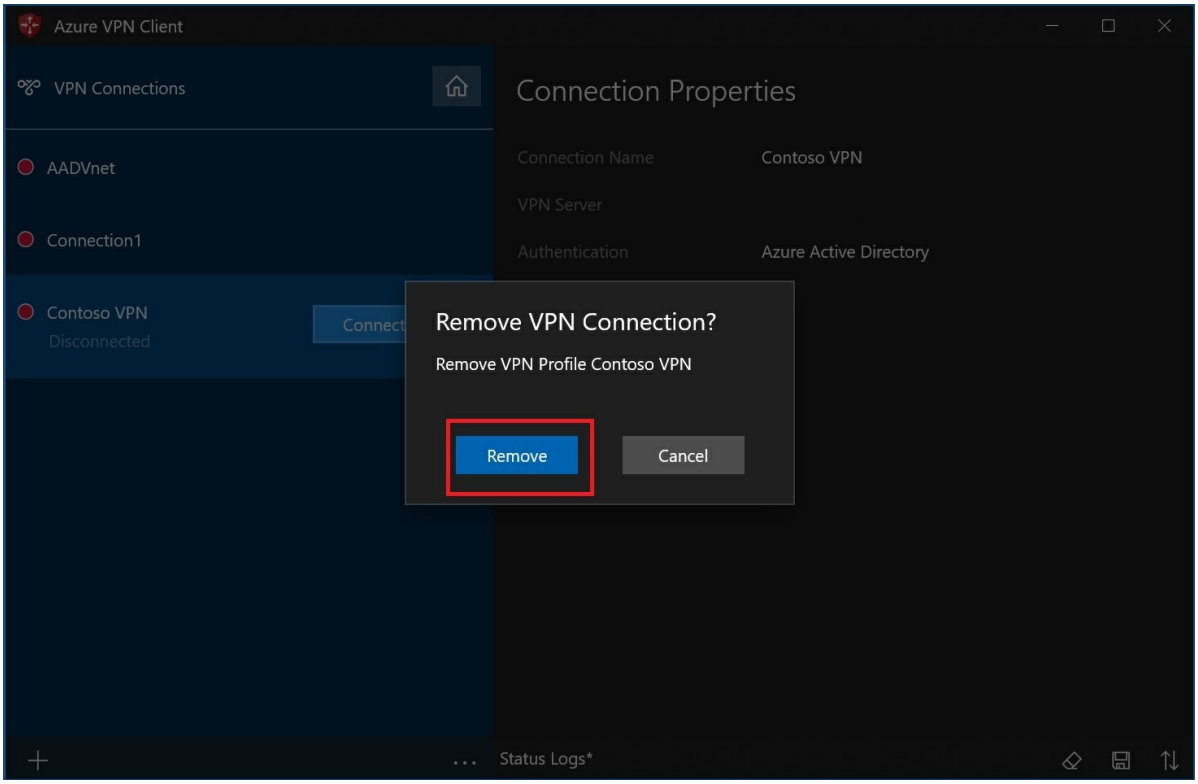


To delete a client profile

1. Select the ellipsis (...) next to the client profile that you want to delete. Then, select **Remove**.

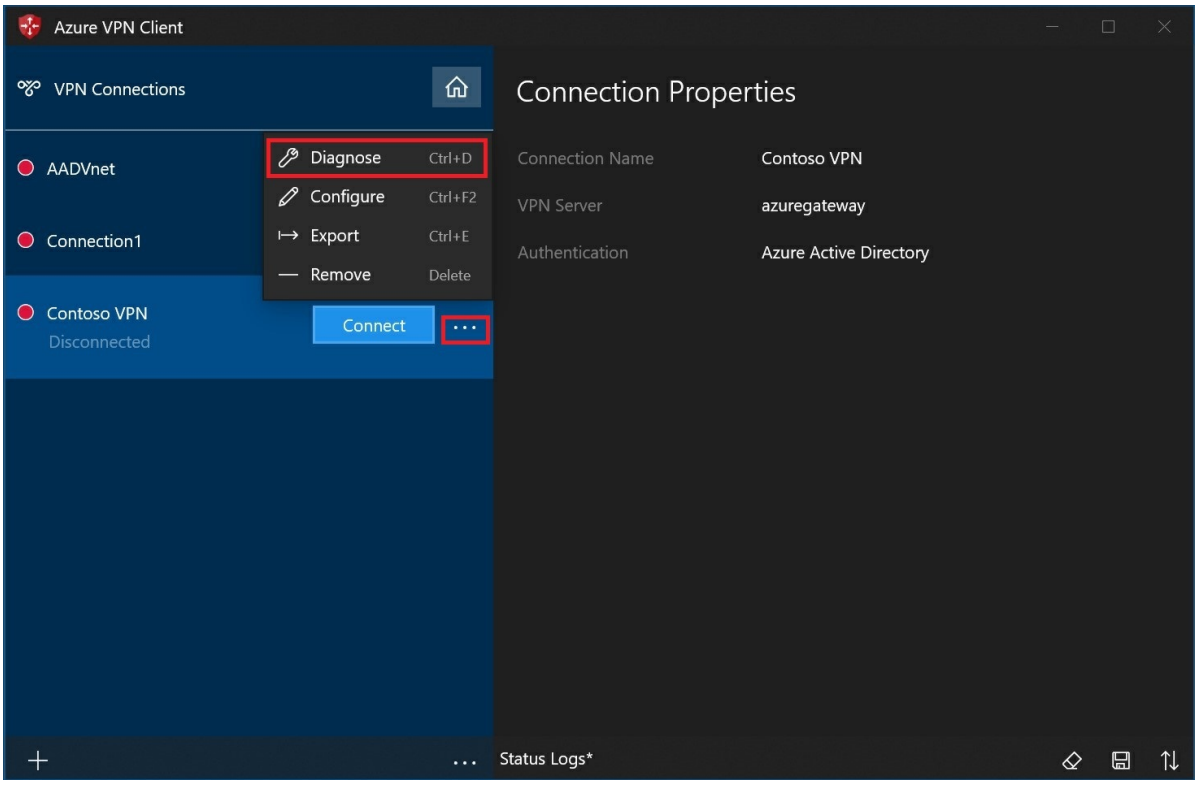


2. Select **Remove** to delete.

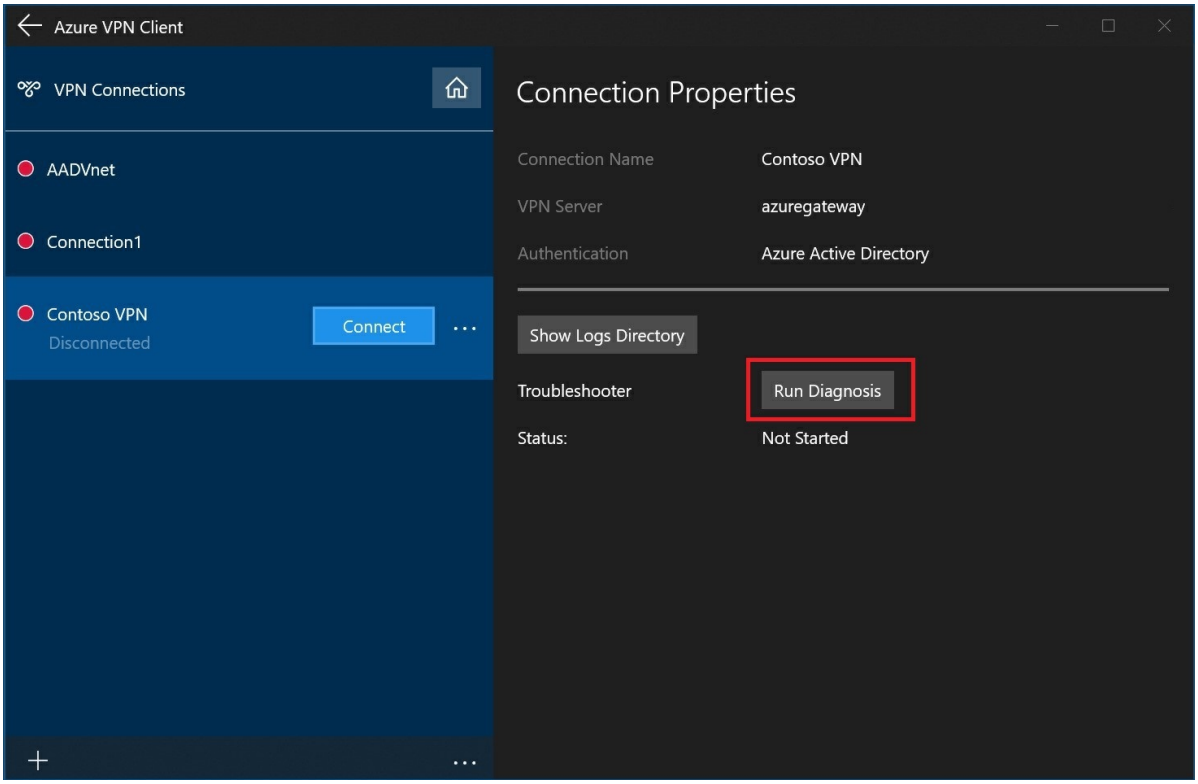


Diagnose connection issues

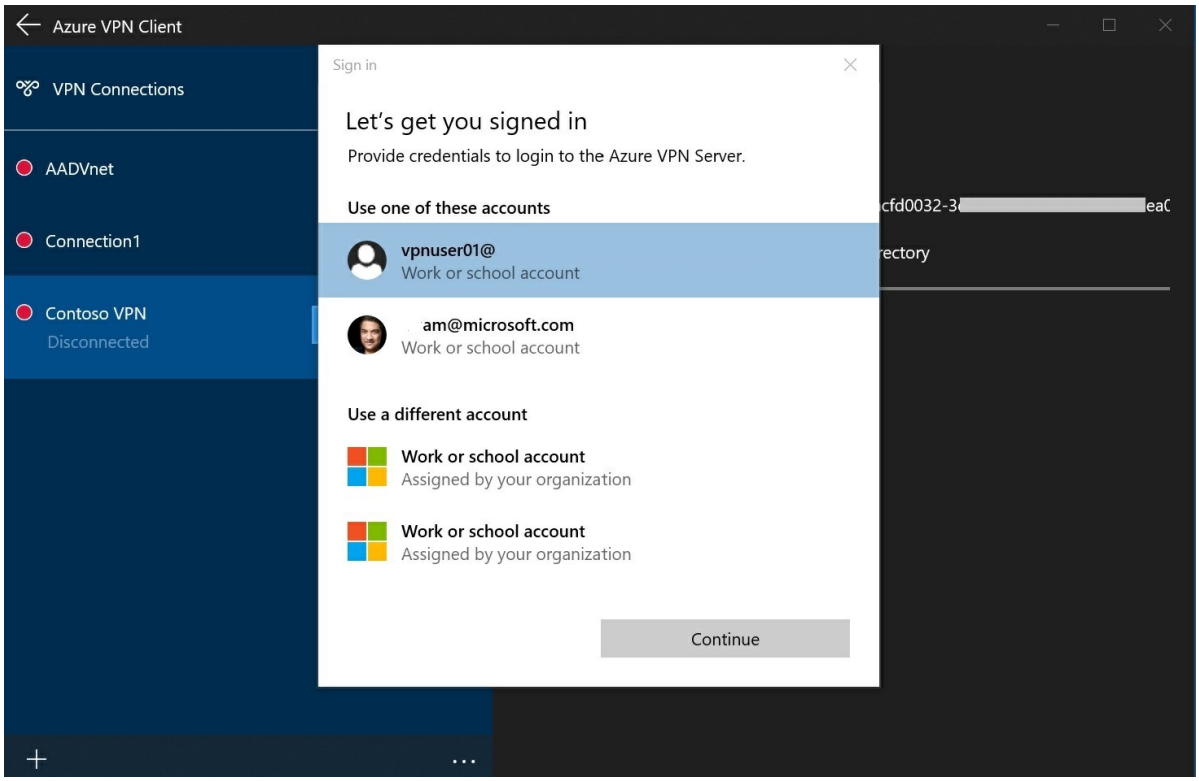
1. To diagnose connection issues, you can use the **Diagnose** tool. Select the ellipsis (...) next to the VPN connection that you want to diagnose to reveal the menu. Then select **Diagnose**.



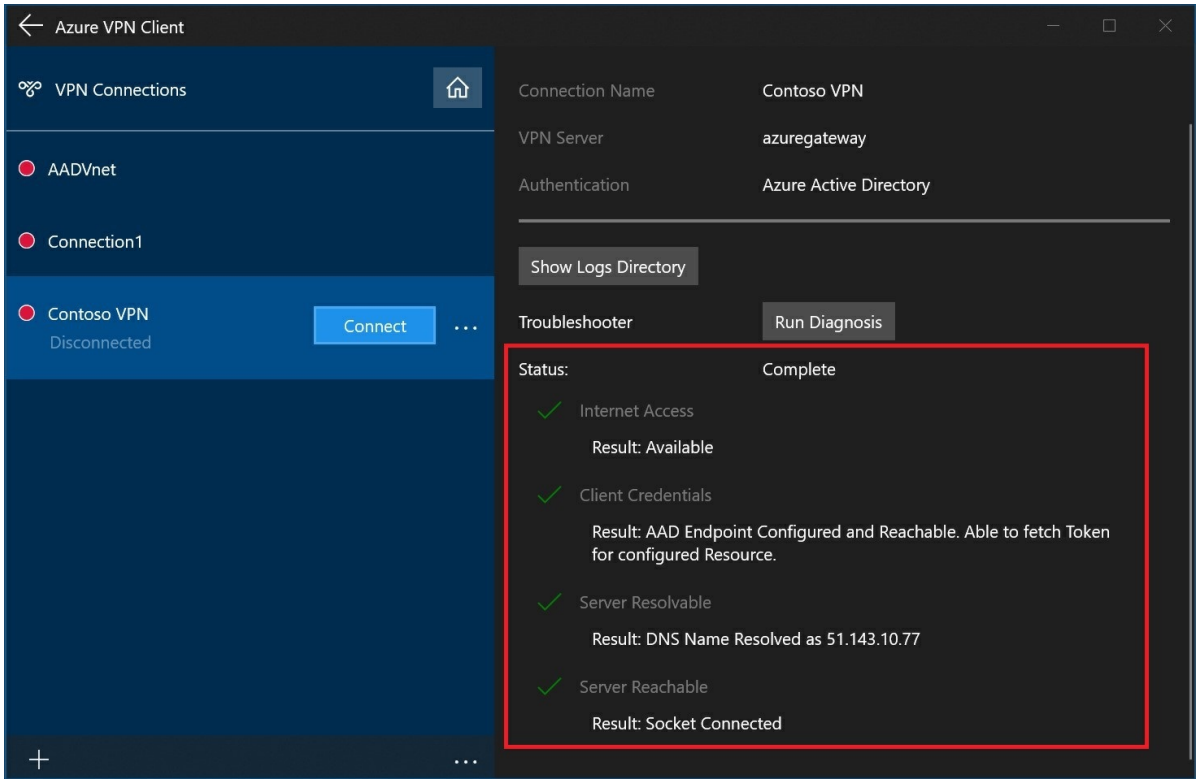
2. On the **Connection Properties** page, select **Run Diagnosis**.



3. Sign in with your credentials.



4. View the diagnosis results.



View your virtual WAN

1. Navigate to the virtual WAN.
2. On the Overview page, each point on the map represents a hub. Hover over any point to view the hub health summary.
3. In the Hubs and connections section, you can view hub status, site, region, VPN connection status, and bytes in and out.

View your resource health

1. Navigate to your WAN.
2. On your WAN page, in the **SUPPORT + Troubleshooting** section, click **Health** and view your resource.

Clean up resources

When you no longer need these resources, you can use Remove-AzureRmResourceGroup to remove the resource group and all of the resources it contains. Replace "myResourceGroup" with the name of your resource group and run the following PowerShell command:

```
Remove-AzureRmResourceGroup -Name myResourceGroup -Force
```

Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Create an Azure Active Directory tenant for P2S OpenVPN protocol connections

2/20/2020 • 6 minutes to read • Edit Online

When connecting to your VNet, you can use certificate-based authentication or RADIUS authentication. However, when you use the Open VPN protocol, you can also use Azure Active Directory authentication. If you want different set of users to be able to connect to different VPN gateways, you can register multiple apps in AD and link them to different VPN gateways.

This article helps you set up an Azure AD tenant for P2S OpenVPN authentication, and create and register multiple apps in Azure AD to allow different access for different users and groups.

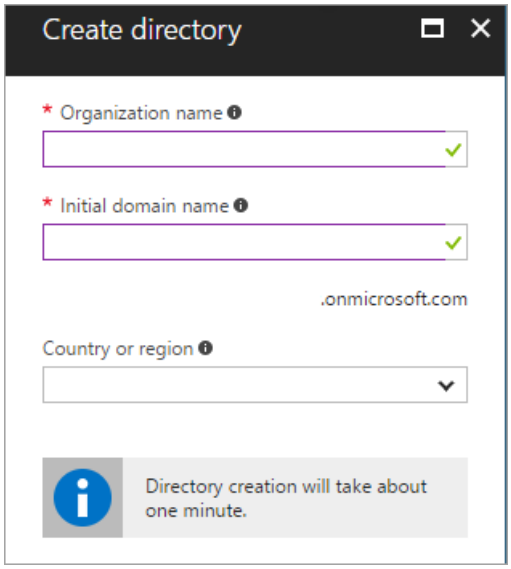
> **NOTE**
> Azure AD authentication is supported only for OpenVPN® protocol connections.

1. Create the Azure AD tenant

Create an Azure AD tenant using the steps in the Create a new tenant article:

- Organizational name
- Initial domain name

  Example:



2. Create tenant users

In this step, you create two Azure AD tenant users: One Global Admin account and one master user account. The master user account is used as your master embedding account (service account). When you create an Azure AD tenant user account, you adjust the Directory role for the type of user that you want to create. Use the steps in this article to create at least two users for your Azure AD tenant. Be sure to change the **Directory Role** to create the account types:

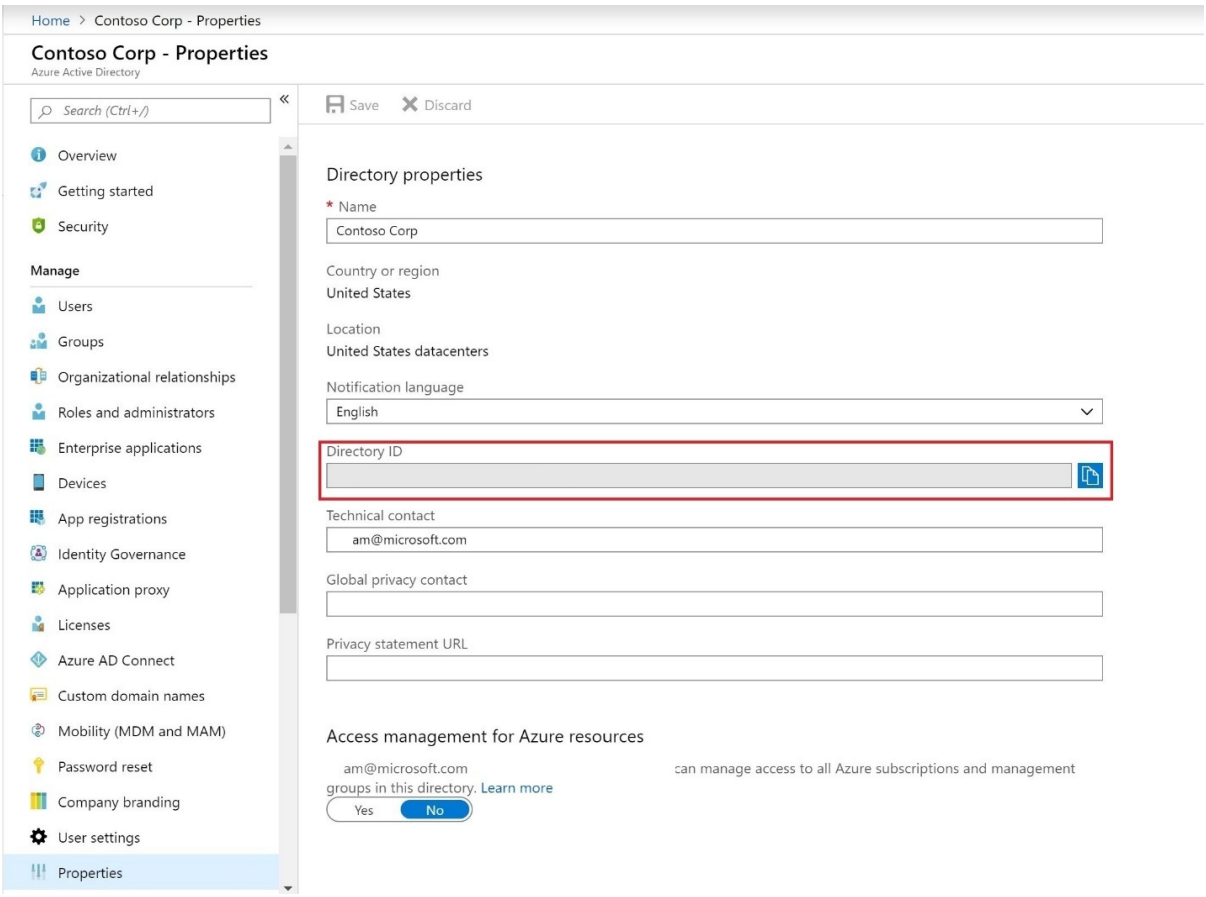
- Global Admin

- User

3. Register the VPN Client

Register the VPN client in the Azure AD tenant.

1. Locate the Directory ID of the directory that you want to use for authentication. It is listed in the properties section of the Active Directory page.



2. Copy the Directory ID.
3. Sign in to the Azure portal as a user that is assigned the **Global administrator** role.
4. Next, give admin consent. Copy and paste the URL that pertains to your deployment location in the address bar of your browser:

   Public

   ```
   https://login.microsoftonline.com/common/oauth2/authorize?client_id=41b23e61-6c1e-4545-b367-cd054e0ed4b4&response_type=code&redirect_uri=https://portal.azure.com&nonce=1234&prompt=admin_consent
   ```

   Azure Government

   ```
   https://login-us.microsoftonline.com/common/oauth2/authorize?client_id=51bb15d4-3a4f-4ebf-9dca-40096fe32426&response_type=code&redirect_uri=https://portal.azure.us&nonce=1234&prompt=admin_consent
   ```

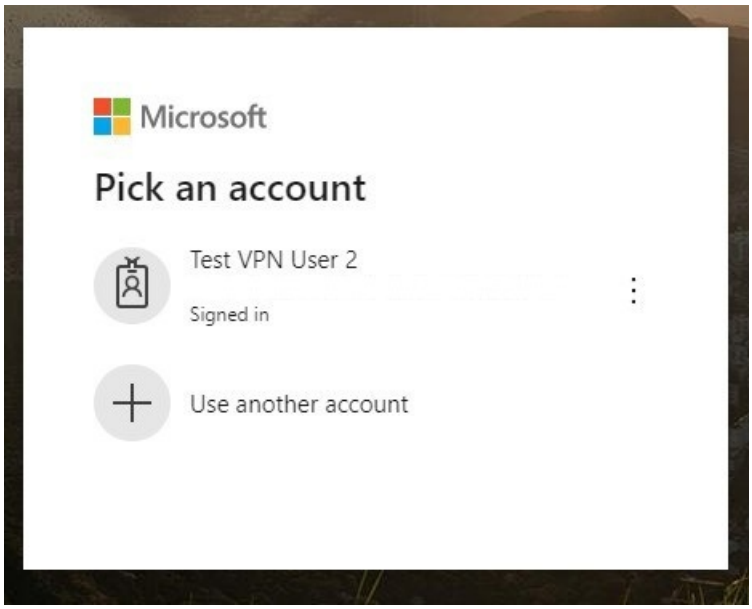
   Microsoft Cloud Germany

```
https://login-us.microsoftonline.de/common/oauth2/authorize?client_id=538ee9e6-310a-468d-afef-ea97365856a9&response_type=code&redirect_uri=https://portal.microsoftazure.de&nonce=1234&prompt=admin_consent
```

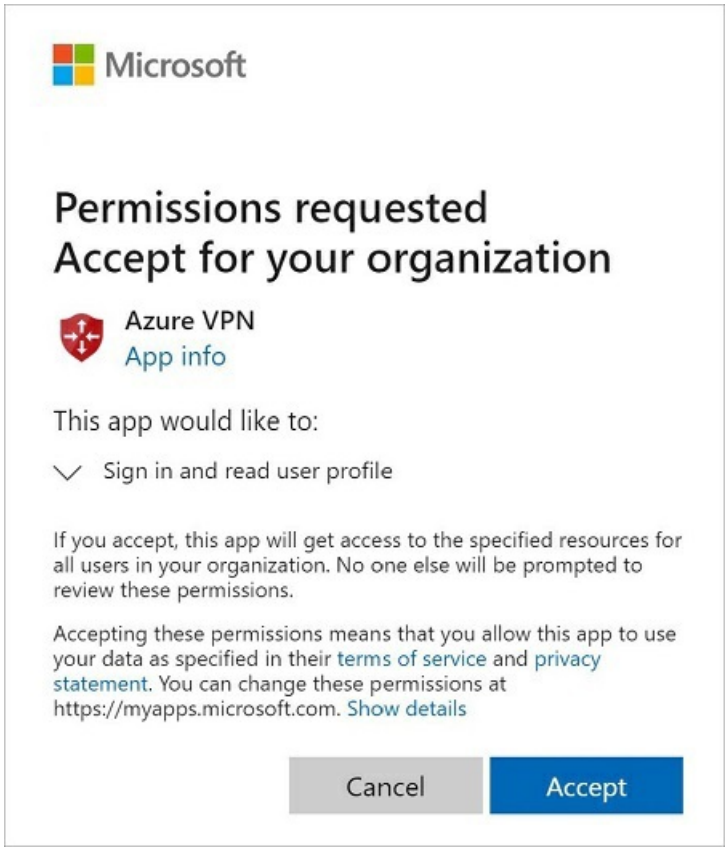
Azure China 21Vianet

```
https://https://login.chinacloudapi.cn/common/oauth2/authorize?client_id=49f817b6-84ae-4cc0-928c-73f27289b3aa&response_type=code&redirect_uri=https://portal.azure.cn&nonce=1234&prompt=admin_consent
```

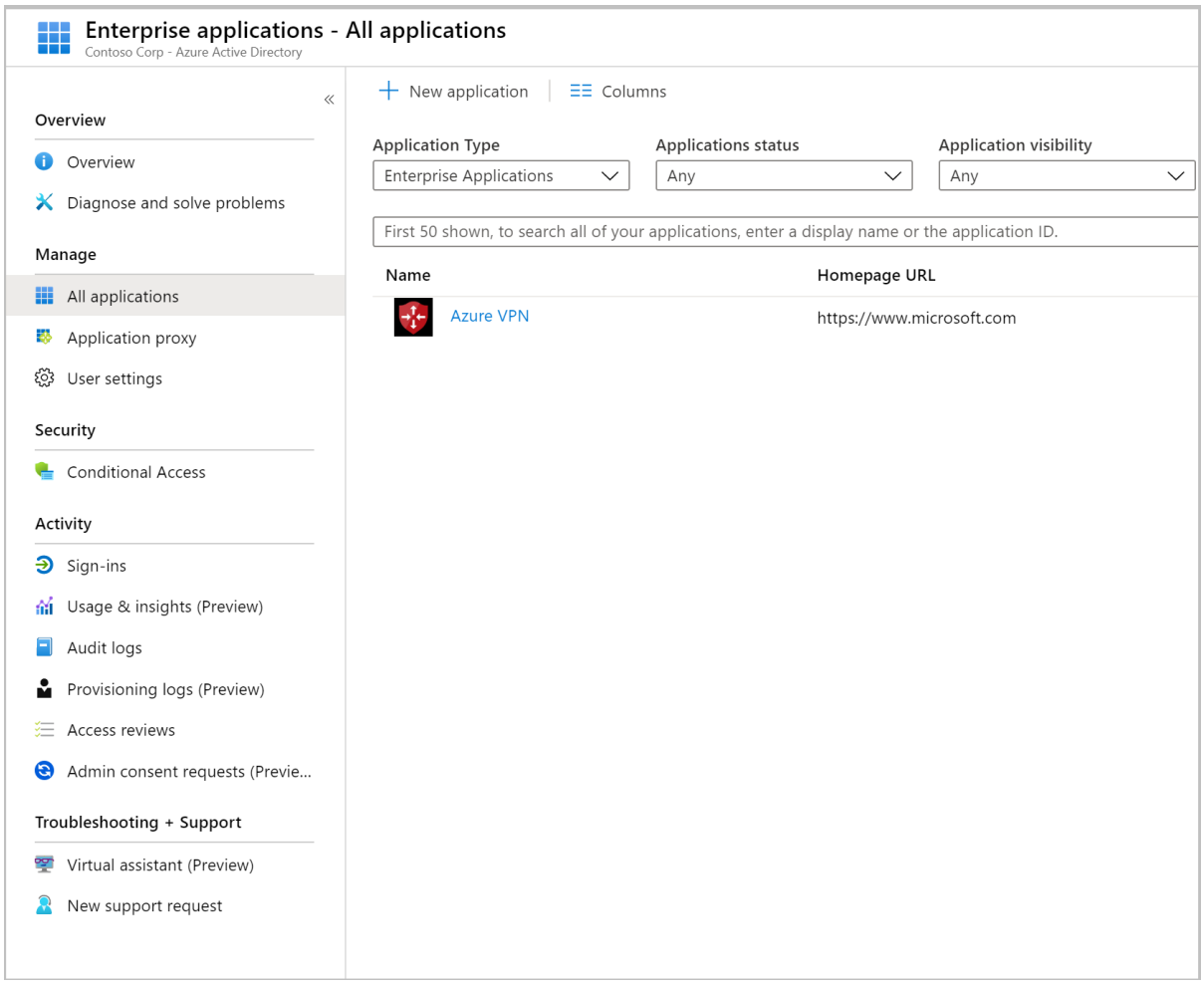
5. Select the **Global Admin** account if prompted.



6. Select **Accept** when prompted.



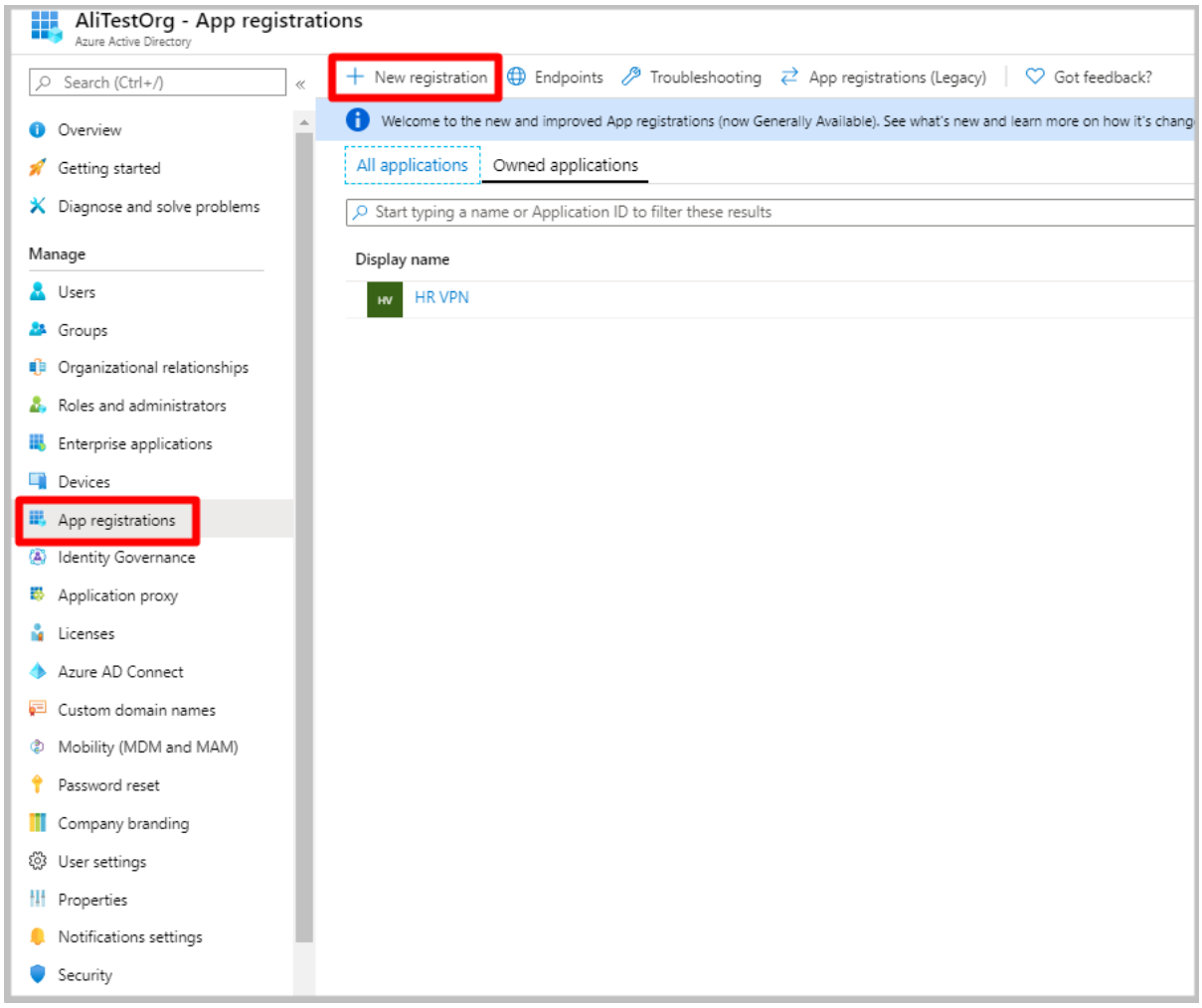
7. Under your Azure AD, in **Enterprise applications**, you will see **Azure VPN** listed.



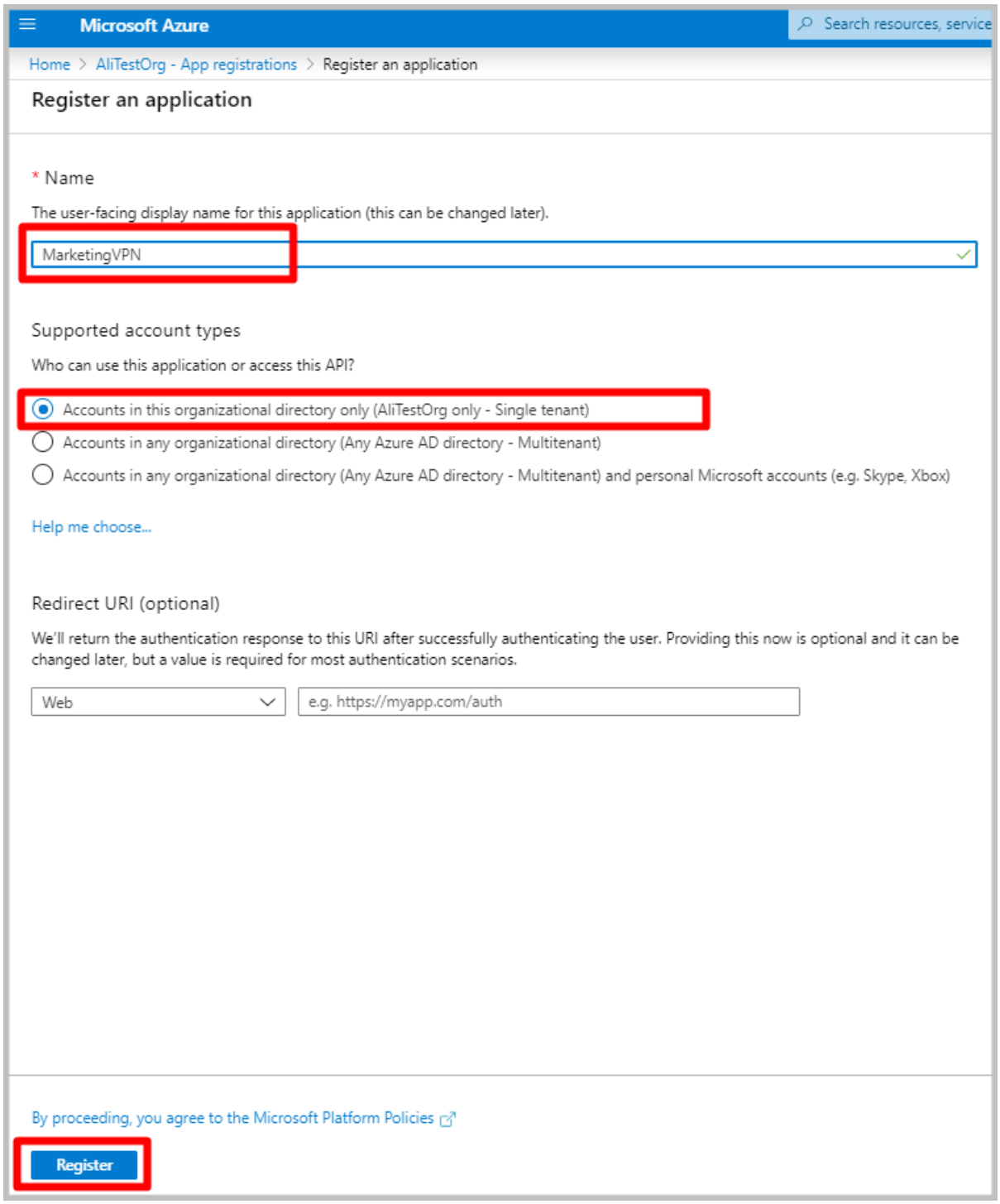
4. Register additional applications

In this step, you register additional applications for various users and groups.

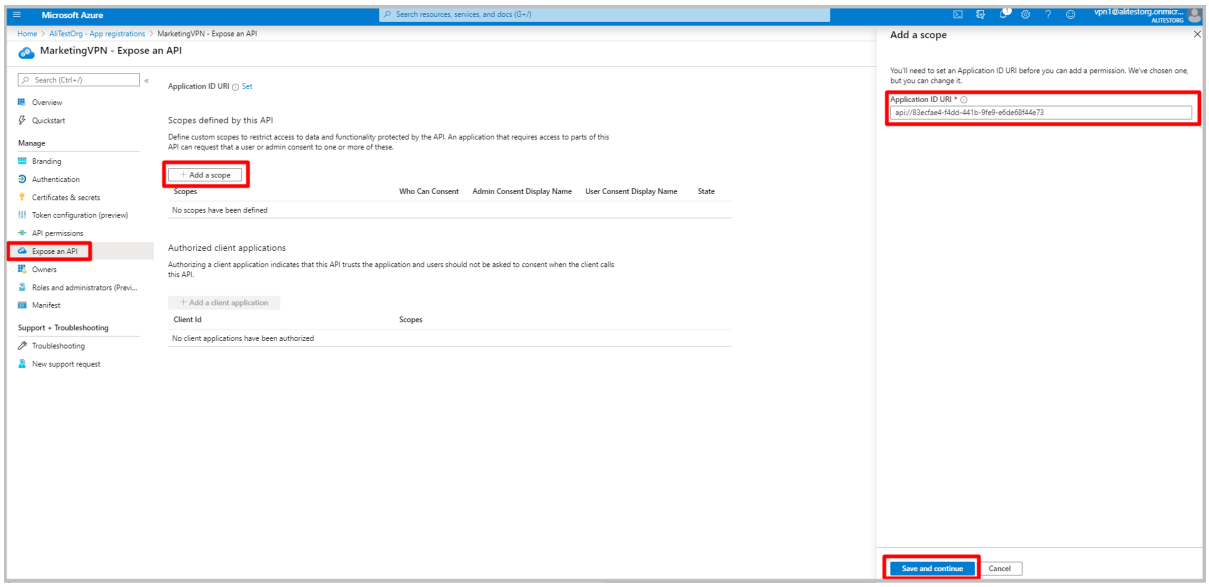
1. Under your Azure Active Directory, click **App registrations** and then **+ New registration**.



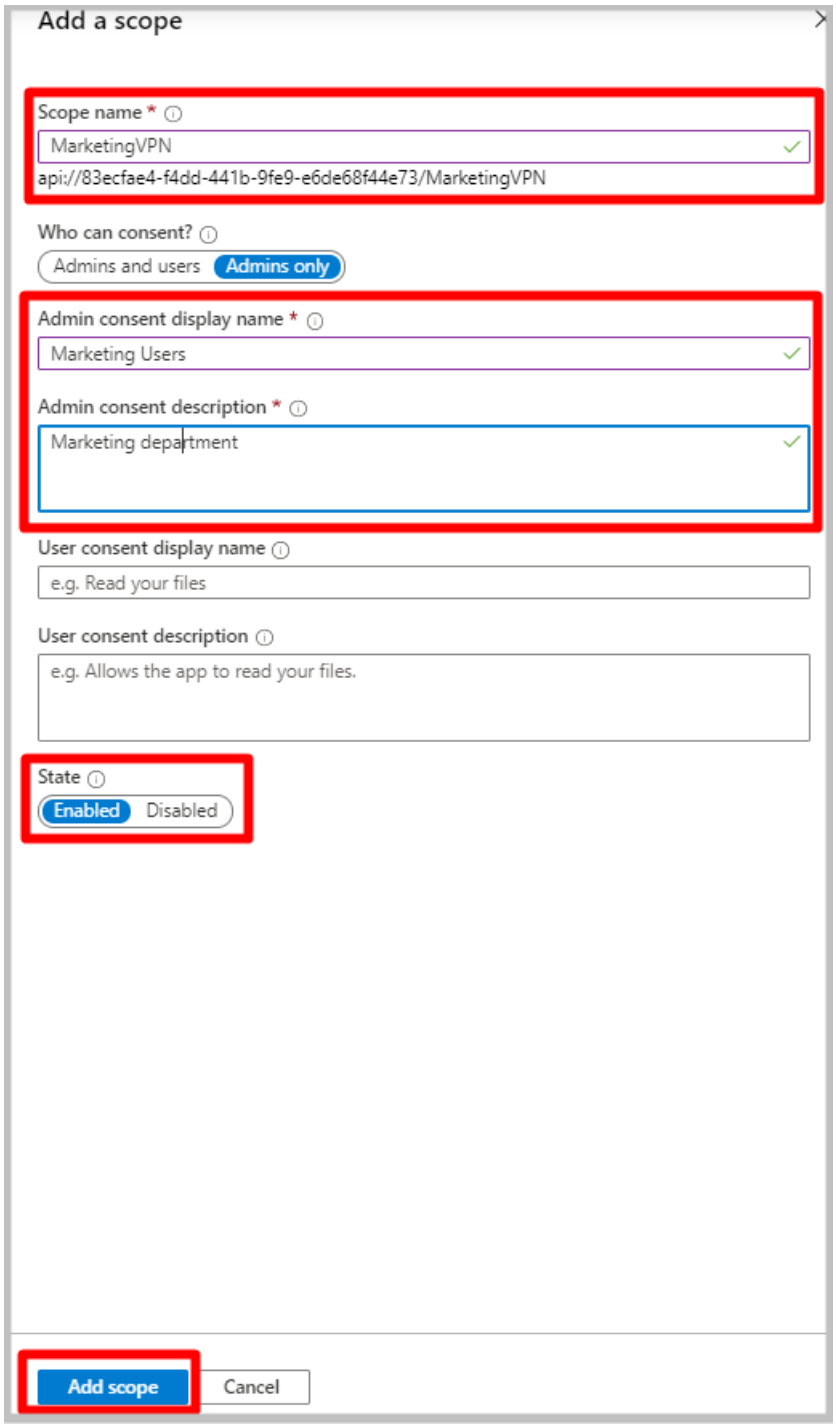
2. On the **Register an application** page, enter the **Name**. Select the desired **Supported account types**, then click **Register**.



3. Once the new app has been registered, click **Expose an API** under the app blade.
4. Click **+ Add a scope**.
5. Leave the default **Application ID URI**. Click **Save and continue**.



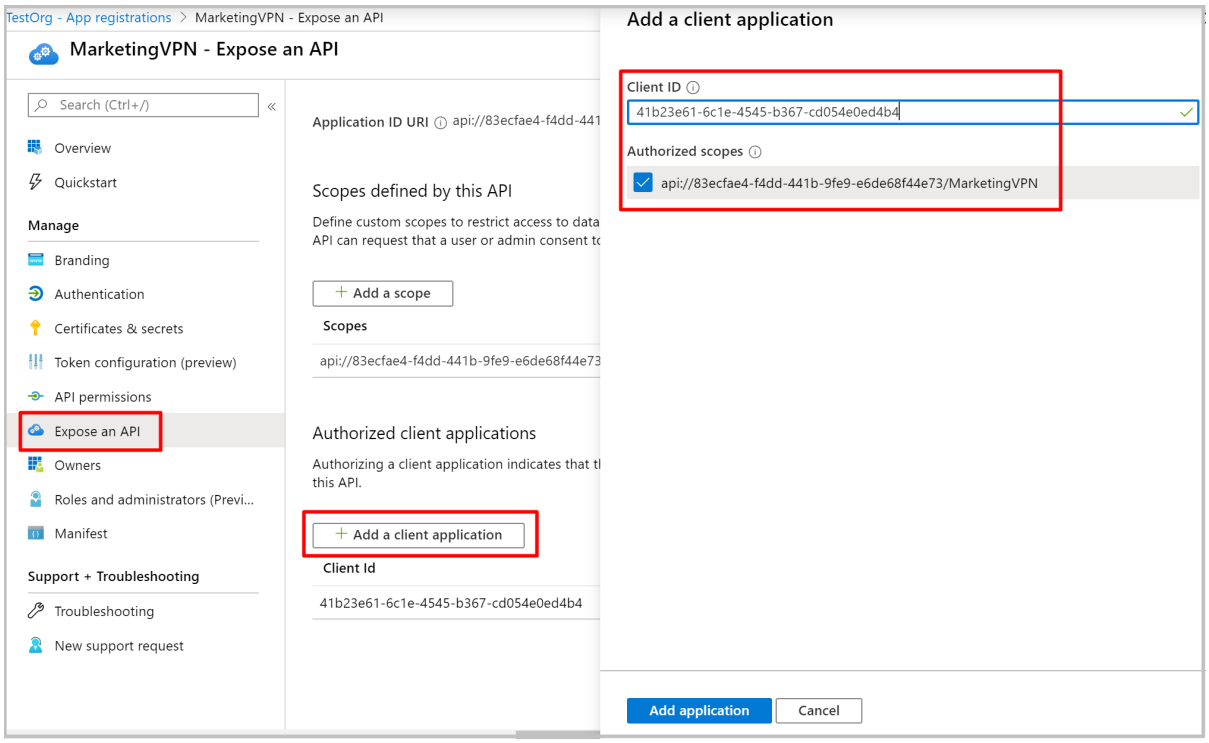
6. Fill in the required fields and ensure that **State** is **Enabled**. Click **Add scope**.



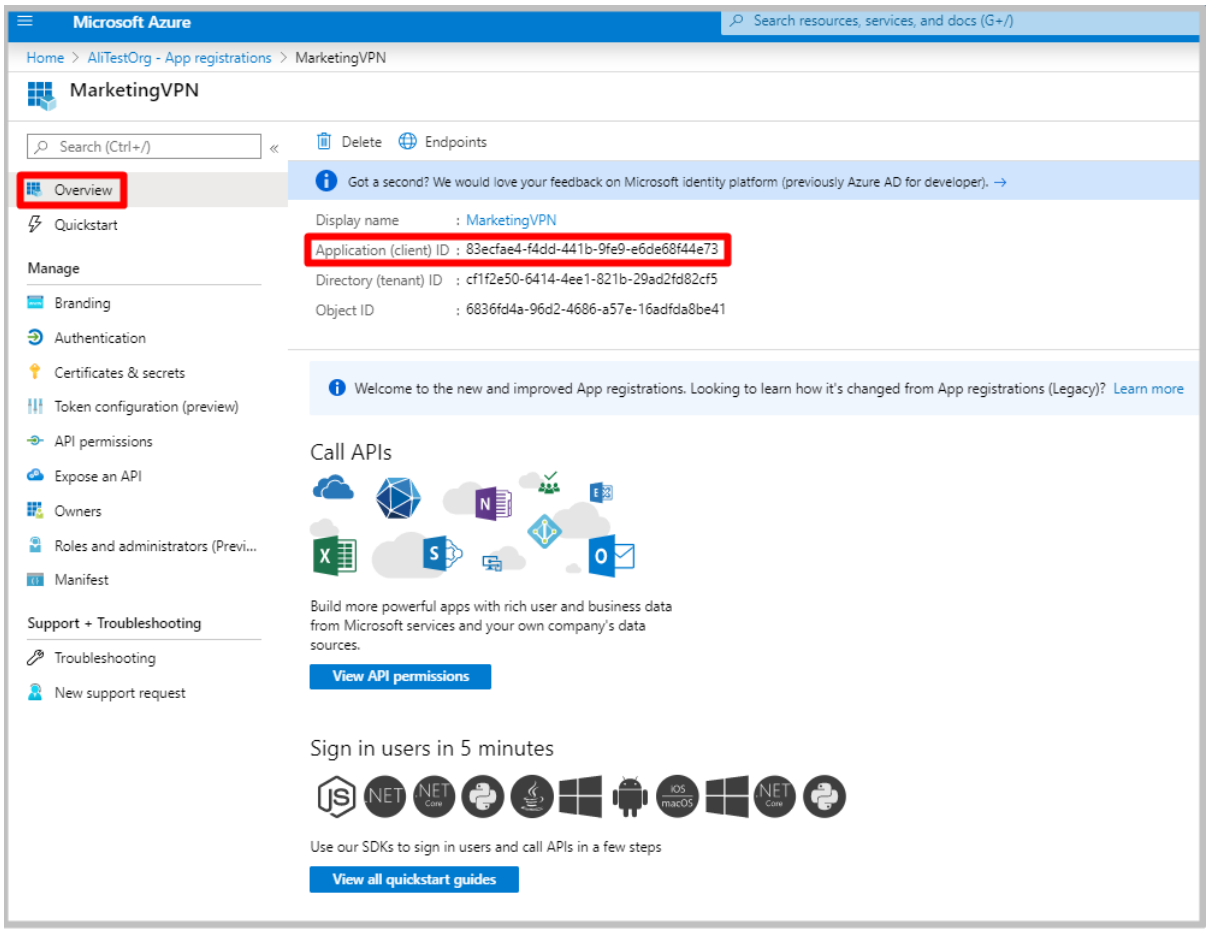
7. Click **Expose an API** then **+ Add a client application**. For **Client ID**, enter the following values depending on the cloud:

   - Enter **41b23e61-6c1e-4545-b367-cd054e0ed4b4** for Azure **Public**
   - Enter **51bb15d4-3a4f-4ebf-9dca-40096fe32426** for Azure **Government**
   - Enter **538ee9e6-310a-468d-afef-ea97365856a9** for Azure **Germany**
   - Enter **49f817b6-84ae-4cc0-928c-73f27289b3aa** for Azure **China 21Vianet**

8. Click **Add application**.



9. Copy the **Application (client) ID** from the **Overview** page. You will need this information to configure your VPN gateway(s).

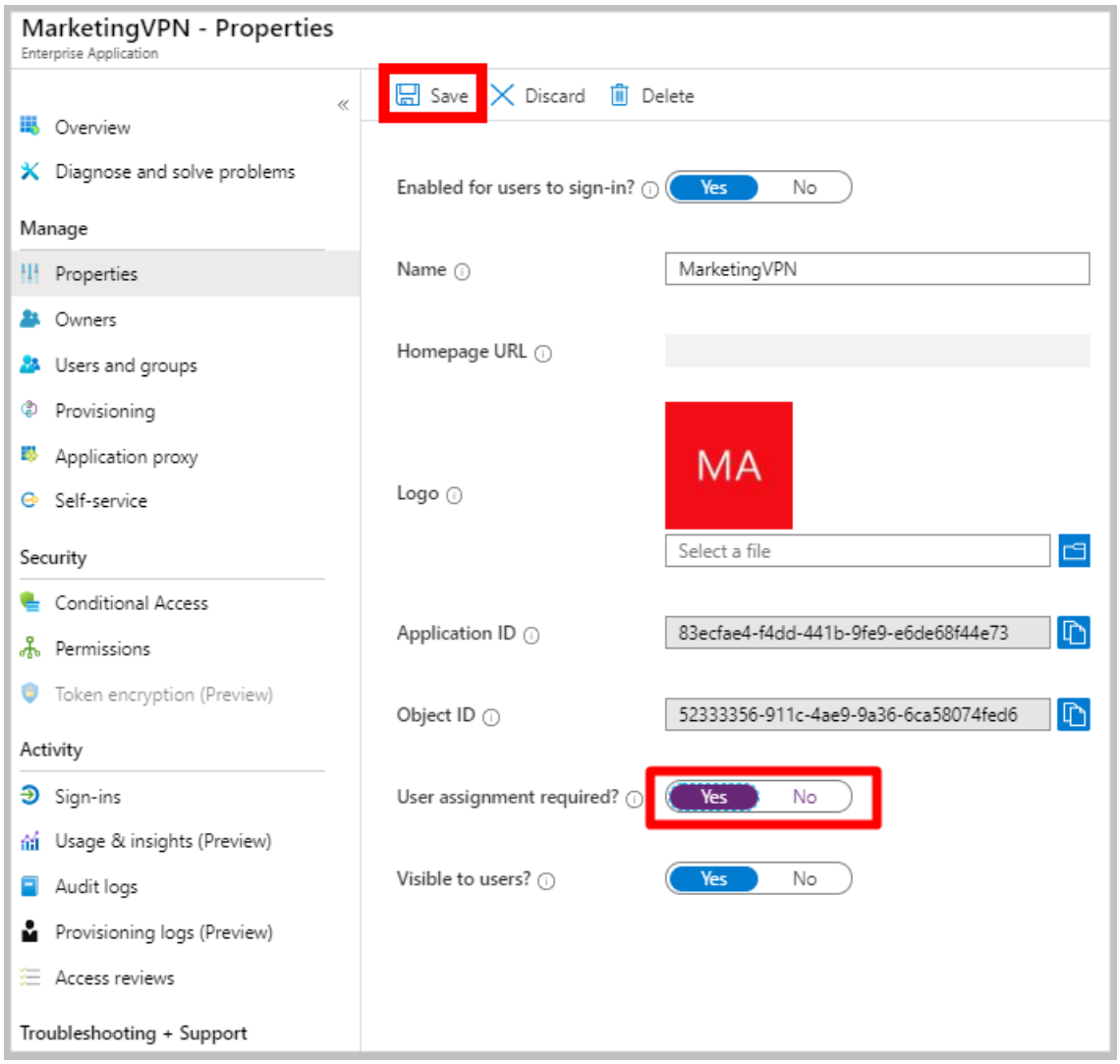


10. Repeat the steps in this register additional applications section to create as many applications that are needed for your security requirement. Each application will be associated to a VPN gateway and can have a different set of users. Only one application can be associated to a gateway.

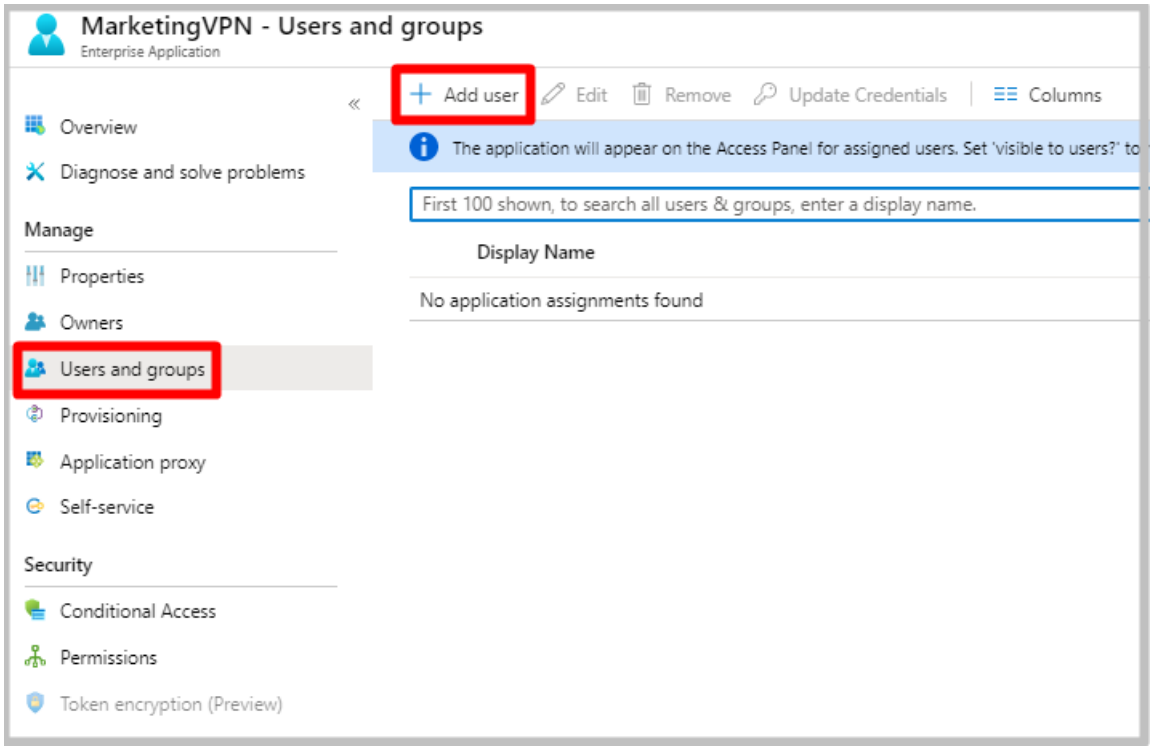
5. Assign users to applications

Assign the users to your applications.

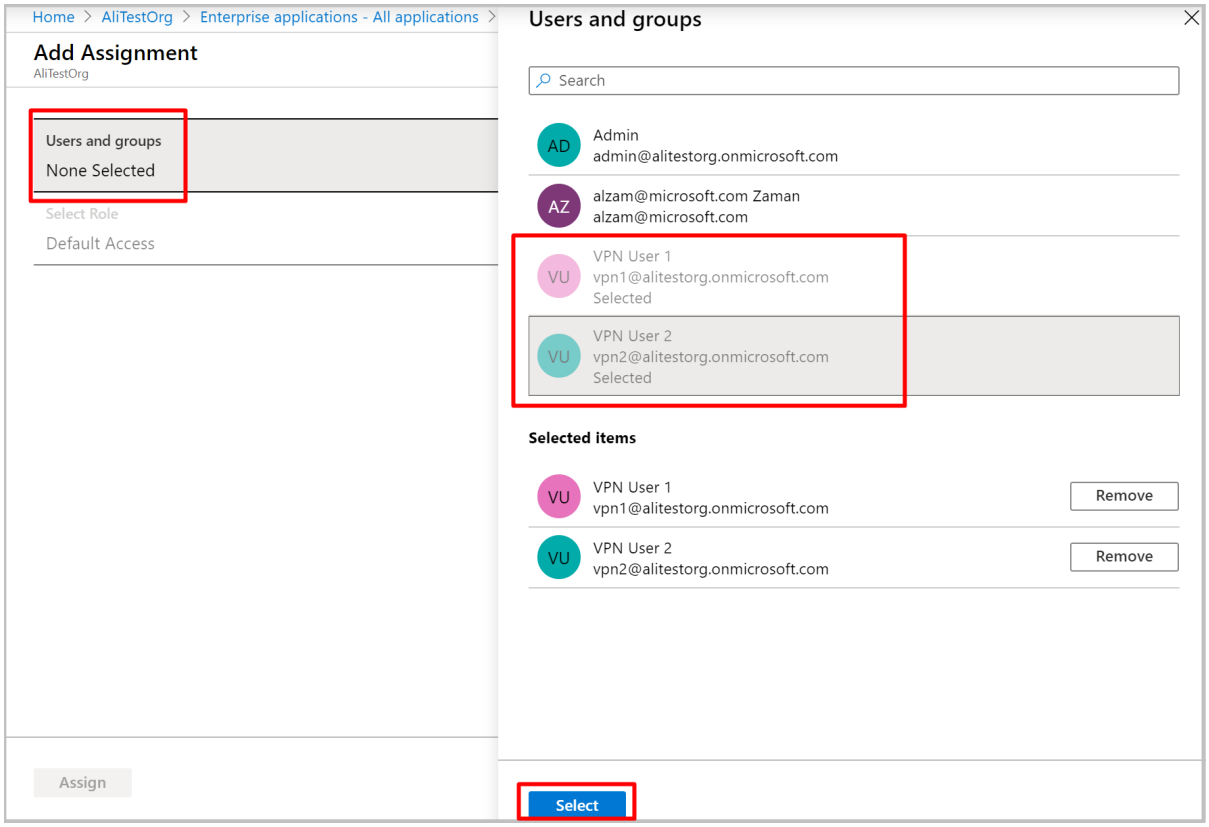
1. Under **Azure AD -> Enterprise applications**, select the newly registered application and click **Properties**. Ensure that **User assignment required?** is set to **yes**. Click **Save**.



2. On the app page, click **Users and groups**, and then click **+Add user**.



3. Under **Add Assignment**, click **Users and groups**. Select the users that you want to be able to access this VPN application. Click **Select**.



6. Create a new P2S configuration

A P2S configuration defines the parameters for connecting remote clients.

1. Set the following variables, replacing values as needed for your environment.

```
$aadAudience = "00000000-abcd-abcd-abcd-999999999999"
$aadIssuer = "https://sts.windows.net/00000000-abcd-abcd-abcd-999999999999/"
$aadTenant = "https://login.microsoftonline.com/00000000-abcd-abcd-abcd-999999999999"
```

2. Run the following commands to create the configuration:

```
$aadConfig = New-AzVpnServerConfiguration -ResourceGroupName <ResourceGroup> -Name newAADConfig -
VpnProtocol OpenVPN -VpnAuthenticationType AAD -AadTenant $aadTenant -AadIssuer $aadIssuer -AadAudience
$aadAudience -Location westcentralus
```

> **NOTE**
>
> Do not use the Azure VPN client's application ID in the commands above: It will grant all users access to the VPN gateway. Use the ID of the application(s) you registered.

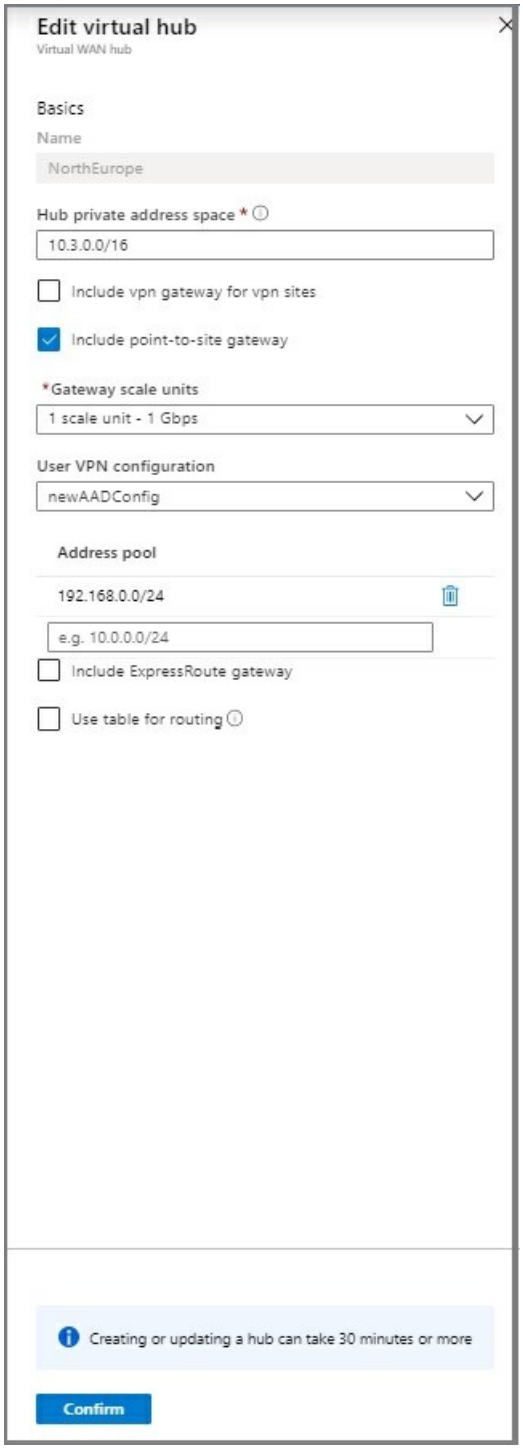
7. Edit hub assignment

1. Navigate to the **Hubs** blade under the virtual WAN.

2. Select the hub that you want to associate the vpn server configuration to and click the ellipsis (...).

3. Click **Edit virtual hub**.

4. Check the **Include point-to-site gateway** check box and pick the **Gateway scale unit** that you want.



5. Enter the **Address pool** from which the VPN clients will be assigned IP addresses.

6. Click **Confirm**.

7. The operation can take up to 30 minutes to complete.

8. Download VPN profile

Use the VPN profile to configure your clients.

1. On the page for your virtual WAN, click **User VPN configurations**.
2. At the top of the page, click **Download user VPN config**.
3. Once the file has finished creating, you can click the link to download it.
4. Use the profile file to configure the VPN clients.
5. Extract the downloaded zip file.
6. Browse to the unzipped “AzureVPN” folder.
7. Make a note of the location of the "azurevpnconfig.xml" file. The azurevpnconfig.xml contains the setting for the VPN connection and can be imported directly into the Azure VPN Client application. You can also distribute this file to all the users that need to connect via e-mail or other means. The user will need valid Azure AD credentials to connect successfully.

9. Configure User VPN clients

To connect, you need to download the Azure VPN Client and import the VPN client profile that was downloaded in the previous steps on every computer that wants to connect to the VNet.

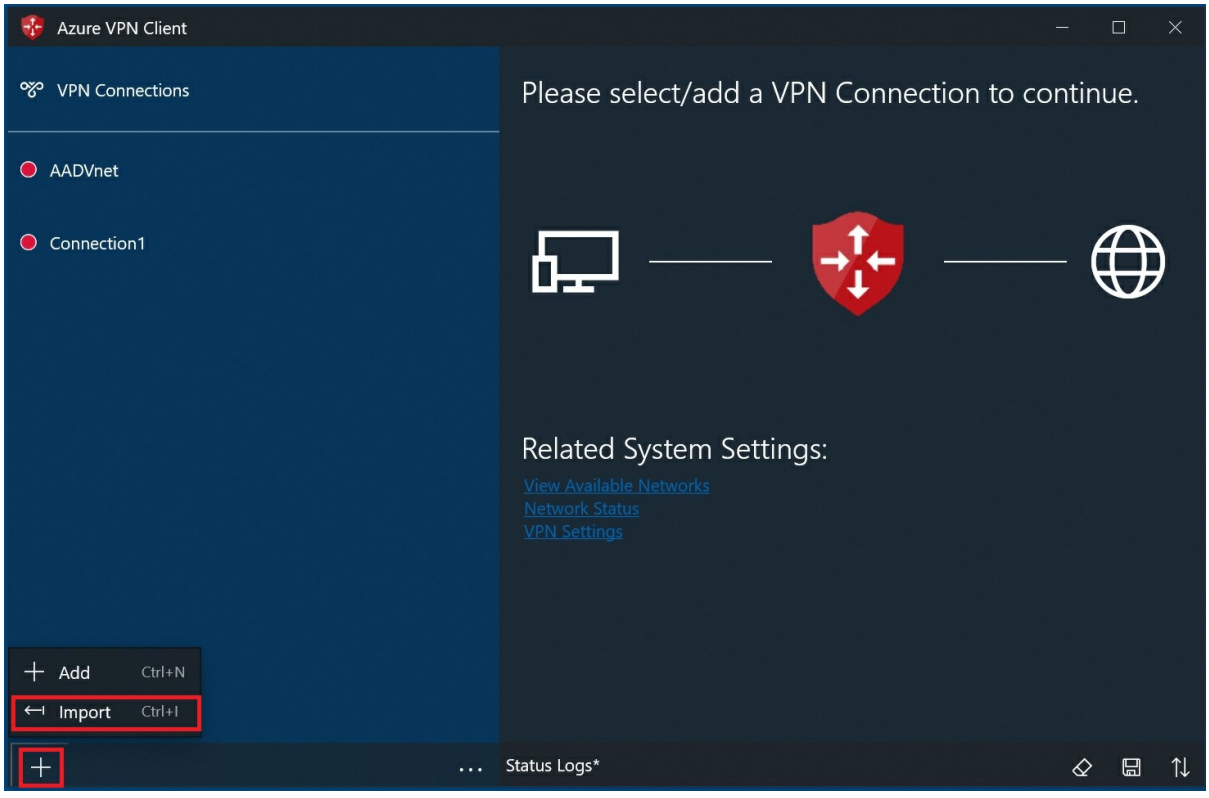
> **NOTE**
> Azure AD authentication is supported only for OpenVPN® protocol connections.

To download the Azure VPN client

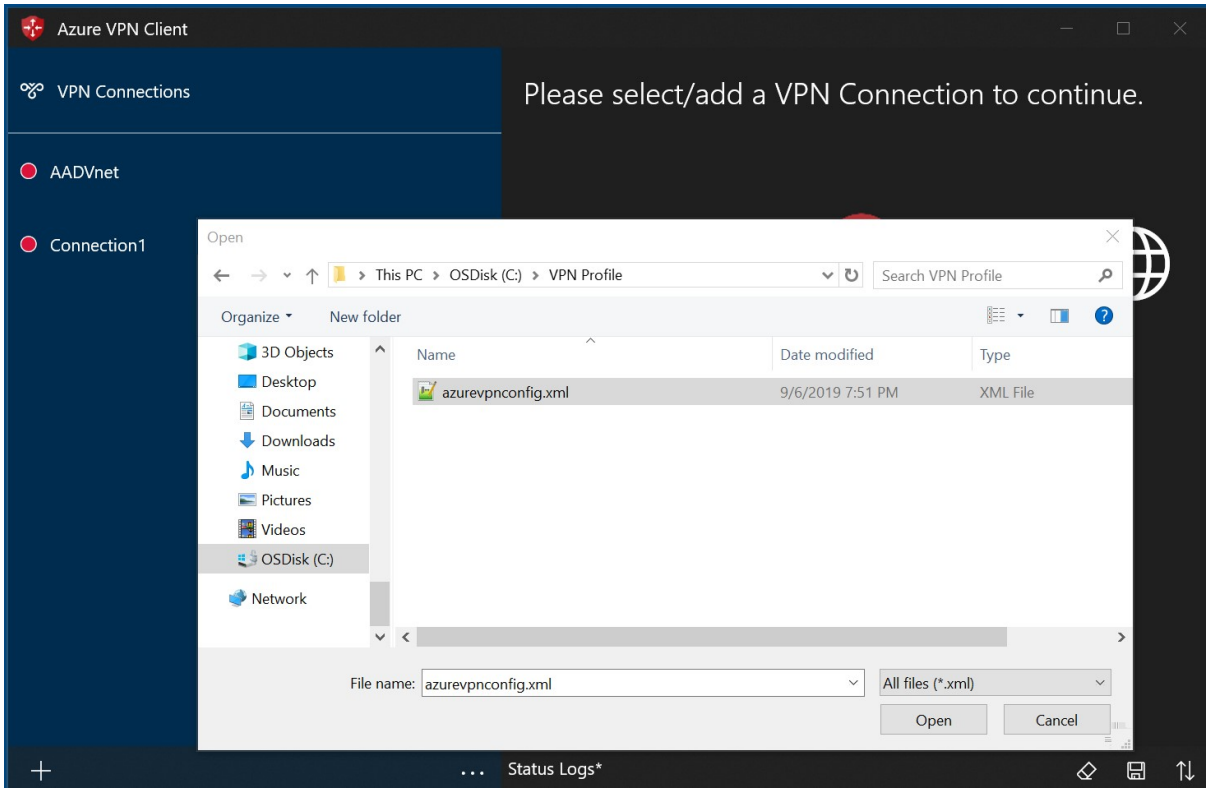
Use this link to download the Azure VPN Client.

To import a client profile

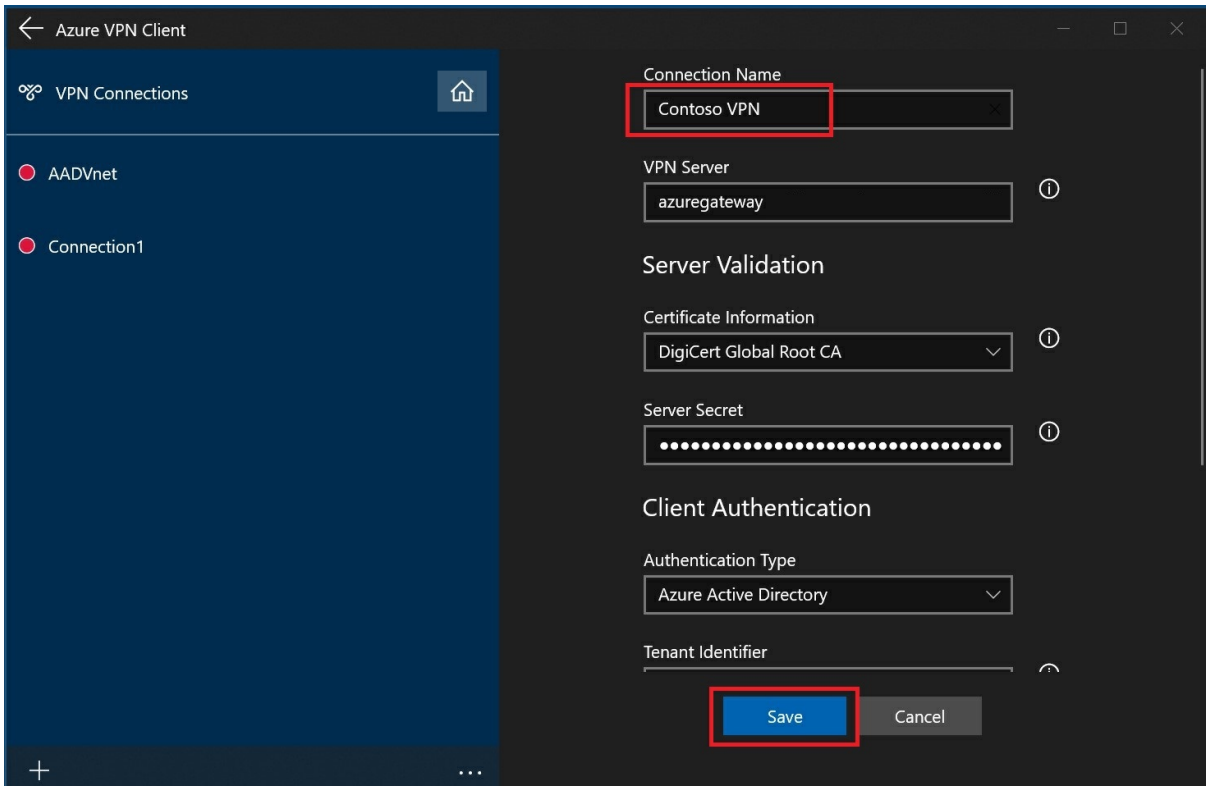
1. On the page, select **Import**.



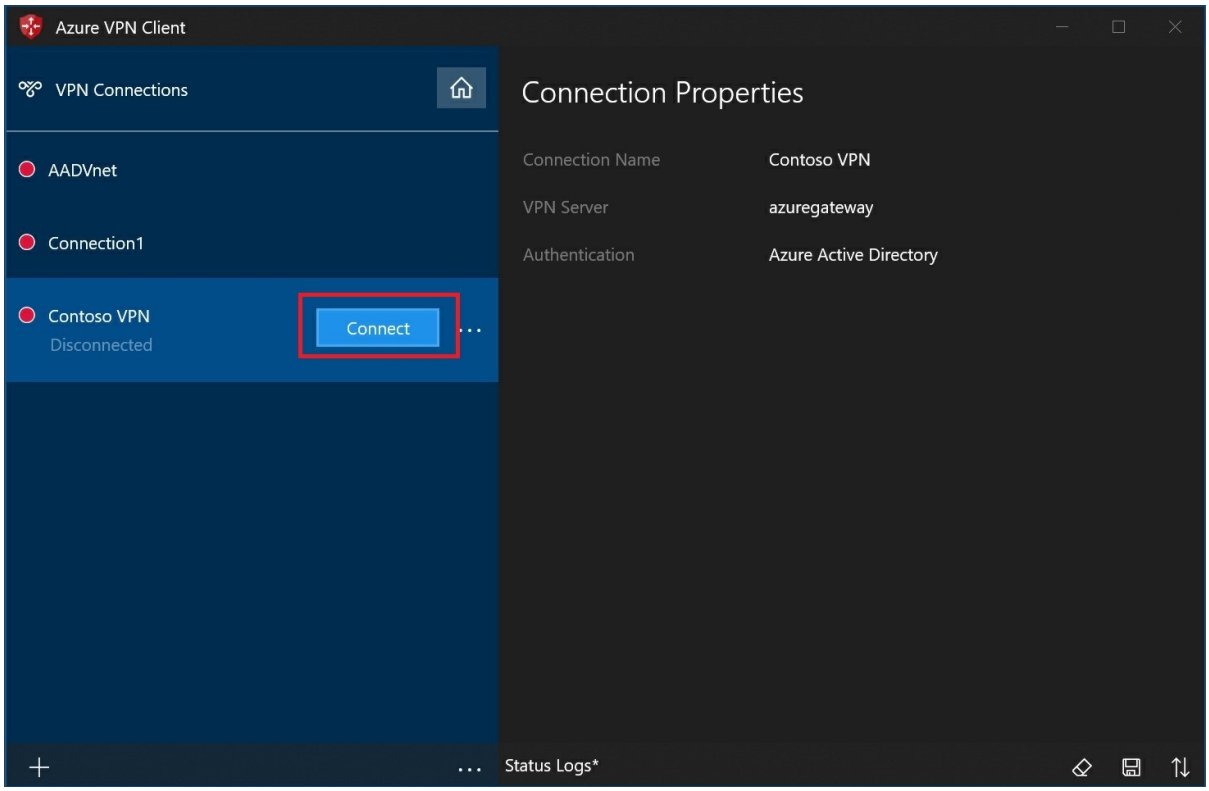
2. Browse to the profile xml file and select it. With the file selected, select **Open**.



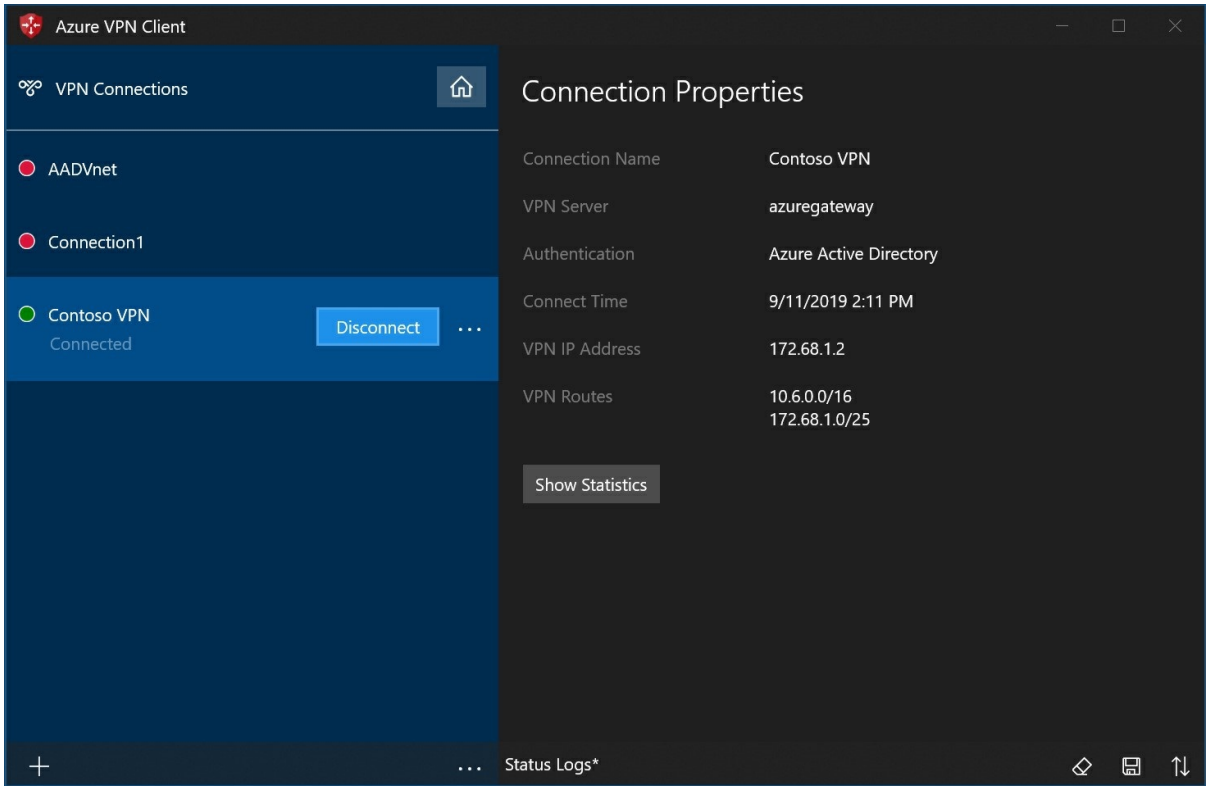
3. Specify the name of the profile and select **Save**.



4. Select **Connect** to connect to the VPN.

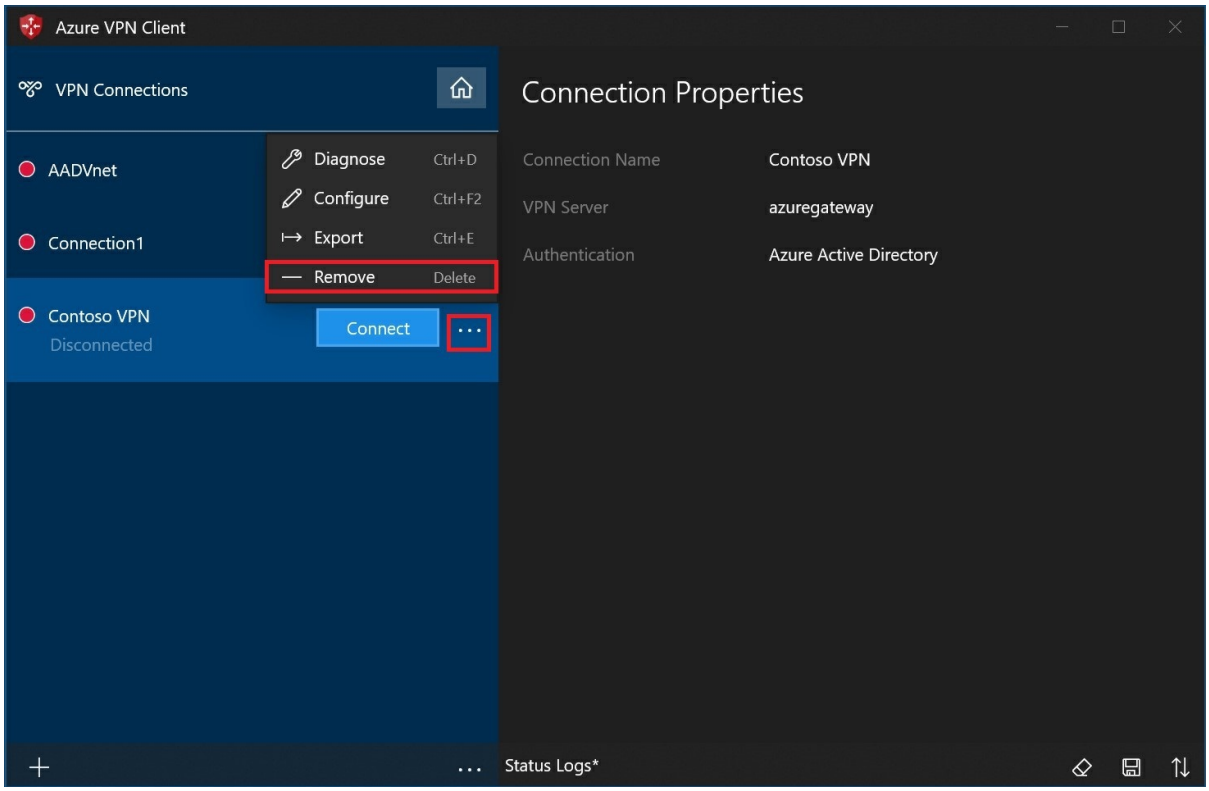


5. Once connected, the icon will turn green and say **Connected**.

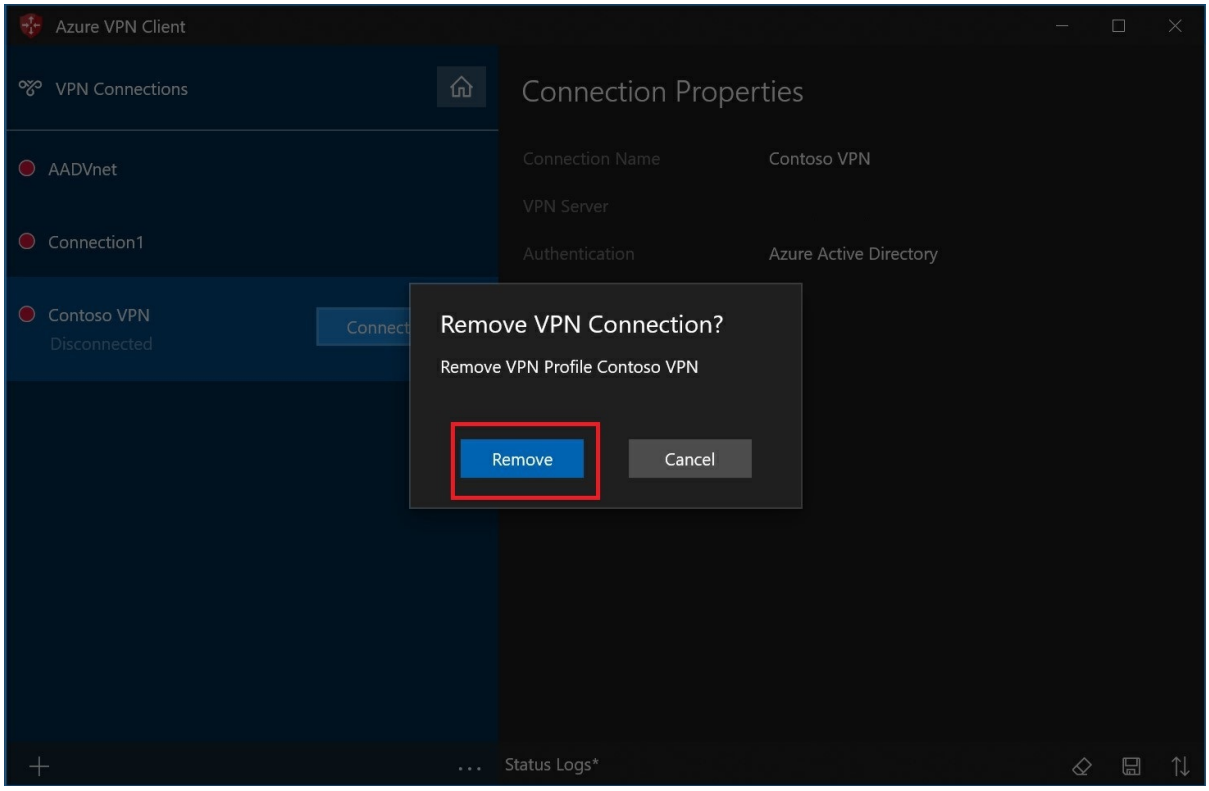


To delete a client profile

1. Select the ellipsis (...) next to the client profile that you want to delete. Then, select **Remove**.

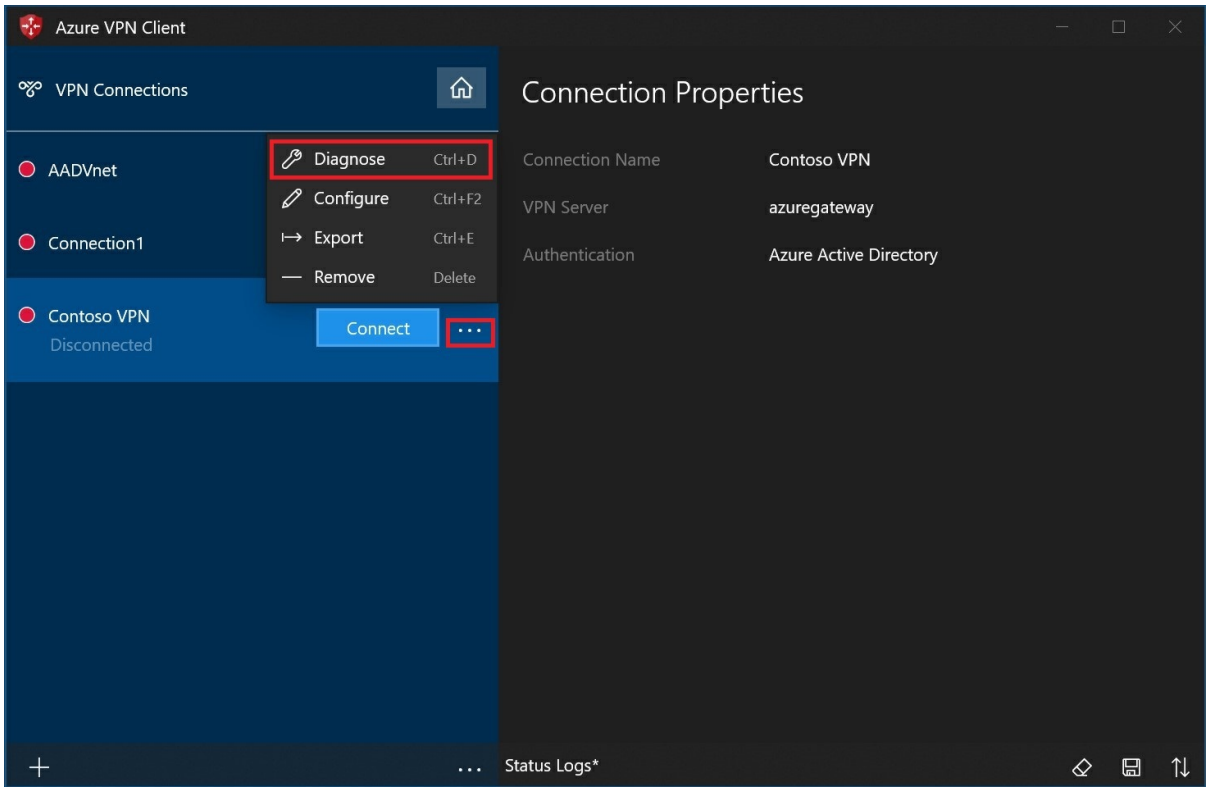


2. Select **Remove** to delete.

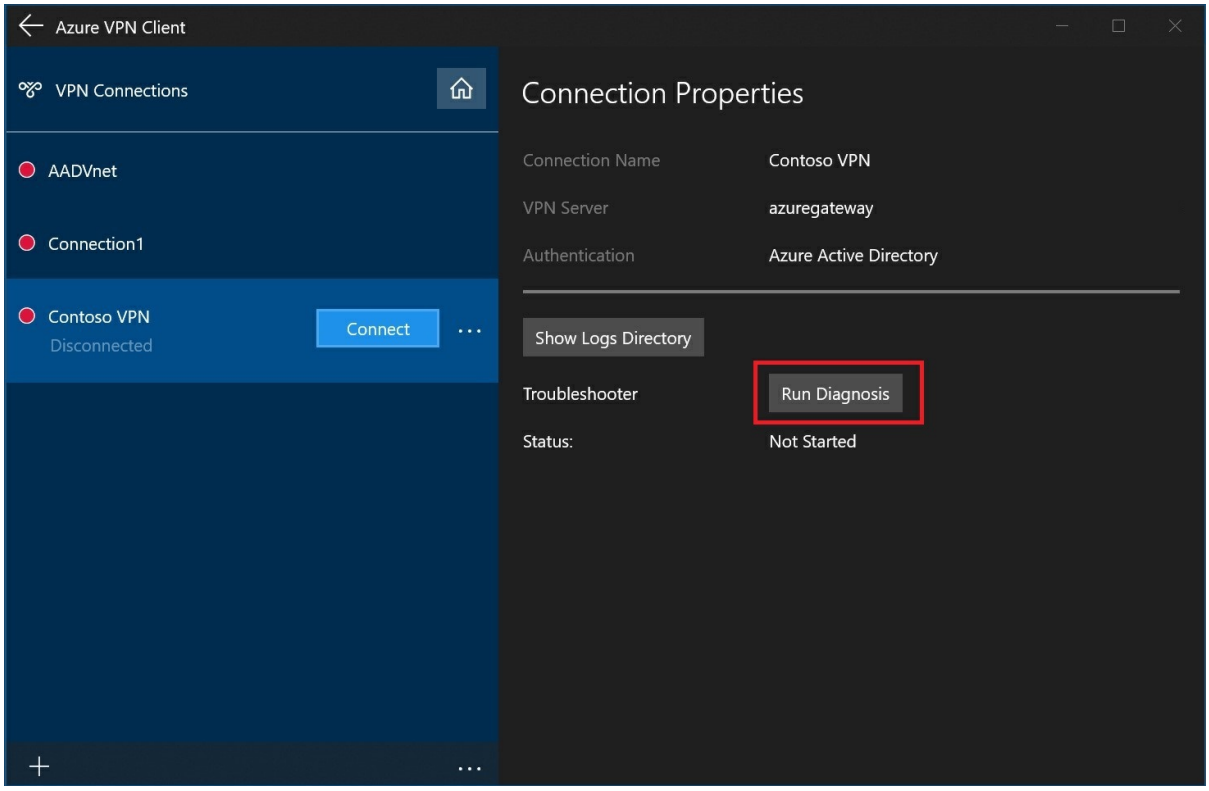


To diagnose connection issues

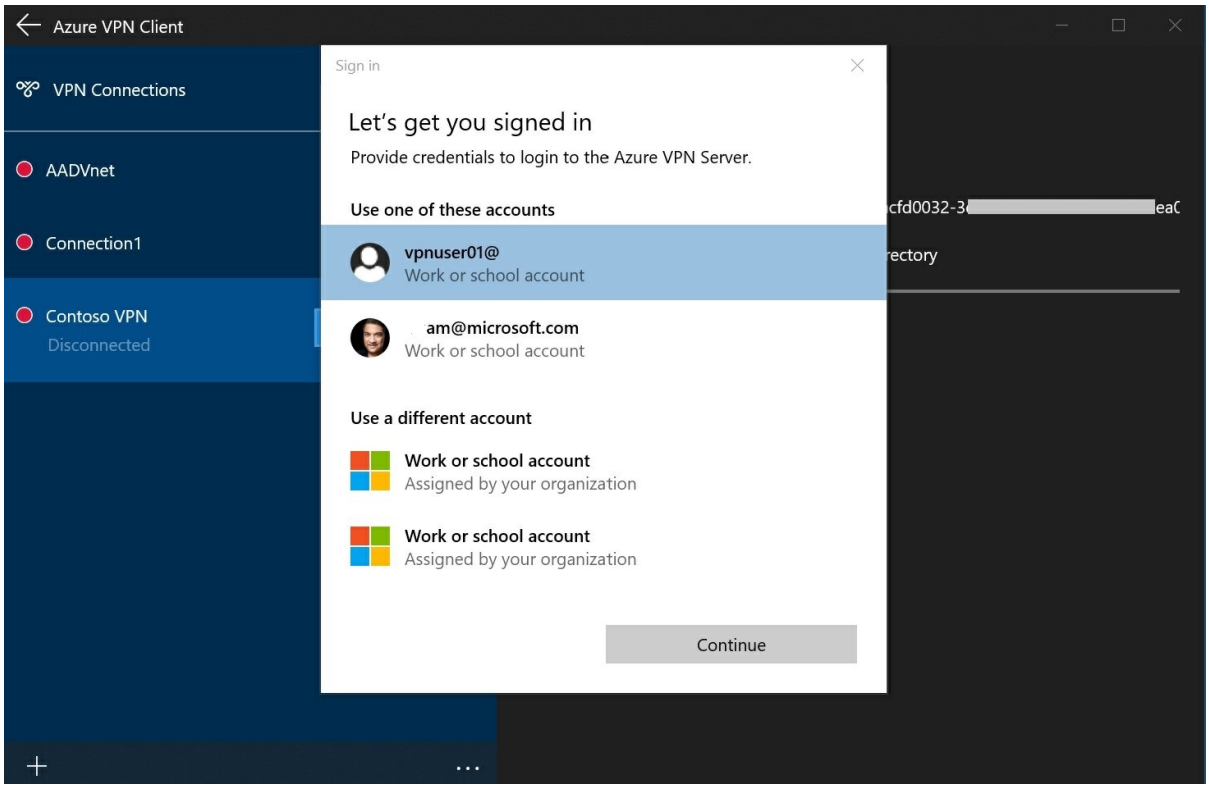
1. To diagnose connection issues, you can use the **Diagnose** tool. Select the ellipsis (...) next to the VPN connection that you want to diagnose to reveal the menu. Then select **Diagnose**.



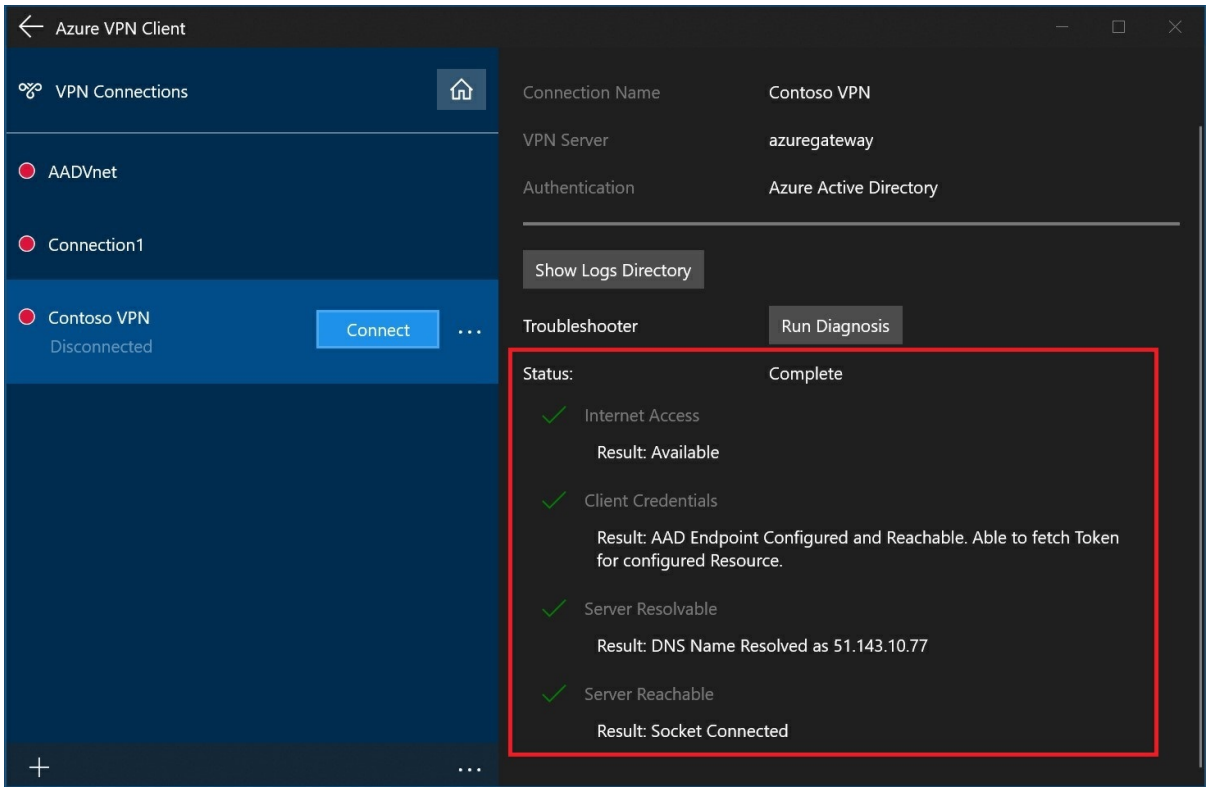
2. On the **Connection Properties** page, select **Run Diagnosis**.



3. Sign in with your credentials.



4. View the diagnosis results.



10. View your virtual WAN

1. Navigate to the virtual WAN.
2. On the Overview page, each point on the map represents a hub. Hover over any point to view the hub health summary.
3. In the Hubs and connections section, you can view hub status, site, region, VPN connection status, and bytes in and out.

11. View your resource health

1. Navigate to your WAN.
2. On your WAN page, in the **SUPPORT + Troubleshooting** section, click **Health** and view your resource.

Clean up resources

When you no longer need these resources, you can use Remove-AzureRmResourceGroup to remove the resource group and all of the resources it contains. Replace "myResourceGroup" with the name of your resource group and run the following PowerShell command:

```
Remove-AzureRmResourceGroup -Name myResourceGroup -Force
```

Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Download a global or hub-based profile for User VPN clients

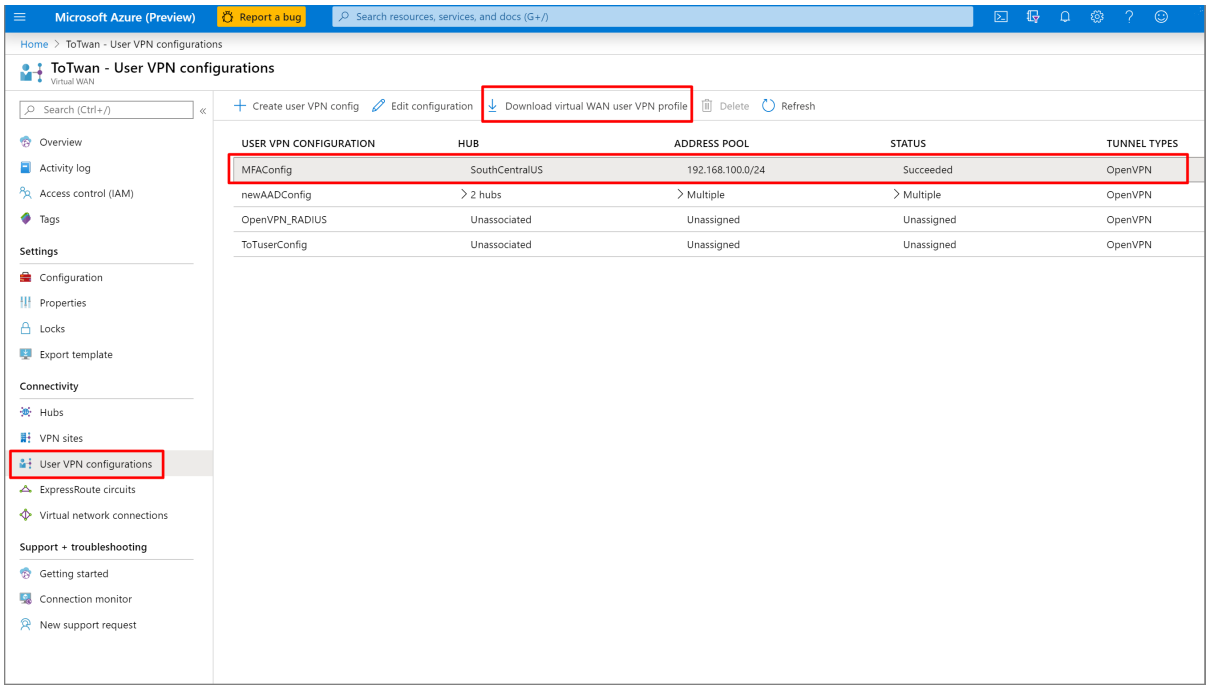
2/2/2020 • 2 minutes to read • Edit Online

Azure Virtual WAN offers two types of connectivity for remote users: Global and Hub-based. Use the following sections to learn about and download a profile.

Global profile

The profile points to a load balancer that includes all active User VPN hubs. The user is directed to the hub that is closest to the user's geographic location. This type of connectivity is useful when users travel to different locations frequently. To download the **global** profile:

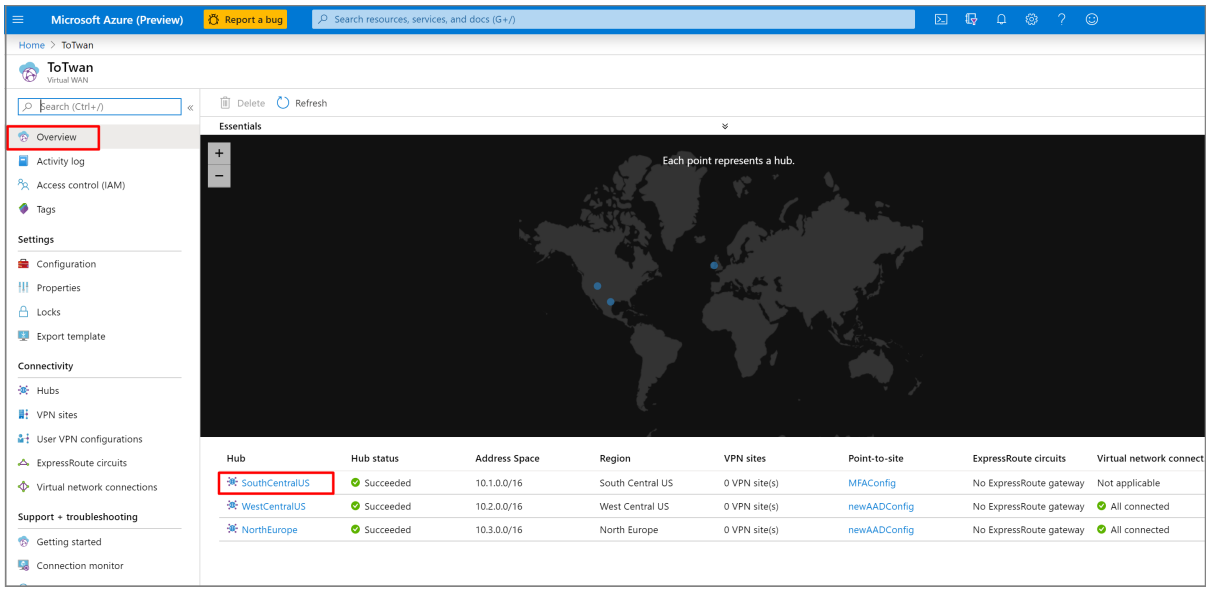
1. Navigate to the virtual WAN.
2. Click **User VPN configuration**.
3. Highlight the configuration for which you want to download the profile.
4. Click **Download virtual WAN user VPN profile**.



Hub-based profile

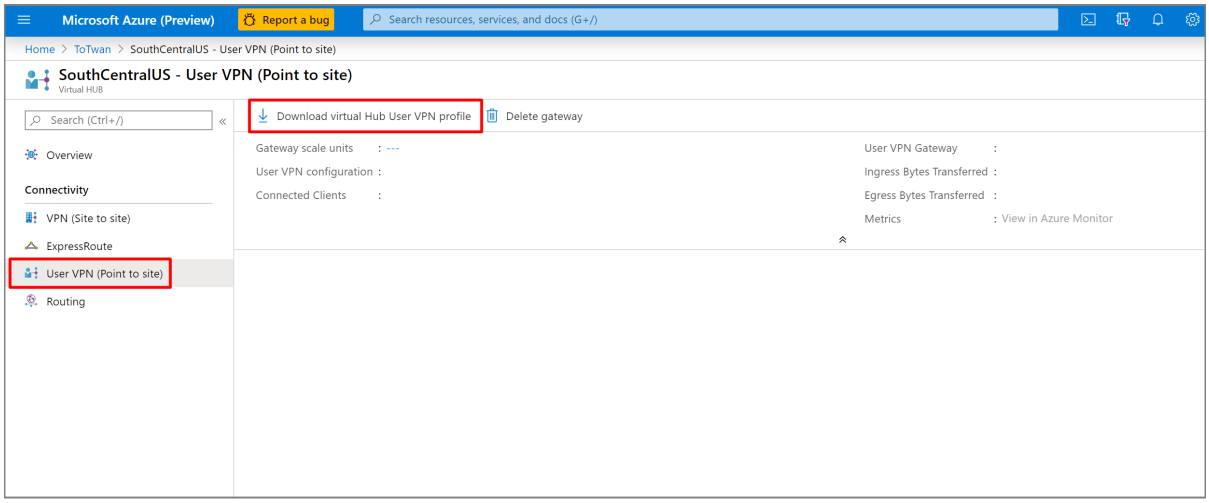
The profile points to a single hub. The user can only connect to the particular hub using this profile. To download the **hub-based** profile:

1. Navigate to the virtual WAN.
2. Click **Hub** in the Overview page.



3. Click **User VPN (Point to site)**.

4. Click **Download virtual Hub User VPN profile**.



5. Check **EAPTLS**.

6. Click **Generate and download profile**.

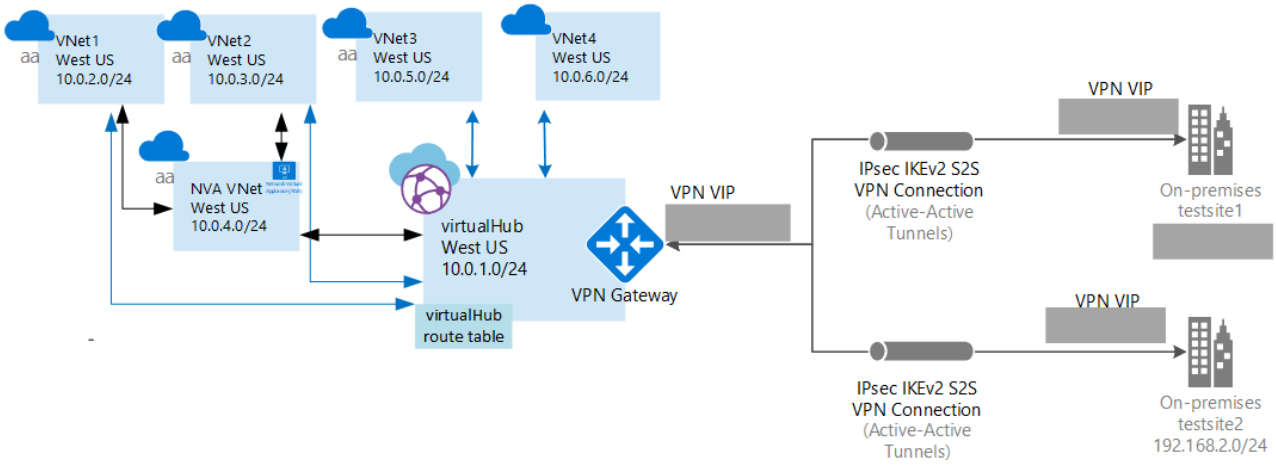
Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Create a Virtual WAN hub route table for NVAs: Azure portal

1/2/2020 • 4 minutes to read • Edit Online

This article shows you how to steer traffic from a branch (on-premises site) connected to the Virtual WAN hub to a Spoke Vnet via a Network Virtual Appliance (NVA).



Before you begin

Verify that you have met the following criteria:

- You have a Network Virtual Appliance (NVA). A Network Virtual Appliance is a third-party software of your choice that is typically provisioned from Azure Marketplace in a virtual network.
  - A private IP address must be assigned to the NVA network interface.
  - The NVA is not deployed in the virtual hub. It must be deployed in a separate VNet.
  - The NVA VNet may have one or many virtual networks connected to it. In this article, we refer to the NVA VNet as an 'indirect spoke VNet'. These VNets can be connected to the NVA VNet by using VNet peering. The Vnet Peering links are depicted by black arrows in the above figure between Vnet 1, Vnet 2 and NVA Vnet.
- You have created 2 VNets. They will be used as spoke VNets.
  - For this exercise, the VNet spoke address spaces are: VNet1: 10.0.2.0/24 and VNet2: 10.0.3.0/24. If you need information on how to create a VNet, see Create a virtual network.
  - Ensure there are no virtual network gateways in any of the VNets.
  - For this configuration, these VNets do not require a gateway subnet.

1. Sign in

From a browser, navigate to the Azure portal and sign in with your Azure account.

2. Create a virtual WAN

Create a virtual WAN. For the purposes of this exercise, you can use the following values:

- **Virtual WAN name:** myVirtualWAN
- **Resource group:** testRG
- **Location:** West US

1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create**.
3. On the **Create WAN** page, fill in the following fields:
   - **Name** - Type the Name that you want to call your WAN.
   - **Subscription** - Select the subscription that you want to use.
   - **Resource Group** - Create new or use existing.
   - **Resource Location** - Choose a resource location from the dropdown. A WAN is a global resource and does not live in a particular region. However, you must select a region in order to more easily manage and locate the WAN resource that you create.
4. After you finish filling out the fields, click **Create**.

3. Create a hub

Create the hub. For the purposes of this exercise, you can use the following values:

- **Location:** West US
- **Name:** westushub
- **Hub private address space:** 10.0.1.0/24

A hub contains the gateway. Once the hub is created, you'll be charged for the hub, even if you don't attach any sites. It takes 30 minutes to create the hub and gateway.

1. Locate the Virtual WAN that you created. On the Virtual WAN page, under the **Virtual WAN architecture** section, click **Hubs**.
2. On the Hubs page, click **+New Hub** to open the **Create virtual hub** page.
3. On the **Create virtual hub** page, complete the following fields:
   - Location
   - Name
   - Hub private address space

Click **Confirm** to create the hub. Click **Refresh** to view the hub on the **Hubs** page.

4. Create and apply a hub route table

Update the hub with a hub route table. For the purposes of this exercise, you can use the following values:

- **Spoke VNet address spaces:** (VNet1 and VNet2) 10.0.2.0/24 and 10.0.3.0/24
- **DMZ NVA network interface private IP address:** 10.0.4.5

1. Navigate to your virtual WAN.
2. Click the hub for which you want to create a route table.
3. Click the **...**, and then click **Edit virtual hub**.
4. On the **Edit virtual hub** page, scroll down and select the checkbox **Use table for routing**.
5. In the **If destination prefix is** column, add the address spaces. In the **Send to next hop** column, add the DMZ NVA network interface private IP address.

6. Click **Confirm** to update the hub resource with the route table settings.

5. Create the VNet connections

Create a Vnet connection from each indirect spoke VNet (VNet1 and VNet2) to the hub. These Vnet connections are depicted by the blue arrows in the above figure. Then, create a Vnet connection from the NVA VNet to the hub (black arrow in the figure).

For this step, you can use the following values:

VNET NAME	CONNECTION NAME
VNet1	testconnection1
VNet2	testconnection2
NVAVNet	testconnection3

Repeat the following procedure for each VNet that you want to connect.

1. On the page for your virtual WAN, click **Virtual network connections**.
2. On the virtual network connection page, click **+Add connection**.
3. On the **Add connection** page, fill in the following fields:
   - **Connection name** - Name your connection.
   - **Hubs** - Select the hub you want to associate with this connection.
   - **Subscription** - Verify the subscription.
   - **Virtual network** - Select the virtual network you want to connect to this hub. The virtual network cannot have an already existing virtual network gateway.
4. Click **OK** to create the connection.

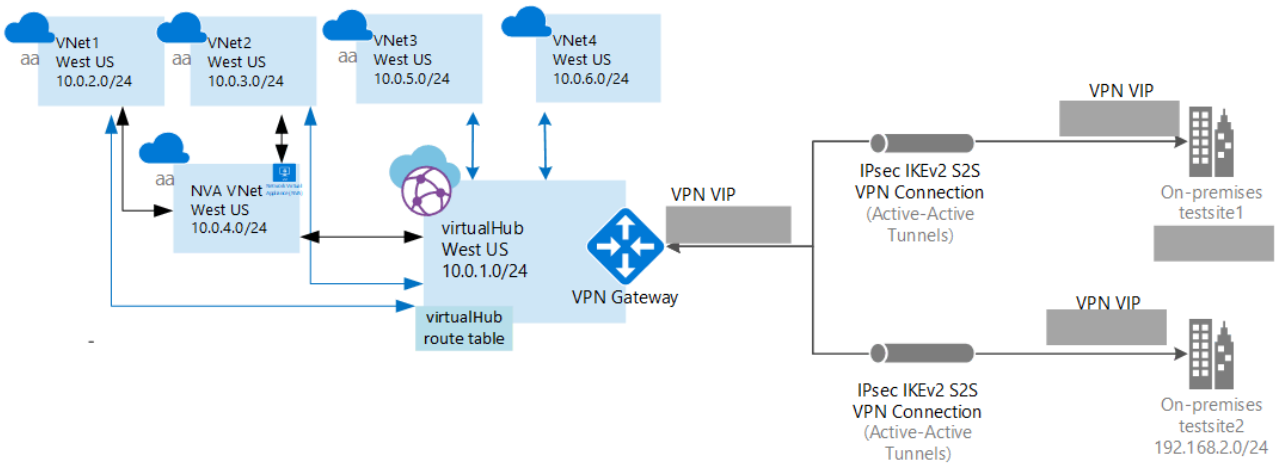
Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

Create a Virtual Hub route table to steer traffic to a Network Virtual Appliance

1/3/2020 • 2 minutes to read • Edit Online

This article shows you how to steer traffic from a Virtual Hub to a Network Virtual Appliance.



In this article you learn how to:

- Create a WAN
- Create a hub
- Create hub virtual network connections
- Create a hub route
- Create a route table
- Apply the route table

Before you begin

> **NOTE**
> This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see Introducing the new Azure PowerShell Az module. For Az module installation instructions, see Install Azure PowerShell.

Verify that you have met the following criteria:

1. You have a Network Virtual Appliance (NVA). This is a third-party software of your choice that is typically provisioned from Azure Marketplace in a virtual network.
2. You have a private IP assigned to the NVA network interface.
3. The NVA cannot be deployed in the virtual hub. It must be deployed in a separate VNet. For this article, the NVA VNet is referred to as the 'DMZ VNet'.
4. The 'DMZ VNet' may have one or many virtual networks connected to it. In this article, this VNet is referred to as 'Indirect spoke VNet'. These VNets can be connected to the DMZ VNet using VNet peering.
5. Verify that you have 2 VNets already created. These will be used as spoke VNets. For this article, the VNet spoke address spaces are 10.0.2.0/24 and 10.0.3.0/24. If you need information on how to create a VNet, see

Create a virtual network using PowerShell.

6. Ensure there are no virtual network gateways in any VNets.

1. Sign in

Make sure you install the latest version of the Resource Manager PowerShell cmdlets. For more information about installing PowerShell cmdlets, see How to install and configure Azure PowerShell. This is important because earlier versions of the cmdlets do not contain the current values that you need for this exercise.

1. Open your PowerShell console with elevated privileges, and sign in to your Azure account. This cmdlet prompts you for the sign-in credentials. After signing in, it downloads your account settings so that they are available to Azure PowerShell.

```
Connect-AzAccount
```

2. Get a list of your Azure subscriptions.

```
Get-AzSubscription
```

3. Specify the subscription that you want to use.

```
Select-AzSubscription -SubscriptionName "Name of subscription"
```

2. Create resources

1. Create a resource group.

```
New-AzResourceGroup -Location "West US" -Name "testRG"
```

2. Create a virtual WAN.

```
$virtualWan = New-AzVirtualWan -ResourceGroupName "testRG" -Name "myVirtualWAN" -Location "West US"
```

3. Create a virtual hub.

```
New-AzVirtualHub -VirtualWan $virtualWan -ResourceGroupName "testRG" -Name "westushub" -AddressPrefix
"10.0.1.0/24" -Location "West US"
```

3. Create connections

Create hub virtual network connections from Indirect Spoke VNet and the DMZ VNet to the virtual hub.

```
$remoteVirtualNetwork1= Get-AzVirtualNetwork -Name "indirectspoke1" -ResourceGroupName "testRG"
$remoteVirtualNetwork2= Get-AzVirtualNetwork -Name "indirectspoke2" -ResourceGroupName "testRG"
$remoteVirtualNetwork3= Get-AzVirtualNetwork -Name "dmzvnet" -ResourceGroupName "testRG"

New-AzVirtualHubVnetConnection -ResourceGroupName "testRG" -VirtualHubName "westushub" -Name
"testvnetconnection1" -RemoteVirtualNetwork $remoteVirtualNetwork1
New-AzVirtualHubVnetConnection -ResourceGroupName "testRG" -VirtualHubName "westushub" -Name
"testvnetconnection2" -RemoteVirtualNetwork $remoteVirtualNetwork2
New-AzVirtualHubVnetConnection -ResourceGroupName "testRG" -VirtualHubName "westushub" -Name
"testvnetconnection3" -RemoteVirtualNetwork $remoteVirtualNetwork3
```

4. Create a virtual hub route

For this article, the Indirect Spoke VNet address spaces are 10.0.2.0/24 and 10.0.3.0/24, and the DMZ NVA network interface private IP address is 10.0.4.5.

```
$route1 = New-AzVirtualHubRoute -AddressPrefix @("10.0.2.0/24", "10.0.3.0/24") -NextHopIpAddress "10.0.4.5"
```

5. Create a virtual hub route table

Create a virtual hub route table, then apply the created route to it.

```
$routeTable = New-AzVirtualHubRouteTable -Route @($route1)
```

6. Commit the changes

Commit the changes into the virtual hub.

```
Update-AzVirtualHub -ResourceGroupName "testRG" -Name "westushub" -RouteTable $routeTable
```

Next steps

To learn more about Virtual WAN, see the Virtual WAN Overview page.

View effective routes of a virtual hub

11/4/2019 • 2 minutes to read • Edit Online

You can view all the routes of your Virtual WAN hub in the Azure portal. To view the routes, navigate to the virtual hub, then select **Routing -> View Effective Routes**.

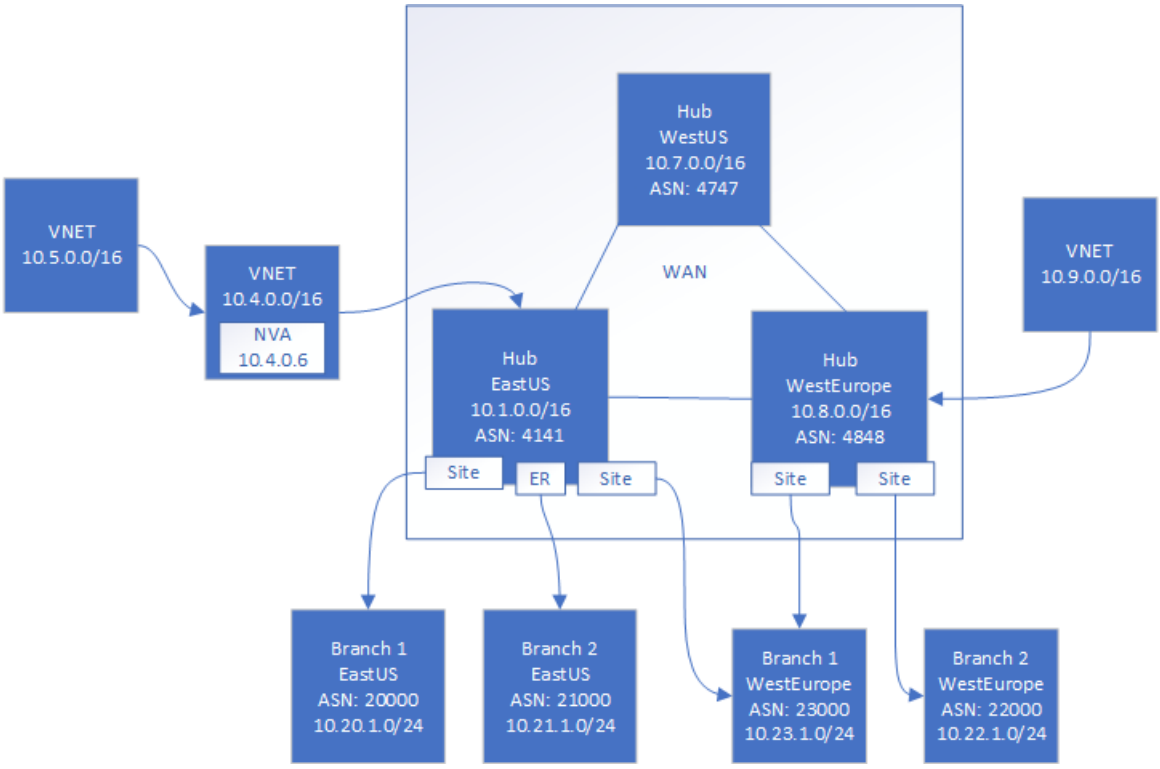
Understanding routes

The following example can help you better understand how Virtual WAN routing appears.

In this example, we have a virtual WAN with three hubs. The first hub is in the East US region, second hub is in the West Europe region, and the third hub is in the West US region. In a virtual WAN, all hubs are interconnected. In this example, we will assume that the East US and West Europe hubs have connections from on-premises branches (spokes) and Azure virtual networks (spokes).

An Azure VNet spoke (10.4.0.0/16) with a Network Virtual Appliance (10.4.0.6) is further peered to a VNet (10.5.0.0/16). See Additional information later in this article for more information about the hub route table.

In this example, we also assume that the West Europe Branch 1 is connected to East US hub, as well as to the West Europe hub. An ExpressRoute circuit in East US connects Branch 2 to the East US hub.



View effective routes

When you select 'View Effective Routes' in the portal, it produces the output shown in the Hub route table for the East US Hub.

To put this in perspective, the first line implies that the East US hub has learned the route of 10.20.1.0/24 (Branch 1) due to the VPN *Next hop type* connection ('Next hop' VPN Gateway Instance0 IP 10.1.0.6, Instance1 IP 10.1.0.7). *Route Origin* points to the resource ID. *AS Path* indicates the AS Path for Branch 1.

Hub route table

Use the scroll bar at the bottom of the table to view the "AS Path".

PREFIX	NEXT HOP TYPE	NEXT HOP	ROUTE ORIGIN	AS PATH
10.20.1.0/24	VPN	10.1.0.6, 10.1.0.7	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/vpnGateways/343a19aa6ac74e4d81f05ccccf1536cf-eastus-gw	20000
10.21.1.0/24	ExpressRoute	10.1.0.10, 10.1.0.11	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/expressRouteGateways/4444a6ac74e4d85555-eastus-gw	21000
10.23.1.0/24	VPN	10.1.0.6, 10.1.0.7	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/vpnGateways/343a19aa6ac74e4d81f05ccccf1536cf-eastus-gw	23000
10.4.0.0/16	Virtual Network Connection	On-link		
10.5.0.0/16	IP Address	10.4.0.6	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/virtualHubs/easthub_1/routeTables/table_1	
0.0.0.0/0	IP Address	`<Azure Firewall IP>`	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/virtualHubs/easthub_1/routeTables/table_1	
10.22.1.0/16	Remote Hub	10.8.0.6, 10.8.0.7	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/virtualHubs/westhub_	4848-22000

PREFIX	NEXT HOP TYPE	NEXT HOP	ROUTE ORIGIN	AS PATH
10.9.0.0/16	Remote Hub	On-link	/subscriptions/ `<sub>` /resourceGroups/ `<rg>` /providers/Microsoft.Network/virtualHubs/westhub_1	

> **NOTE**
> If the East US and the West Europe hubs were not communicating with each other in the example topology, the route learned (10.9.0.0/16) would not exist. Hubs only advertise networks that are directly connected to them.

Additional information

About the hub route table

You can create a virtual hub route and apply the route to the virtual hub route table. You can apply multiple routes to the virtual hub route table. This lets you set a route for destination VNet via an IP address (typically the Network Virtual Appliance (NVA) in a spoke VNet). For more information about NVAs, see Route traffic from a virtual hub to an NVA.

About default route (0.0.0.0/0)

A virtual hub has the ability to propagate a learned default route to a virtual network, a site-to-site VPN, and an ExpressRoute connection if the flag is 'Enabled' on the connection. This flag is visible when you edit a virtual network connection, a VPN connection, or an ExpressRoute connection. 'EnableInternetSecurity' is always false by default on Hub VNet, ExpressRoute, and VPN connections.

The default route does not originate in the virtual WAN hub. The default route is propagated if it is already learned by the virtual WAN hub as a result of deploying a firewall in the hub, or if another connected site has forced tunneling enabled.

Next steps

For more information about Virtual WAN, see the Virtual WAN Overview.

Virtual WAN FAQ

11/4/2019 • 11 minutes to read • Edit Online

What is the difference between an Azure virtual network gateway (VPN Gateway) and an Azure Virtual WAN VPN gateway?

Virtual WAN provides large-scale site-to-site connectivity and is built for throughput, scalability, and ease of use. When you connect a site to a Virtual WAN VPN gateway, it is different from a regular virtual network gateway that uses a gateway type 'VPN'. Similarly, when you connect an ExpressRoute circuit to a Virtual WAN hub, it uses a different resource for the ExpressRoute gateway than the regular virtual network gateway that uses gateway type 'ExpressRoute'. Virtual WAN supports up to 20 Gbps aggregate throughput both for VPN and ExpressRoute. Virtual WAN also has automation for connectivity with an ecosystem of CPE branch device partners. CPE branch devices have built-in automation that auto-provisions and connects into Azure Virtual WAN. These devices are available from a growing ecosystem of SD-WAN and VPN partners. See the Preferred Partner List.

How is Virtual WAN different from an Azure virtual network gateway?

A virtual network gateway VPN is limited to 30 tunnels. For connections, you should use Virtual WAN for large-scale VPN. You can connect up to 1,000 branch connections per region (virtual hub) with aggregate of 20 Gbps per hub. A connection is an active-active tunnel from the on-premises VPN device to the virtual hub. You can have one hub per region, which means you can connect more than 1,000 branches across hubs.

What is a Virtual WAN Gateway Scale Unit

A scale unit is an unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps . 1 scale unit of ExpressRoute = 2 Gbps. Example : 10 scale unit of VPN would imply 500 Mbps * 10 = 5 Gbps

Which device providers (Virtual WAN partners) are supported?

At this time, many partners support the fully automated Virtual WAN experience. For more information, see Virtual WAN partners.

What are the Virtual WAN partner automation steps?

For partner automation steps, see Virtual WAN partner automation.

Am I required to use a preferred partner device?

No. You can use any VPN-capable device that adheres to the Azure requirements for IKEv2/IKEv1 IPsec support.

How do Virtual WAN partners automate connectivity with Azure Virtual WAN?

Software-defined connectivity solutions typically manage their branch devices using a controller, or a device provisioning center. The controller can use Azure APIs to automate connectivity to the Azure Virtual WAN. The automation includes uploading branch information, downloading the Azure configuration, setting up IPSec tunnels into Azure Virtual hubs, and automatically setting up connectivity form the branch device to Azure Virtual WAN. When you have hundreds of branches, connecting using Virtual WAN CPE Partners is easy because the onboarding experience takes away the need to set up, configure, and manage large-scale IPsec connectivity. For more information, see Virtual WAN partner automation.

How is Virtual WAN supporting SD-WAN devices?

Virtual WAN partners automate IPsec connectivity to Azure VPN end points. If the Virtual WAN partner is an SD-WAN provider, then it is implied that the SD-WAN controller manages automation and IPsec connectivity to Azure VPN end points. If the SD-WAN device requires its own end point instead of Azure VPN for any proprietary SD-WAN functionality, you can deploy the SD-WAN end point in an Azure VNet and coexist with Azure Virtual WAN.

Does Virtual WAN change any existing connectivity features?

There are no changes to existing Azure connectivity features.

Are there new Resource Manager resources available for Virtual WAN?

Yes, Virtual WAN introduces new Resource Manager resources. For more information, please see the Overview.

How many VPN devices can connect to a single hub?

Up to 1,000 connections are supported per virtual hub. Each connection consists of four links and each link connection supports two tunnels that are in an active-active configuration. The tunnels terminate in an Azure virtual hub vpngateway.

Can the on-premises VPN device connect to multiple Hubs?

Yes. Traffic flow, when commencing, is from the on-premises device to the closest Microsoft network edge, and then to the virtual hub.

Can I deploy and use my favorite network virtual appliance (in an NVA VNet) with Azure Virtual WAN?

Yes, you can connect your favorite network virtual appliance (NVA) VNet to the Azure Virtual WAN. First, connect the network virtual appliance VNet to the hub with a Hub Virtual Network connection. Then, create a virtual hub route with a next hop pointing to the Virtual Appliance. You can apply multiple routes to the virtual hub Route Table. Any spokes connected to the NVA VNet must additionally be connected to the virtual hub to ensure that the spoke VNet routes are propagated to on-premises systems.

Can I create a Network Virtual Appliance inside the virtual hub?

A Network Virtual Appliance (NVA) cannot be deployed inside a virtual hub. However, you can create it in a spoke VNet that is connected to the virtual hub and enable a route in the hub to direct traffic for destination VNet via the NVA IP address (of the NIC).

Can a spoke VNet have a virtual network gateway?

No. The spoke VNet cannot have a virtual network gateway if it is connected to the virtual hub.

Is there support for BGP?

Yes, BGP is supported. When you create a VPN site, you can provide the BGP parameters in it. This will imply that any connections created in Azure for that site will be enabled for BGP. Additionally, if you had a VNet with an NVA, and if this NVA VNet was attached to a Virtual WAN hub, in order to ensure that routes from an NVA VNet are advertised appropriately, spokes that are attached to NVA VNet must disable BGP. Additionally, connect these spoke VNets to the virtual hub VNet to ensure spoke VNet routes are propagated to on-premises systems.

Can I direct traffic using UDR in the virtual hub?

Yes, you can direct traffic to a VNet using a virtual hub route table. This allows you to set routes for destination VNets in Azure via a specific IP address (typically of the NVA NIC).

Is there any licensing or pricing information for Virtual WAN?

Yes. See the Pricing page.

How do I calculate price of a hub?

- You would pay for the services in the hub. For example, lets say you have 10 branches or on-premises devices requiring to connect to Azure Virtual WAN would imply connecting to VPN end points in the hub. Lets say this is VPN of 1 scale unit = 500 Mbps, this is charged at $0.361/hr. Each connection is charged at $0.05/hr. For 10 connections, the total charge of service/hr would be $0.361 + $.5/hr. Data charges for traffic leaving Azure apply.
- There is additional hub charge. See the Pricing page.
- If you had ExpressRoute gateway due to ExpressRoute circuits connecting to a virtual hub, then you would pay for the scale unit price. Each scale unit in ER is 2 Gbps and each connection unit is charged at the same

rate as the VPN Connection unit.

How do new partners that are not listed in your launch partner list get onboarded?

All virtual WAN APIs are open API. You can go over the documentation to assess technical feasibility. If you have any question, send an email to azurevirtualwan@microsoft.com. An ideal partner is one that has a device that can be provisioned for IKEv1 or IKEv2 IPsec connectivity.

What if a device I am using is not in the Virtual WAN partner list? Can I still use it to connect to Azure Virtual WAN VPN?

Yes as long as the device supports IPsec IKEv1 or IKEv2. Virtual WAN partners automate connectivity from the device to Azure VPN end points. This implies automating steps such as 'branch information upload', 'IPsec and configuration' and 'connectivity'.Since your device is not from a Virtual WAN partner ecosystem, you will need to do the heavy lifting of manually taking the Azure configuration and updating your device to set up IPsec connectivity.

Is it possible to construct Azure Virtual WAN with a Resource Manager template?

A simple configuration of one Virtual WAN with one hub and one vpnsite can be created using an quickstart template. Virtual WAN is primarily a REST or portal driven service.

Is Global VNet peering supported with Azure Virtual WAN?

You can connect a VNet in a different region than your virtual WAN.

Can spoke VNets connected to a virtual hub communicate with each other (V2V Transit)?

Yes. Standard Virtual WAN supports Vnet to Vnet transitive connectivity via the Virtual WAN hub that the Vnets are connected to. In Virtual WAN terminology, we refer to these paths as “local Virtual WAN VNet transit” for VNets connected to a Virtual Wan Hub within a single region, and “global Virtual WAN VNet transit” for VNets connected through multiple Virtual WAN Hubs across two or more regions. VNet transit supports up to 3 Gbps of throughput during public preview. Throughput will expanded when global transit goes GA.

NOTE: Currently V2V transit preview requires a VPN GW to be deployed in a Virtual Hub to trigger the routing elements to be launched. This VPN GW is not used for the V2V transit path. This is a known limitation and will be removed at the time of V2V GA. You can delete the VPN Gateway in the hub(s) after it is fully launched as it is not needed for V2V transit functionality.

For some scenarios, spoke Vnets can also be directly peered with each other using Virtual Network Peering in addition to local or global Virtual WAN VNet transit. In this case, Vnet Peering takes precedence over the transitive connection via the Virtual WAN hub.

What is a branch connection to Azure Virtual WAN?

A connection from a branch device into Azure Virtual WAN supports up to four links. A link is the physical connectivity link at the branch location (for example: ATT, Verizon etc.). Each link connection is composed of two active/active IPsec tunnels.

Is branch-to-branch connectivity allowed in Virtual WAN?

Yes, branch-to-branch connectivity is available in Virtual WAN for VPN and VPN to ExpressRoute.

Does branch-to-branch traffic traverse through the Azure Virtual WAN?

Yes.

Does Virtual WAN require ExpressRoute from each site?

No, the Virtual WAN does not require ExpressRoute from each site. It uses standard IPsec site-to-site connectivity via internet links from the device to an Azure Virtual WAN hub. Your sites may be connected to a provider network using an ExpressRoute circuit. For Sites that are connected using ExpressRoute in a virtual hub, sites can have branch to branch traffic flow between VPN and ExpressRoute.

Is there a network throughput limit when using Azure Virtual WAN?

Number of branches is limited to 1000 connections per hub/region and a total of 20 Gbps in the hub. You can have 1 hub per region.

How many VPN connections does a Virtual WAN hub support?

An Azure Virtual WAN hub can support up to 1,000 S2S connections, 10,000 P2S connections, and 4 ExpressRoute connections simultaneously.

What is the total VPN throughput of a VPN tunnel and a connection?

The total VPN throughput of a hub is up to 20 Gbps based on the chosen scale unit. Throughput is shared by all existing connections. Each tunnel in a connection can support up to 1 Gbps.

I don't see the 20 Gbps setting for the virtual hub in the portal. How do I configure that?

Navigate to the VPN gateway inside a hub on the portal and click on the scale unit to change it to the appropriate setting.

Does Virtual WAN allow the on-premises device to utilize multiple ISPs in parallel, or is it always a single VPN tunnel?

A connection coming into a virtual WAN VPN is always an active-active tunnel (for resiliency within the same hub/region) using a link available at the branch. This link may be an ISP link at the on-premises branch. Virtual WAN 'VPNSite' provides the ability to add link information to the site. If you have multiple ISPs at the branch and each of the ISPs provided a link, that information can be set up in the VPN site info in Azure. However, managing failover across ISPs at the branch is completely a branch-centric routing operation.

What is global transit architecture?

For information about global transit architecture, see Global transit network architecture and Virtual WAN.

How is traffic routed on the Azure backbone?

The traffic follows the pattern: branch device ->ISP->Microsoft network edge->Microsoft DC (hub VNet)->Microsoft network edge->ISP->branch device

In this model, what do you need at each site? Just an internet connection?

Yes. An internet connection and physical device that supports IPsec, preferably from our integrated Virtual WAN partners. Optionally, you can manually manage the configuration and connectivity to Azure from your preferred device.

How do I enable default route (0.0.0.0/0) in a connection (VPN, ExpressRoute, or Virtual Network):

A virtual hub can propagate a learned default route to a virtual network/site-to-site VPN/ExpressRoute connection if the flag is 'Enabled' on the connection. This flag is visible when the user edits a virtual network connection, a VPN connection, or an ExpressRoute connection. By default, this flag is disabled when a site or an ExpressRoute circuit is connected to a hub. It is enabled by default when a virtual network connection is added to connect a VNet to a virtual hub. The default route does not originate in the Virtual WAN hub; the default route is propagated if it is already learned by the Virtual WAN hub as a result of deploying a firewall in the hub, or if another connected site has forced-tunneling enabled.

What are the differences between the Virtual WAN types (Basic and Standard)?

The 'Basic' WAN type lets you create a basic hub (SKU = Basic). A 'Standard' WAN type lets you create standard hub (SKU = Standard). Basic hubs are limited to site-to-site VPN functionality. Standard hubs let you have ExpressRoute, User VPN (P2S), full mesh hub, and VNet-to-VNet transit through the hubs. You pay a base charge of $0.25/hr for standard hubs and a data processing fee for transiting through the hubs during VNet-to-VNet connectivity, as well as data processing for hub to hub traffic. For more information, see Basic and Standard virtual WANs. For pricing, see the Pricing page.

Azure subscription and service limits, quotas, and constraints

2/25/2020 • 85 minutes to read • Edit Online

This document lists some of the most common Microsoft Azure limits, which are also sometimes called quotas.

To learn more about Azure pricing, see Azure pricing overview. There, you can estimate your costs by using the pricing calculator. You also can go to the pricing details page for a particular service, for example, Windows VMs. For tips to help manage your costs, see Prevent unexpected costs with Azure billing and cost management.

Managing limits

If you want to raise the limit or quota above the default limit, open an online customer support request at no charge. The limits can't be raised above the maximum limit value shown in the following tables. If there's no maximum limit column, the resource doesn't have adjustable limits.

Free Trial subscriptions aren't eligible for limit or quota increases. If you have a Free Trial subscription, you can upgrade to a Pay-As-You-Go subscription. For more information, see Upgrade your Azure Free Trial subscription to a Pay-As-You-Go subscription and the Free Trial subscription FAQ.

Some limits are managed at a regional level.

Let's use vCPU quotas as an example. To request a quota increase with support for vCPUs, you must decide how many vCPUs you want to use in which regions. You then make a specific request for Azure resource group vCPU quotas for the amounts and regions that you want. If you need to use 30 vCPUs in West Europe to run your application there, you specifically request 30 vCPUs in West Europe. Your vCPU quota isn't increased in any other region--only West Europe has the 30-vCPU quota.

As a result, decide what your Azure resource group quotas must be for your workload in any one region. Then request that amount in each region into which you want to deploy. For help in how to determine your current quotas for specific regions, see Resolve errors for resource quotas.

General limits

For limits on resource names, see Naming rules and restrictions for Azure resources.

For information about Resource Manager API read and write limits, see Throttling Resource Manager requests.

Subscription limits

The following limits apply when you use Azure Resource Manager and Azure resource groups.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Subscriptions per Azure Active Directory tenant	Unlimited.	Unlimited.
Coadministrators per subscription	Unlimited.	Unlimited.
Resource groups per subscription	980	980

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Azure Resource Manager API request size	4,194,304 bytes.	4,194,304 bytes.
Tags per subscription[1]	Unlimited.	Unlimited.
Unique tag calculations per subscription[1]	10,000	10,000
Subscription-level deployments per location	800[2]	800

[1]You can apply an unlimited number of tags per subscription. The number of tags per resource or resource group is limited to 50. Resource Manager returns a list of unique tag name and values in the subscription only when the number of tags is 10,000 or less. You still can find a resource by tag when the number exceeds 10,000.

[2]If you reach the limit of 800 deployments, delete deployments from the history that are no longer needed. To delete subscription level deployments, use Remove-AzDeployment or az deployment delete.

Resource group limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Resources per resource group	N/A	Resources aren't limited by resource group. Instead, they're limited by resource type in a resource group. See next row.
Resources per resource group, per resource type	800	Some resource types can exceed the 800 limit. See Resources not limited to 800 instances per resource group.
Deployments per resource group in the deployment history	800[1]	800
Resources per deployment	800	800
Management locks per unique scope	20	20
Number of tags per resource or resource group	50	50
Tag key length	512	512
Tag value length	256	256

[1]If you reach the limit of 800 deployments per resource group, delete deployments from the history that are no longer needed. Deleting an entry from the deployment history doesn't affect the deployed resources. For more information, see Resolve error when deployment count exceeds 800.

Template limits

VALUE	DEFAULT LIMIT	MAXIMUM LIMIT
Parameters	256	256

VALUE	DEFAULT LIMIT	MAXIMUM LIMIT
Variables	256	256
Resources (including copy count)	800	800
Outputs	64	64
Template expression	24,576 chars	24,576 chars
Resources in exported templates	200	200
Template size	4 MB	4 MB
Parameter file size	64 KB	64 KB

You can exceed some template limits by using a nested template. For more information, see Use linked templates when you deploy Azure resources. To reduce the number of parameters, variables, or outputs, you can combine several values into an object. For more information, see Objects as parameters.

Active Directory limits

Here are the usage constraints and other service limits for the Azure Active Directory (Azure AD) service.

CATEGORY	LIMITS
Directories	A single user can belong to a maximum of 500 Azure AD directories as a member or a guest. A single user can create a maximum of 20 directories.
Domains	You can add no more than 900 managed domain names. If you set up all of your domains for federation with on-premises Active Directory, you can add no more than 450 domain names in each directory.
Resources	• A maximum of 50,000 Azure AD resources can be created in a single directory by users of the Free edition of Azure Active Directory by default. If you have at least one verified domain, the default directory service quota in Azure AD is extended to 300,000 Azure AD resources. • A non-admin user can create no more than 250 Azure AD resources. Both active resources and deleted resources that are available to restore count toward this quota. Only deleted Azure AD resources that were deleted fewer than 30 days ago are available to restore. Deleted Azure AD resources that are no longer available to restore count toward this quota at a value of one-quarter for 30 days. If you have developers who are likely to repeatedly exceed this quota in the course of their regular duties, you can create and assign a custom role with permission to create a limitless number of app registrations.

CATEGORY	LIMITS
Schema extensions	• String-type extensions can have a maximum of 256 characters. • Binary-type extensions are limited to 256 bytes. • Only 100 extension values, across *all* types and *all* applications, can be written to any single Azure AD resource. • Only User, Group, TenantDetail, Device, Application, and ServicePrincipal entities can be extended with string-type or binary-type single-valued attributes. • Schema extensions are available only in the Graph API version 1.21 preview. The application must be granted write access to register an extension.
Applications	A maximum of 100 users can be owners of a single application.
Application Manifest	A maximum of 1200 entries can be added in the Application Manifest.

CATEGORY	LIMITS
Groups	• A user can create a maximum of 250 groups in an Azure AD organization. • An Azure AD organization can have a maximum of 5000 dynamic groups. • A maximum of 100 users can be owners of a single group. • Any number of Azure AD resources can be members of a single group. • A user can be a member of any number of groups. • The number of members in a group that you can synchronize from your on-premises Active Directory to Azure Active Directory by using Azure AD Connect is limited to 50,000 members. • Nested Groups in Azure AD are not supported within all scenarios At this time the following are the supported scenarios with nested groups. • One group can be added as a member of another group and you can achieve group nesting. • Group membership claims (when an app is configured to receive group membership claims in the token, nested groups the signed-in user is a member of are included) • Conditional access (when scoping a conditional access policy to a group) • Restricting access to self-serve password reset • Restricting which users can do Azure AD Join and device registration The following scenarios DO NOT supported nested groups: • App role assignment (assigning groups to an app is supported, but groups nested within the directly assigned group will not have access), both for access and for provisioning • Group-based licensing (assigning a license automatically to all members of a group) • Office 365 Groups.
Application Proxy	• A maximum of 500 transactions per second per App Proxy application • A maximum of 750 transactions per second for the Azure AD organization A transaction is defined as a single http request and response for a unique resource. When throttled, clients will receive a 429 response (too many requests).

CATEGORY	LIMITS
Access Panel	• There's no limit to the number of applications that can be seen in the Access Panel per user. This applies to users assigned licenses for Azure AD Premium or the Enterprise Mobility Suite. • A maximum of 10 app tiles can be seen in the Access Panel for each user. This limit applies to users who are assigned licenses for Azure AD Free license plan. Examples of app tiles include Box, Salesforce, or Dropbox. This limit doesn't apply to administrator accounts.
Reports	A maximum of 1,000 rows can be viewed or downloaded in any report. Any additional data is truncated.
Administrative units	An Azure AD resource can be a member of no more than 30 administrative units.
Admin roles and permissions	• A group cannot be added as an owner. • A group cannot be assigned to a role. • Users' ability to read other users' directory information cannot be restricted outside of the Azure AD organization-wide switch to disable all non-admin users' access to all directory information (not recommended). More information on default permissions here. • It may take up to 15 minutes or signing out/signing in before admin role membership additions and revocations take effect.

API Management limits

RESOURCE	LIMIT
Maximum number of scale units	10 per region[1]
Cache size	5 GiB per unit[2]
Concurrent back-end connections[3] per HTTP authority	2,048 per unit[4]
Maximum cached response size	2 MiB
Maximum policy document size	256 KiB[5]
Maximum custom gateway domains per service instance[6]	20
Maximum number of CA certificates per service instance	10
Maximum number of service instances per subscription[7]	20
Maximum number of subscriptions per service instance[7]	500
Maximum number of client certificates per service instance[7]	50

RESOURCE	LIMIT
Maximum number of APIs per service instance[7]	50
Maximum number of API operations per service instance[7]	1,000
Maximum total request duration[7]	30 seconds
Maximum buffered payload size[7]	2 MiB
Maximum request URL size[8]	4096 bytes

[1]Scaling limits depend on the pricing tier. To see the pricing tiers and their scaling limits, see API Management pricing.
[2]Per unit cache size depends on the pricing tier. To see the pricing tiers and their scaling limits, see API Management pricing.
[3]Connections are pooled and reused unless explicitly closed by the back end.
[4]This limit is per unit of the Basic, Standard, and Premium tiers. The Developer tier is limited to 1,024. This limit doesn't apply to the Consumption tier.
[5]This limit applies to the Basic, Standard, and Premium tiers. In the Consumption tier, policy document size is limited to 4 KiB.
[6]This resource is available in the Premium tier only.
[7]This resource applies to the Consumption tier only.
[8]Applies to the Consumption tier only. Includes an up to 2048 bytes long query string.

App Service limits

The following App Service limits include limits for Web Apps, Mobile Apps, and API Apps.

RESOURCE	FREE	SHARED	BASIC	STANDARD	PREMIUM (V2)	ISOLATED
Web, mobile, or API apps per Azure App Service plan[1]	10	100	Unlimited[2]	Unlimited[2]	Unlimited[2]	Unlimited[2]
App Service plan	10 per region	10 per resource group	100 per resource group	100 per resource group	100 per resource group	100 per resource group
Compute instance type	Shared	Shared	Dedicated[3]	Dedicated[3]	Dedicated[3]	Dedicated[3]
Scale out (maximum instances)	1 shared	1 shared	3 dedicated[3]	10 dedicated[3]	30 dedicated[3]	100 dedicated[4]
Storage[5]	1 GB[5]	1 GB[5]	10 GB[5]	50 GB[5]	250 GB[5]	1 TB[5]
CPU time (5 minutes)[6]	3 minutes	3 minutes	Unlimited, pay at standard rates	Unlimited, pay at standard rates	Unlimited, pay at standard rates	Unlimited, pay at standard rates

RESOURCE	FREE	SHARED	BASIC	STANDARD	PREMIUM (V2)	ISOLATED
CPU time (day)[6]	60 minutes	240 minutes	Unlimited, pay at standard rates	Unlimited, pay at standard rates	Unlimited, pay at standard rates	Unlimited, pay at standard rates
Memory (1 hour)	1,024 MB per App Service plan	1,024 MB per app	N/A	N/A	N/A	N/A
Bandwidth	165 MB	Unlimited, data transfer rates apply	Unlimited, data transfer rates apply	Unlimited, data transfer rates apply	Unlimited, data transfer rates apply	Unlimited, data transfer rates apply
Application architecture	32-bit	32-bit	32-bit/64-bit	32-bit/64-bit	32-bit/64-bit	32-bit/64-bit
Web sockets per instance[7]	5	35	350	Unlimited	Unlimited	Unlimited
IP connections	600	600	Depends on instance size[8]	Depends on instance size[8]	Depends on instance size[8]	16,000
Concurrent debugger connections per application	1	1	1	5	5	5
App Service Certificates per subscription[9]	Not supported	Not supported	10	10	10	10
Custom domains per app	0 (azurewebsites.net subdomain only)	500	500	500	500	500
Custom domain SSL support	Not supported, wildcard certificate for *.azurewebsites.net available by default	Not supported, wildcard certificate for *.azurewebsites.net available by default	Unlimited SNI SSL connections	Unlimited SNI SSL and 1 IP SSL connections included	Unlimited SNI SSL and 1 IP SSL connections included	Unlimited SNI SSL and 1 IP SSL connections included
Hybrid connections per plan			5	25	200	200
Integrated load balancer		X	X	X	X	X[10]
Always On			X	X	X	X

RESOURCE	FREE	SHARED	BASIC	STANDARD	PREMIUM (V2)	ISOLATED
Scheduled backups				Scheduled backups every 2 hours, a maximum of 12 backups per day (manual + scheduled)	Scheduled backups every hour, a maximum of 50 backups per day (manual + scheduled)	Scheduled backups every hour, a maximum of 50 backups per day (manual + scheduled)
Autoscale				X	X	X
WebJobs[11]	X	X	X	X	X	X
Endpoint monitoring			X	X	X	X
Staging slots				5	20	20
SLA			99.95%	99.95%	99.95%	99.95%

[1]Apps and storage quotas are per App Service plan unless noted otherwise.
[2]The actual number of apps that you can host on these machines depends on the activity of the apps, the size of the machine instances, and the corresponding resource utilization.
[3]Dedicated instances can be of different sizes. For more information, see App Service pricing.
[4]More are allowed upon request.
[5]The storage limit is the total content size across all apps in the same App service plan. The total content size of all apps across all App service plans in a single resource group and region cannot exceed 500GB.
[6]These resources are constrained by physical resources on the dedicated instances (the instance size and the number of instances).
[7]If you scale an app in the Basic tier to two instances, you have 350 concurrent connections for each of the two instances. For Standard tier and above, there are no theoretical limits to web sockets, but other factors can limit the number of web sockets. For example, maximum concurrent requests allowed (defined by `maxConcurrentRequestsPerCpu`) are: 7,500 per small VM, 15,000 per medium VM (7,500 x 2 cores), and 75,000 per large VM (18,750 x 4 cores).
[8]The maximum IP connections are per instance and depend on the instance size: 1,920 per B1/S1/P1V2 instance, 3,968 per B2/S2/P2V2 instance, 8,064 per B3/S3/P3V2 instance.
[9]The App Service Certificate quota limit per subscription can be increased via a support request to a maximum limit of 200.
[10]App Service Isolated SKUs can be internally load balanced (ILB) with Azure Load Balancer, so there's no public connectivity from the internet. As a result, some features of an ILB Isolated App Service must be used from machines that have direct access to the ILB network endpoint.
[11]Run custom executables and/or scripts on demand, on a schedule, or continuously as a background task within your App Service instance. Always On is required for continuous WebJobs execution. There's no predefined limit on the number of WebJobs that can run in an App Service instance. There are practical limits that depend on what the application code is trying to do.

Automation limits

Process automation

RESOURCE	MAXIMUM LIMIT	NOTES
Maximum number of new jobs that can be submitted every 30 seconds per Azure Automation account (nonscheduled jobs)	100	When this limit is reached, the subsequent requests to create a job fail. The client receives an error response.
Maximum number of concurrent running jobs at the same instance of time per Automation account (nonscheduled jobs)	200	When this limit is reached, the subsequent requests to create a job fail. The client receives an error response.
Maximum storage size of job metadata for a 30-day rolling period	10 GB (approximately 4 million jobs)	When this limit is reached, the subsequent requests to create a job fail.
Maximum job stream limit	1MB	A single stream cannot be larger than 1 MB.
Maximum number of modules that can be imported every 30 seconds per Automation account	5	
Maximum size of a module	100 MB	
Job run time, Free tier	500 minutes per subscription per calendar month	
Maximum amount of disk space allowed per sandbox[1]	1 GB	Applies to Azure sandboxes only.
Maximum amount of memory given to a sandbox[1]	400 MB	Applies to Azure sandboxes only.
Maximum number of network sockets allowed per sandbox[1]	1,000	Applies to Azure sandboxes only.
Maximum runtime allowed per runbook[1]	3 hours	Applies to Azure sandboxes only.
Maximum number of Automation accounts in a subscription	No limit	
Maximum number of Hybrid Worker Groups per Automation Account	4,000	
Maximum number of concurrent jobs that can be run on a single Hybrid Runbook Worker	50	
Maximum runbook job parameter size	512 kilobits	
Maximum runbook parameters	50	If you reach the 50-parameter limit, you can pass a JSON or XML string to a parameter and parse it with the runbook.

RESOURCE	MAXIMUM LIMIT	NOTES
Maximum webhook payload size	512 kilobits	
Maximum days that job data is retained	30 days	
Maximum PowerShell workflow state size	5 MB	Applies to PowerShell workflow runbooks when checkpointing workflow.

[1]A sandbox is a shared environment that can be used by multiple jobs. Jobs that use the same sandbox are bound by the resource limitations of the sandbox.

Change Tracking and Inventory

The following table shows the tracked item limits per machine for change tracking.

RESOURCE	LIMIT	NOTES
File	500	
Registry	250	
Windows software	250	Doesn't include software updates.
Linux packages	1,250	
Services	250	
Daemon	250	

Update Management

The following table shows the limits for Update Management.

RESOURCE	LIMIT	NOTES
Number of machines per update deployment	1000	

Azure Cache for Redis limits

RESOURCE	LIMIT
Cache size	1.2 TB
Databases	64
Maximum connected clients	40,000
Azure Cache for Redis replicas, for high availability	1
Shards in a premium cache with clustering	10

Azure Cache for Redis limits and sizes are different for each pricing tier. To see the pricing tiers and their associated sizes, see Azure Cache for Redis pricing.

For more information on Azure Cache for Redis configuration limits, see Default Redis server configuration.

Because configuration and management of Azure Cache for Redis instances is done by Microsoft, not all Redis commands are supported in Azure Cache for Redis. For more information, see Redis commands not supported in Azure Cache for Redis.

Azure Cloud Services limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Web or worker roles per deployment[1]	25	25
Instance input endpoints per deployment	25	25
Input endpoints per deployment	25	25
Internal endpoints per deployment	25	25
Hosted service certificates per deployment	199	199

[1]Each Azure Cloud Service with web or worker roles can have two deployments, one for production and one for staging. This limit refers to the number of distinct roles, that is, configuration. This limit doesn't refer to the number of instances per role, that is, scaling.

Azure Cognitive Search limits

Pricing tiers determine the capacity and limits of your search service. Tiers include:

- **Free** multi-tenant service, shared with other Azure subscribers, is intended for evaluation and small development projects.
- **Basic** provides dedicated computing resources for production workloads at a smaller scale, with up to three replicas for highly available query workloads.
- **Standard**, which includes S1, S2, S3, and S3 High Density, is for larger production workloads. Multiple levels exist within the Standard tier so that you can choose a resource configuration that best matches your workload profile.

Limits per subscription

You can create multiple services within a subscription. Each one can be provisioned at a specific tier. You're limited only by the number of services allowed at each tier. For example, you could create up to 12 services at the Basic tier and another 12 services at the S1 tier within the same subscription. For more information about tiers, see Choose an SKU or tier for Azure Cognitive Search.

Maximum service limits can be raised upon request. If you need more services within the same subscription, contact Azure Support.

RESOURCE	FREE[1]	BASIC	S1	S2	S3	S3 HD	L1	L2
Maximum services	1	16	16	8	6	6	6	6

RESOURCE	FREE	BASIC	S1	S2	S3	S3 HD	L1	L2
Maximum scale in search units (SU)[2]	N/A	3 SU	36 SU	36 SU	36 SU	36 SU	36 SU	36 SU

[1] Free is based on shared, not dedicated, resources. Scale-up is not supported on shared resources.

[2] Search units are billing units, allocated as either a *replica* or a *partition*. You need both resources for storage, indexing, and query operations. To learn more about SU computations, see Scale resource levels for query and index workloads.

Limits per search service

Storage is constrained by disk space or by a hard limit on the *maximum number* of indexes, document, or other high-level resources, whichever comes first. The following table documents storage limits. For maximum limits on indexes, documents, and other objects, see Limits by resource.

RESOURCE	FREE	BASIC[1]	S1	S2	S3	S3 HD[2]	L1	L2
Service level agreement (SLA)[3]	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Storage per partition	50 MB	2 GB	25 GB	100 GB	200 GB	200 GB	1 TB	2 TB
Partitions per service	N/A	1	12	12	12	3	12	12
Partition size	N/A	2 GB	25 GB	100 GB	200 GB	200 GB	1 TB	2 TB
Replicas	N/A	3	12	12	12	12	12	12

[1] Basic has one fixed partition. At this tier, additional search units are used for allocating more replicas for increased query workloads.

[2] S3 HD has a hard limit of three partitions, which is lower than the partition limit for S3. The lower partition limit is imposed because the index count for S3 HD is substantially higher. Given that service limits exist for both computing resources (storage and processing) and content (indexes and documents), the content limit is reached first.

[3] Service level agreements are offered for billable services on dedicated resources. Free services and preview features have no SLA. For billable services, SLAs take effect when you provision sufficient redundancy for your service. Two or more replicas are required for query (read) SLAs. Three or more replicas are required for query and indexing (read-write) SLAs. The number of partitions isn't an SLA consideration.

To learn more about limits on a more granular level, such as document size, queries per second, keys, requests, and responses, see Service limits in Azure Cognitive Search.

Azure Cognitive Services limits

The following limits are for the number of Cognitive Services resources per Azure subscription. Each of the Cognitive Services may have additional limitations, for more information see Azure Cognitive Services.

TYPE	LIMIT	EXAMPLE
A mixture of Cognitive Services resources	Maximum of 200 total Cognitive Services resources.	100 Computer Vision resources in West US 2, 50 Speech Service resources in West US, and 50 Text Analytics resources in East US.
A single type of Cognitive Services resources.	Maximum of 100 resources per region, with a maximum of 200 total Cognitive Services resources.	100 Computer Vision resources in West US 2, and 100 Computer Vision resources in East US.

Azure Cosmos DB limits

For Azure Cosmos DB limits, see Limits in Azure Cosmos DB.

Azure Data Explorer limits

The following table describes the maximum limits for Azure Data Explorer clusters.

RESOURCE	LIMIT
Clusters per region per subscription	20
Instances per cluster	1000
Number of databases in a cluster	10,000
Number of attached database configurations in a cluster	70

The following table describes the limits on management operations performed on Azure Data Explorer clusters.

SCOPE	OPERATION	LIMIT
Cluster	read (for example, get a cluster)	500 per 5 minutes
Cluster	write (for example, create a database)	1000 per hour

Azure Database for MySQL

For Azure Database for MySQL limits, see Limitations in Azure Database for MySQL.

Azure Database for PostgreSQL

For Azure Database for PostgreSQL limits, see Limitations in Azure Database for PostgreSQL.

Azure Functions limits

RESOURCE	CONSUMPTION PLAN	PREMIUM PLAN	APP SERVICE PLAN[1]
Scale out	Event driven	Event driven	Manual/autoscale

RESOURCE	CONSUMPTION PLAN	PREMIUM PLAN	APP SERVICE PLAN
Max instances	200	100	10-20
Default timeout duration (min)	5	30	30[2]
Max timeout duration (min)	10	unbounded[8]	unbounded[3]
Max outbound connections (per instance)	600 active (1200 total)	unbounded	unbounded
Max request size (MB)[4]	100	100	100
Max query string length[4]	4096	4096	4096
Max request URL length[4]	8192	8192	8192
ACU per instance	100	210-840	100-840
Max memory (GB per instance)	1.5	3.5-14	1.75-14
Function apps per plan	100	100	unbounded[5]
App Service plans	100 per region	100 per resource group	100 per resource group
Storage[6]	1 GB	250 GB	50-1000 GB
Custom domains per app	500[7]	500	500
Custom domain SSL support	unbounded SNI SSL connection included	unbounded SNI SSL and 1 IP SSL connections included	unbounded SNI SSL and 1 IP SSL connections included

[1] For specific limits for the various App Service plan options, see the App Service plan limits.
[2] By default, the timeout for the Functions 1.x runtime in an App Service plan is unbounded.
[3] Requires the App Service plan be set to Always On. Pay at standard rates.
[4] These limits are set in the host.
[5] The actual number of function apps that you can host depends on the activity of the apps, the size of the machine instances, and the corresponding resource utilization.
[6] The storage limit is the total content size in temporary storage across all apps in the same App Service plan. Consumption plan uses Azure Files for temporary storage.
[7] When your function app is hosted in a Consumption plan, only the CNAME option is supported. For function apps in a Premium plan or an App Service plan, you can map a custom domain using either a CNAME or an A record.
[8] Guaranteed for up to 60 minutes.

Azure Kubernetes Service limits

RESOURCE	DEFAULT LIMIT
Maximum clusters per subscription	100

RESOURCE	DEFAULT LIMIT
Maximum nodes per cluster with Virtual Machine Availability Sets and Basic Load Balancer SKU	100
Maximum nodes per cluster with Virtual Machine Scale Sets and Standard Load Balancer SKU	1000 (100 nodes per node pool)
Maximum pods per node: Basic networking with Kubenet	110
Maximum pods per node: Advanced networking with Azure Container Networking Interface	Azure CLI deployment: 30[1] Azure Resource Manager template: 30[1] Portal deployment: 30

[1]When you deploy an Azure Kubernetes Service (AKS) cluster with the Azure CLI or a Resource Manager template, this value is configurable up to 250 pods per node. You can't configure maximum pods per node after you've already deployed an AKS cluster, or if you deploy a cluster by using the Azure portal.

Azure Machine Learning limits

The latest values for Azure Machine Learning Compute quotas can be found in the Azure Machine Learning quota page

Azure Maps limits

The following table shows the usage limit for the Azure Maps S0 pricing tier. Usage limit depends on the pricing tier.

RESOURCE	S0 PRICING TIER LIMIT
Maximum request rate per subscription	50 requests per second

The following table shows the data size limit for Azure Maps. The Azure Maps data service is available only at the S1 pricing tier.

RESOURCE	LIMIT
Maximum size of data	50 MB

For more information on the Azure Maps pricing tiers, see Azure Maps pricing.

Azure Monitor limits

Alerts

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Metric alerts (classic)	100 active alert rules per subscription.	Call support.
Metric alerts	1000 active alert rules per subscription in Azure public, Azure China 21Vianet and Azure Government clouds.	Call support.
Activity log alerts	100 active alert rules per subscription.	Same as default.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Log alerts	512	Call support.
Action groups	2,000 action groups per subscription.	Call support.
Autoscale settings	100 per region per subscription.	Same as default.

Action groups

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Azure app push	10 Azure app actions per action group.	Call support.
Email	1,000 email actions in an action group. No more than 100 emails in an hour. Also see the rate limiting information.	Call support.
ITSM	10 ITSM actions in an action group.	Call support.
Logic app	10 logic app actions in an action group.	Call support.
Runbook	10 runbook actions in an action group.	Call support.
SMS	10 SMS actions in an action group. No more than 1 SMS message every 5 minutes. Also see the rate limiting information.	Call support.
Voice	10 voice actions in an action group. No more than 1 voice call every 5 minutes. Also see the rate limiting information.	Call support.
Webhook	10 webhook actions in an action group. Maximum number of webhook calls is 1500 per minute per subscription. Other limits are available at action-specific information.	Call support.

Log queries and language

LIMIT	DESCRIPTION
Query language	Azure Monitor uses the same Kusto query language as Azure Data Explorer. See Azure Monitor log query language differences for KQL language elements not supported in Azure Monitor.
Azure regions	Log queries can experience excessive overhead when data spans Log Analytics workspaces in multiple Azure regions. See Query limits for details.

LIMIT	DESCRIPTION
Cross resource queries	Maximum number of Application Insights resources and Log Analytics workspaces in a single query limited to 100. Cross-resource query is not supported in View Designer. Cross-resource query in log alerts is supported in the new scheduledQueryRules API. See Cross-resource query limits for details.
Query throttling	A user is limited to 200 queries per 30 seconds on any number of workspaces. This limit applies to programmatic queries or to queries initiated by visualization parts such as Azure dashboards and the Log Analytics workspace summary page.

Log Analytics workspaces

Data collection volume and retention

TIER	LIMIT PER DAY	DATA RETENTION	COMMENT
Current Per GB pricing tier (introduced April 2018)	No limit	30 - 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Free tiers (introduced April 2016)	500 MB	7 days	When your workspace reaches the 500 MB per day limit, data ingestion stops and resumes at the start of the next day. A day is based on UTC. Note that data collected by Azure Security Center is not included in this 500 MB per day limit and will continue to be collected above this limit.
Legacy Standalone Per GB tier (introduced April 2016)	No limit	30 to 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Per Node (OMS) (introduced April 2016)	No limit	30 to 730 days	Data retention beyond 31 days is available for additional charges. Learn more about Azure Monitor pricing.
Legacy Standard tier	No limit	30 days	Retention can't be adjusted
Legacy Premium tier	No limit	365 days	Retention can't be adjusted

Number of workspaces per subscription.

PRICING TIER	WORKSPACE LIMIT	COMMENTS
Free tier	10	This limit can't be increased.
All other tiers	No limit	You're limited by the number of resources within a resource group and the number of resource groups per subscription.

Azure portal

CATEGORY	LIMITS	COMMENTS
Maximum records returned by a log query	10,000	Reduce results using query scope, time range, and filters in the query.

Data Collector API

CATEGORY	LIMITS	COMMENTS
Maximum size for a single post	30 MB	Split larger volumes into multiple posts.
Maximum size for field values	32 KB	Fields longer than 32 KB are truncated.

Search API

CATEGORY	LIMITS	COMMENTS
Maximum records returned in a single query	500,000	
Maximum size of data returned	64,000,000 bytes (~61 MiB)	
Maximum query running time	10 minutes	See Timeouts for details.
Maximum request rate	200 requests per 30 seconds per AAD user or client IP address	See Rate limits for details.

General workspace limits

CATEGORY	LIMITS	COMMENTS
Maximum columns in a table	500	
Maximum characters for column name	500	
Data export	Not currently available	Use Azure Function or Logic App to aggregate and export data.

Data ingestion volume rate

Azure Monitor is a high scale data service that serves thousands of customers sending terabytes of data each month at a growing pace. The default ingestion volume rate limit for data sent from Azure resources using diagnostic settings is approximately **6 GB/min** per workspace. This is an approximate value since the actual size can vary between data types depending on the log length and its compression ratio. This limit does not apply to

data that is sent from agents or Data Collector API.

If you send data at a higher rate to a single workspace, some data is dropped, and an event is sent to the *Operation* table in your workspace every 6 hours while the threshold continues to be exceeded. If your ingestion volume continues to exceed the rate limit or you are expecting to reach it sometime soon, you can request an increase to your workspace by opening a support request.

To be notified on such an event in your workspace, create a log alert rule using the following query with alert logic base on number of results grater than zero.

```
Operation
|where OperationCategory == "Ingestion"
|where Detail startswith "The rate of data crossed the threshold"
```

> **NOTE**
> Depending on how long you've been using Log Analytics, you might have access to legacy pricing tiers. Learn more about Log Analytics legacy pricing tiers.

Application Insights

There are some limits on the number of metrics and events per application, that is, per instrumentation key. Limits depend on the pricing plan that you choose.

RESOURCE	DEFAULT LIMIT	NOTE
Total data per day	100 GB	You can reduce data by setting a cap. If you need more data, you can increase the limit in the portal, up to 1,000 GB. For capacities greater than 1,000 GB, send email to AIDataCap@microsoft.com.
Throttling	32,000 events/second	The limit is measured over a minute.
Data retention	90 days	This resource is for Search, Analytics, and Metrics Explorer.
Availability multi-step test detailed results retention	90 days	This resource provides detailed results of each step.
Maximum event size	64,000,000 bytes	
Property and metric name length	150	See type schemas.
Property value string length	8,192	See type schemas.
Trace and exception message length	32,768	See type schemas.
Availability tests count per app	100	
Profiler data retention	5 days	
Profiler data sent per day	10 GB	

For more information, see About pricing and quotas in Application Insights.

Azure Policy limits

There's a maximum count for each object type for Azure Policy. An entry of *Scope* means either the subscription or the management group.

WHERE	WHAT	MAXIMUM COUNT
Scope	Policy definitions	500
Scope	Initiative definitions	100
Tenant	Initiative definitions	1,000
Scope	Policy or initiative assignments	100
Policy definition	Parameters	20
Initiative definition	Policies	100
Initiative definition	Parameters	100
Policy or initiative assignments	Exclusions (notScopes)	400
Policy rule	Nested conditionals	512

Azure SignalR Service limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Azure SignalR Service units per instance for Free tier	1	1
Azure SignalR Service units per instance for Standard tier	100	100
Azure SignalR Service units per subscription per region for Free tier	5	5
Total Azure SignalR Service unit counts per subscription per region	150	Unlimited
Connections per unit per day for Free tier	20	20
Connections per unit per day for Standard tier	1,000	1,000
Included messages per unit per day for Free tier	20,000	20,000

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Included messages per unit per day for Standard tier	1,000,000	1,000,000

To request an update to your subscription's default limits, open a support ticket.

Backup limits

For a summary of Azure Backup support settings and limitations, see Azure Backup Support Matrices.

Batch limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Azure Batch accounts per region per subscription	1-3	50
Dedicated cores per Batch account	90-900	Contact support
Low-priority cores per Batch account	10-100	Contact support
Active jobs and job schedules per Batch account (**completed** jobs have no limit)	100-300	1,000[1]
Pools per Batch account	20-100	500[1]

> **NOTE**
> Default limits vary depending on the type of subscription you use to create a Batch account. Cores quotas shown are for Batch accounts in Batch service mode. View the quotas in your Batch account.

[1]To request an increase beyond this limit, contact Azure Support.

Classic deployment model limits

If you use classic deployment model instead of the Azure Resource Manager deployment model, the following limits apply.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
vCPUs per subscription[1]	20	10,000
Coadministrators per subscription	200	200
Storage accounts per subscription[2]	100	100
Cloud services per subscription	20	200
Local networks per subscription	10	500
DNS servers per subscription	9	100

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Reserved IPs per subscription	20	100
Affinity groups per subscription	256	256
Subscription name length (characters)	64	64

[1]Extra small instances count as one vCPU toward the vCPU limit despite using a partial CPU core.

[2]The storage account limit includes both Standard and Premium storage accounts.

Container Instances limits

RESOURCE	DEFAULT LIMIT
Standard sku container groups per region per subscription	100[1]
Dedicated sku container groups per region per subscription	0[1]
Number of containers per container group	60
Number of volumes per container group	20
Ports per IP	5
Container instance log size - running instance	4 MB
Container instance log size - stopped instance	16 KB or 1,000 lines
Container creates per hour	300[1]
Container creates per 5 minutes	100[1]
Container deletes per hour	300[1]
Container deletes per 5 minutes	100[1]

[1]To request a limit increase, create an Azure Support request.

Container Registry limits

The following table details the features and limits of the Basic, Standard, and Premium service tiers.

RESOURCE	BASIC	STANDARD	PREMIUM
Storage[1]	10 GiB	100 GiB	500 GiB
Maximum image layer size	200 GiB	200 GiB	200 GiB
ReadOps per minute[2, 3]	1,000	3,000	10,000
WriteOps per minute[2, 4]	100	500	2,000

RESOURCE	BASIC	STANDARD	PREMIUM
Download bandwidth MBps[2]	30	60	100
Upload bandwidth MBps[2]	10	20	50
Webhooks	2	10	500
Geo-replication	N/A	N/A	Supported
Content trust	N/A	N/A	Supported
Virtual network access	N/A	N/A	Preview
Repository-scoped permissions	N/A	N/A	Preview
• Tokens	N/A	N/A	20,000
• Scope maps	N/A	N/A	20,000
• Repositories per scope map	N/A	N/A	500

[1]The specified storage limits are the amount of *included* storage for each tier. You're charged an additional daily rate per GiB for image storage above these limits. For rate information, see Azure Container Registry pricing.

[2]*ReadOps*, *WriteOps*, and *Bandwidth* are minimum estimates. Azure Container Registry strives to improve performance as usage requires.

[3]A docker pull translates to multiple read operations based on the number of layers in the image, plus the manifest retrieval.

[4]A docker push translates to multiple write operations, based on the number of layers that must be pushed. A `docker push` includes *ReadOps* to retrieve a manifest for an existing image.

Content Delivery Network limits

RESOURCE	DEFAULT LIMIT
Azure Content Delivery Network profiles	25
Content Delivery Network endpoints per profile	25
Custom domains per endpoint	25

A Content Delivery Network subscription can contain one or more Content Delivery Network profiles. A Content Delivery Network profile can contain one or more Content Delivery Network endpoints. You might want to use multiple profiles to organize your Content Delivery Network endpoints by internet domain, web application, or some other criteria.

Data Factory limits

Azure Data Factory is a multitenant service that has the following default limits in place to make sure customer

subscriptions are protected from each other's workloads. To raise the limits up to the maximum for your subscription, contact support.

Version 2

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Data factories in an Azure subscription	50	Contact support.
Total number of entities, such as pipelines, data sets, triggers, linked services, and integration runtimes, within a data factory	5,000	Contact support.
Total CPU cores for Azure-SSIS Integration Runtimes under one subscription	256	Contact support.
Concurrent pipeline runs per data factory that's shared among all pipelines in the factory	10,000	Contact support.
Concurrent External activity runs per subscription per Azure Integration Runtime region External activities are managed on integration runtime but execute on linked services, including Databricks, stored procedure, HDInsights, Web, and others.	3000	Contact support.
Concurrent Pipeline activity runs per subscription per Azure Integration Runtime region Pipeline activities execute on integration runtime, including Lookup, GetMetadata, and Delete.	1000	Contact support.
Concurrent authoring operations per subscription per Azure Integration Runtime region Including test connection, browse folder list and table list, preview data.	200	Contact support.
Concurrent Data Integration Units[1] consumption per subscription per Azure Integration Runtime region	Region group 1[2]: 6000 Region group 2[2]: 3000 Region group 3[2]: 1500	Contact support.
Maximum activities per pipeline, which includes inner activities for containers	40	40
Maximum number of linked integration runtimes that can be created against a single self-hosted integration runtime	100	Contact support.
Maximum parameters per pipeline	50	50
ForEach items	100,000	100,000

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
ForEach parallelism	20	50
Maximum queued runs per pipeline	100	100
Characters per expression	8,192	8,192
Minimum tumbling window trigger interval	15 min	15 min
Maximum timeout for pipeline activity runs	7 days	7 days
Bytes per object for pipeline objects[3]	200 KB	200 KB
Bytes per object for dataset and linked service objects[3]	100 KB	2,000 KB
Data Integration Units[1] per copy activity run	256	Contact support.
Write API calls	1,200/h This limit is imposed by Azure Resource Manager, not Azure Data Factory.	Contact support.
Read API calls	12,500/h This limit is imposed by Azure Resource Manager, not Azure Data Factory.	Contact support.
Monitoring queries per minute	1,000	Contact support.
Entity CRUD operations per minute	50	Contact support.
Maximum time of data flow debug session	8 hrs	8 hrs
Concurrent number of data flows per factory	50	Contact support.
Concurrent number of data flow debug sessions per user per factory	3	3
Data Flow Azure IR TTL limit	4 hrs	Contact support.

[1] The data integration unit (DIU) is used in a cloud-to-cloud copy operation, learn more from Data integration units (version 2). For information on billing, see Azure Data Factory pricing.

[2] Azure Integration Runtime is globally available to ensure data compliance, efficiency, and reduced network egress costs.

REGION GROUP	REGIONS
Region group 1	Central US, East US, East US2, North Europe, West Europe, West US, West US 2
Region group 2	Australia East, Australia Southeast, Brazil South, Central India, Japan East, Northcentral US, Southcentral US, Southeast Asia, West Central US
Region group 3	Canada Central, East Asia, France Central, Korea Central, UK South

[3] Pipeline, data set, and linked service objects represent a logical grouping of your workload. Limits for these objects don't relate to the amount of data you can move and process with Azure Data Factory. Data Factory is designed to scale to handle petabytes of data.

Version 1

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Pipelines within a data factory	2,500	Contact support.
Data sets within a data factory	5,000	Contact support.
Concurrent slices per data set	10	10
Bytes per object for pipeline objects[1]	200 KB	200 KB
Bytes per object for data set and linked service objects[1]	100 KB	2,000 KB
Azure HDInsight on-demand cluster cores within a subscription[2]	60	Contact support.
Cloud data movement units per copy activity run[3]	32	Contact support.
Retry count for pipeline activity runs	1,000	MaxInt (32 bit)

[1] Pipeline, data set, and linked service objects represent a logical grouping of your workload. Limits for these objects don't relate to the amount of data you can move and process with Azure Data Factory. Data Factory is designed to scale to handle petabytes of data.

[2] On-demand HDInsight cores are allocated out of the subscription that contains the data factory. As a result, the previous limit is the Data Factory-enforced core limit for on-demand HDInsight cores. It's different from the core limit that's associated with your Azure subscription.

[3] The cloud data movement unit (DMU) for version 1 is used in a cloud-to-cloud copy operation, learn more from Cloud data movement units (version 1). For information on billing, see Azure Data Factory pricing.

RESOURCE	DEFAULT LOWER LIMIT	MINIMUM LIMIT
Scheduling interval	15 minutes	15 minutes
Interval between retry attempts	1 second	1 second

RESOURCE	DEFAULT LOWER LIMIT	MINIMUM LIMIT
Retry timeout value	1 second	1 second

Web service call limits

Azure Resource Manager has limits for API calls. You can make API calls at a rate within the Azure Resource Manager API limits.

Data Lake Analytics limits

Azure Data Lake Analytics makes the complex task of managing distributed infrastructure and complex code easy. It dynamically provisions resources, and you can use it to do analytics on exabytes of data. When the job completes, it winds down resources automatically. You pay only for the processing power that was used. As you increase or decrease the size of data stored or the amount of compute used, you don't have to rewrite code. To raise the default limits for your subscription, contact support.

RESOURCE	DEFAULT LIMIT	COMMENTS
Maximum number of concurrent jobs	20	
Maximum number of analytics units (AUs) per account	250	Use any combination of up to a maximum of 250 AUs across 20 jobs. To increase this limit, contact Microsoft Support.
Maximum script size for job submission	3 MB	
Maximum number of Data Lake Analytics accounts per region per subscription	5	To increase this limit, contact Microsoft Support.

Data Lake Store limits

Azure Data Lake Storage Gen1 is an enterprise-wide hyper-scale repository for big data analytic workloads. You can use Data Lake Storage Gen1 to capture data of any size, type, and ingestion speed in one single place for operational and exploratory analytics. There's no limit to the amount of data you can store in a Data Lake Storage Gen1 account.

RESOURCE	DEFAULT LIMIT	COMMENTS
Maximum number of Data Lake Storage Gen1 accounts, per subscription, per region	10	To request an increase for this limit, contact support.
Maximum number of access ACLs, per file or folder	32	This is a hard limit. Use groups to manage access with fewer entries.
Maximum number of default ACLs, per file or folder	32	This is a hard limit. Use groups to manage access with fewer entries.

Data Share limits

Azure Data Share enables organizations to simply and securely share data with their customers and partners.

RESOURCE	LIMIT
Maximum number of Data Share resources per Azure subscription	50
Maximum number of sent shares per Data Share resource	100
Maximum number of received shares per Data Share resource	100
Maximum number of invitations per sent share	100
Maximum number of share subscriptions per sent share	100
Maximum number of datasets per share	100
Maximum number of snapshot schedules per share	1

Database Migration Service Limits

Azure Database Migration Service is a fully managed service designed to enable seamless migrations from multiple database sources to Azure data platforms with minimal downtime.

RESOURCE	DEFAULT LIMIT	COMMENTS
Maximum number of services per subscription, per region	2	To request an increase for this limit, contact support.

Event Grid limits

The following limits apply to Azure Event Grid system topics and custom topics, *not* event domains.

RESOURCE	LIMIT
Custom topics per Azure subscription	100
Event subscriptions per topic	500
Publish rate for a custom topic (ingress)	5,000 events per second per topic
Publish requests	250 per second
Event size	1 MB (charged in as multiple 64-KB events)

The following limits apply to event domains only.

RESOURCE	LIMIT
Topics per event domain	100,000
Event subscriptions per topic within a domain	500
Domain scope event subscriptions	50

RESOURCE	LIMIT
Publish rate for an event domain (ingress)	5,000 events per second
Publish requests	250 per second
Event Domains per Azure Subscription	100

Event Hubs limits

The following tables provide quotas and limits specific to Azure Event Hubs. For information about Event Hubs pricing, see Event Hubs pricing.

The following limits are common across basic, standard, and dedicated tiers.

LIMIT	SCOPE	NOTES	VALUE
Number of Event Hubs namespaces per subscription	Subscription	-	100
Number of event hubs per namespace	Namespace	Subsequent requests for creation of a new event hub are rejected.	10
Number of partitions per event hub	Entity	-	32
Maximum size of an event hub name	Entity	-	50 characters
Number of non-epoch receivers per consumer group	Entity	-	5
Maximum throughput units	Namespace	Exceeding the throughput unit limit causes your data to be throttled and generates a server busy exception. To request a larger number of throughput units for a Standard tier, file a support request. Additional throughput units are available in blocks of 20 on a committed purchase basis.	20
Number of authorization rules per namespace	Namespace	Subsequent requests for authorization rule creation are rejected.	12
Number of calls to the GetRuntimeInformation method	Entity	-	50 per second
Number of virtual network (VNet) and IP Config rules	Entity	-	128

Event Hubs Basic and Standard - quotas and limits

LIMIT	SCOPE	NOTES	BASIC	STANDARD
Maximum size of Event Hubs event	Entity		256 KB	1 MB
Number of consumer groups per event hub	Entity		1	20
Number of AMQP connections per namespace	Namespace	Subsequent requests for additional connections are rejected, and an exception is received by the calling code.	100	5,000
Maximum retention period of event data	Entity		1 day	1-7 days
Apache Kafka enabled namespace	Namespace	Event Hubs namespace streams applications using Kafka protocol	No	Yes
Capture	Entity	When enabled, micro-batches on the same stream	No	Yes

Event Hubs Dedicated - quotas and limits

The Event Hubs Dedicated offering is billed at a fixed monthly price, with a minimum of 4 hours of usage. The Dedicated tier offers all the features of the Standard plan, but with enterprise scale capacity and limits for customers with demanding workloads.

FEATURE	LIMITS
Bandwidth	20 CUs
Namespaces	50 per CU
Event Hubs	1000 per namespace
Ingress events	Included
Message Size	1 MB
Partitions	2000 per CU
Consumer groups	No limit per CU, 1000 per event hub
Brokered connections	100 K included
Message Retention	90 days, 10 TB included per CU
Capture	Included

Identity Manager limits

CATEGORY	LIMIT
User-assigned managed identities	• When you create user-assigned managed identities, only alphanumeric characters (0-9, a-z, and A-Z) and the hyphen (-) are supported. For the assignment to a virtual machine or virtual machine scale set to work properly, the name is limited to 24 characters. • If you use the managed identity virtual machine extension, the supported limit is 32 user-assigned managed identities. Without the managed identity virtual machine extension, the supported limit is 512 user-assigned identities.

IoT Central limits

IoT Central limits the number of applications you can deploy in a subscription to 10. If you need to increase this limit, contact Microsoft support.

IoT Hub limits

The following table lists the limits associated with the different service tiers S1, S2, S3, and F1. For information about the cost of each *unit* in each tier, see Azure IoT Hub pricing.

RESOURCE	S1 STANDARD	S2 STANDARD	S3 STANDARD	F1 FREE
Messages/day	400,000	6,000,000	300,000,000	8,000
Maximum units	200	200	10	1

> **NOTE**
> If you anticipate using more than 200 units with an S1 or S2 tier hub or 10 units with an S3 tier hub, contact Microsoft Support.

The following table lists the limits that apply to IoT Hub resources.

RESOURCE	LIMIT
Maximum paid IoT hubs per Azure subscription	100
Maximum free IoT hubs per Azure subscription	1
Maximum number of characters in a device ID	128
Maximum number of device identities returned in a single call	1,000
IoT Hub message maximum retention for device-to-cloud messages	7 days
Maximum size of device-to-cloud message	256 KB

RESOURCE	LIMIT
Maximum size of device-to-cloud batch	AMQP and HTTP: 256 KB for the entire batch MQTT: 256 KB for each message
Maximum messages in device-to-cloud batch	500
Maximum size of cloud-to-device message	64 KB
Maximum TTL for cloud-to-device messages	2 days
Maximum delivery count for cloud-to-device messages	100
Maximum cloud-to-device queue depth per device	50
Maximum delivery count for feedback messages in response to a cloud-to-device message	100
Maximum TTL for feedback messages in response to a cloud-to-device message	2 days
Maximum size of device twin	8 KB for tags section, and 32 KB for desired and reported properties sections each
Maximum length of device twin string key	1 KB
Maximum length of device twin string value	4 KB
Maximum depth of object in device twin	10
Maximum size of direct method payload	128 KB
Job history maximum retention	30 days
Maximum concurrent jobs	10 (for S3), 5 for (S2), 1 (for S1)
Maximum additional endpoints	10 (for S1, S2, and S3)
Maximum message routing rules	100 (for S1, S2, and S3)
Maximum number of concurrently connected device streams	50 (for S1, S2, S3, and F1 only)
Maximum device stream data transfer	300 MB per day (for S1, S2, S3, and F1 only)

NOTE

If you need more than 100 paid IoT hubs in an Azure subscription, contact Microsoft Support.

> **NOTE**
> Currently, the total number of devices plus modules that can be registered to a single IoT hub is capped at 1,000,000. If you want to increase this limit, contact Microsoft Support.

IoT Hub throttles requests when the following quotas are exceeded.

THROTTLE	PER-HUB VALUE
Identity registry operations (create, retrieve, list, update, and delete), individual or bulk import/export	83.33/sec/unit (5,000/min/unit) (for S3). 1.67/sec/unit (100/min/unit) (for S1 and S2).
Device connections	6,000/sec/unit (for S3), 120/sec/unit (for S2), 12/sec/unit (for S1). Minimum of 100/sec.
Device-to-cloud sends	6,000/sec/unit (for S3), 120/sec/unit (for S2), 12/sec/unit (for S1). Minimum of 100/sec.
Cloud-to-device sends	83.33/sec/unit (5,000/min/unit) (for S3), 1.67/sec/unit (100/min/unit) (for S1 and S2).
Cloud-to-device receives	833.33/sec/unit (50,000/min/unit) (for S3), 16.67/sec/unit (1,000/min/unit) (for S1 and S2).
File upload operations	83.33 file upload initiations/sec/unit (5,000/min/unit) (for S3), 1.67 file upload initiations/sec/unit (100/min/unit) (for S1 and S2). 10,000 SAS URIs can be out for an Azure Storage account at one time. 10 SAS URIs/device can be out at one time.
Direct methods	24 MB/sec/unit (for S3), 480 KB/sec/unit (for S2), 160 KB/sec/unit (for S1). Based on 8-KB throttling meter size.
Device twin reads	500/sec/unit (for S3), Maximum of 100/sec or 10/sec/unit (for S2), 100/sec (for S1)
Device twin updates	250/sec/unit (for S3), Maximum of 50/sec or 5/sec/unit (for S2), 50/sec (for S1)
Jobs operations (create, update, list, and delete)	83.33/sec/unit (5,000/min/unit) (for S3), 1.67/sec/unit (100/min/unit) (for S2), 1.67/sec/unit (100/min/unit) (for S1).
Jobs per-device operation throughput	50/sec/unit (for S3), maximum of 10/sec or 1/sec/unit (for S2), 10/sec (for S1).
Device stream initiation rate	5 new streams/sec (for S1, S2, S3, and F1 only).

IoT Hub Device Provisioning Service limits

The following table lists the limits that apply to Azure IoT Hub Device Provisioning Service resources.

RESOURCE	LIMIT
Maximum device provisioning services per Azure subscription	10
Maximum number of enrollments	1,000,000
Maximum number of registrations	1,000,000
Maximum number of enrollment groups	100
Maximum number of CAs	25
Maximum number of linked IoT hubs	50
Maximum size of message	96 KB

NOTE

To increase the number of enrollments and registrations on your provisioning service, contact Microsoft Support.

NOTE

Increasing the maximum number of CAs is not supported.

The Device Provisioning Service throttles requests when the following quotas are exceeded.

THROTTLE	PER-UNIT VALUE
Operations	200/min/service
Device registrations	200/min/service
Device polling operation	5/10 sec/device

Key Vault limits

Key transactions (maximum transactions allowed in 10 seconds, per vault per region[1]):

KEY TYPE	HSM KEY CREATE KEY	HSM KEY ALL OTHER TRANSACTIONS	SOFTWARE KEY CREATE KEY	SOFTWARE KEY ALL OTHER TRANSACTIONS
RSA 2,048-bit	5	1,000	10	2,000
RSA 3,072-bit	5	250	10	500
RSA 4,096-bit	5	125	10	250
ECC P-256	5	1,000	10	2,000
ECC P-384	5	1,000	10	2,000

KEY TYPE	HSM KEY CREATE KEY	HSM KEY ALL OTHER TRANSACTIONS	SOFTWARE KEY CREATE KEY	SOFTWARE KEY ALL OTHER TRANSACTIONS
ECC P-521	5	1,000	10	2,000
ECC SECP256K1	5	1,000	10	2,000

NOTE

In the previous table, we see that for RSA 2,048-bit software keys, 2,000 GET transactions per 10 seconds are allowed. For RSA 2,048-bit HSM-keys, 1,000 GET transactions per 10 seconds are allowed.

The throttling thresholds are weighted, and enforcement is on their sum. For example, as shown in the previous table, when you perform GET operations on RSA HSM-keys, it's eight times more expensive to use 4,096-bit keys compared to 2,048-bit keys. That's because 1,000/125 = 8.

In a given 10-second interval, an Azure Key Vault client can do *only one* of the following operations before it encounters a `429` throttling HTTP status code:

- 2,000 RSA 2,048-bit software-key GET transactions
- 1,000 RSA 2,048-bit HSM-key GET transactions
- 125 RSA 4,096-bit HSM-key GET transactions
- 124 RSA 4,096-bit HSM-key GET transactions and 8 RSA 2,048-bit HSM-key GET transactions

Secrets, managed storage account keys, and vault transactions:

TRANSACTIONS TYPE	MAXIMUM TRANSACTIONS ALLOWED IN 10 SECONDS, PER VAULT PER REGION[1]
All transactions	2,000

For information on how to handle throttling when these limits are exceeded, see Azure Key Vault throttling guidance.

[1] A subscription-wide limit for all transaction types is five times per key vault limit. For example, HSM-other transactions per subscription are limited to 5,000 transactions in 10 seconds per subscription.

Media Services limits

NOTE

For resources that aren't fixed, open a support ticket to ask for an increase in the quotas. Don't create additional Azure Media Services accounts in an attempt to obtain higher limits.

RESOURCE	DEFAULT LIMIT
Azure Media Services accounts in a single subscription	25 (fixed)
Media reserved units per Media Services account	25 (S1) 10 (S2, S3)[1]
Jobs per Media Services account	50,000[2]
Chained tasks per job	30 (fixed)

RESOURCE	DEFAULT LIMIT
Assets per Media Services account	1,000,000
Assets per task	50
Assets per job	100
Unique locators associated with an asset at one time	5[4]
Live channels per Media Services account	5
Programs in stopped state per channel	50
Programs in running state per channel	3
Streaming endpoints that are stopped or running per Media Services account	2
Streaming units per streaming endpoint	10
Storage accounts	1,000[5] (fixed)
Policies	1,000,000[6]
File size	In some scenarios, there's a limit on the maximum file size supported for processing in Media Services.[7]

[1]If you change the type, for example, from S2 to S1, the maximum reserved unit limits are reset.

[2]This number includes queued, finished, active, and canceled jobs. It doesn't include deleted jobs. You can delete old jobs by using **IJob.Delete** or the **DELETE** HTTP request.

As of April 1, 2017, any job record in your account older than 90 days is automatically deleted, along with its associated task records. Automatic deletion occurs even if the total number of records is below the maximum quota. To archive the job and task information, use the code described in Manage assets with the Media Services .NET SDK.

[3]When you make a request to list job entities, a maximum of 1,000 jobs is returned per request. To keep track of all submitted jobs, use the top or skip queries as described in OData system query options.

[4]Locators aren't designed for managing per-user access control. To give different access rights to individual users, use digital rights management (DRM) solutions. For more information, see Protect your content with Azure Media Services.

[5]The storage accounts must be from the same Azure subscription.

[6]There's a limit of 1,000,000 policies for different Media Services policies. An example is for the Locator policy or ContentKeyAuthorizationPolicy.

> **NOTE**
> If you always use the same days and access permissions, use the same policy ID. For information and an example, see Manage assets with the Media Services .NET SDK.

[7]The maximum size supported for a single blob is currently up to 5 TB in Azure Blob Storage. Additional limits apply in Media Services based on the VM sizes that are used by the service. The size limit applies to the files that you upload and also the files that get generated as a result of Media Services processing (encoding or analyzing). If your source file is larger than 260-GB, your Job will likely fail.

The following table shows the limits on the media reserved units S1, S2, and S3. If your source file is larger than the limits defined in the table, your encoding job fails. If you encode 4K resolution sources of long duration, you're required to use S3 media reserved units to achieve the performance needed. If you have 4K content that's larger than the 260-GB limit on the S3 media reserved units, open a support ticket.

MEDIA RESERVED UNIT TYPE	MAXIMUM INPUT SIZE (GB)
S1	26
S2	60
S3	260

Mobile Services limits

TIER	FREE	BASIC	STANDARD
API calls	500,000	1.5 million per unit	15 million per unit
Active devices	500	Unlimited	Unlimited
Scale	N/A	Up to 6 units	Unlimited units
Push notifications	Azure Notification Hubs Free tier included, up to 1 million pushes	Notification Hubs Basic tier included, up to 10 million pushes	Notification Hubs Standard tier included, up to 10 million pushes
Real-time messaging/ Web Sockets	Limited	350 per mobile service	Unlimited
Offline synchronizations	Limited	Included	Included
Scheduled jobs	Limited	Included	Included
Azure SQL Database (required) Standard rates apply for additional capacity	20 MB included	20 MB included	20 MB included
CPU capacity	60 minutes per day	Unlimited	Unlimited
Outbound data transfer	165 MB per day (daily rollover)	Included	Included

For more information on limits and pricing, see Azure Mobile Services pricing.

Multi-Factor Authentication limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Maximum number of trusted IP addresses or ranges per subscription	0	50
Remember my devices, number of days	14	60
Maximum number of app passwords	0	No limit
Allow **X** attempts during MFA call	1	99
Two-way text message timeout seconds	60	600
Default one-time bypass seconds	300	1,800
Lock user account after **X** consecutive MFA denials	Not set	99
Reset account lockout counter after **X** minutes	Not set	9,999
Unlock account after **X** minutes	Not set	9,999

Networking limits

Networking limits - Azure Resource Manager The following limits apply only for networking resources managed through **Azure Resource Manager** per region per subscription. Learn how to view your current resource usage against your subscription limits.

> **NOTE**
> We recently increased all default limits to their maximum limits. If there's no maximum limit column, the resource doesn't have adjustable limits. If you had these limits increased by support in the past and don't see updated limits in the following tables, open an online customer support request at no charge

RESOURCE	DEFAULT/MAXIMUM LIMIT
Virtual networks	1,000
Subnets per virtual network	3,000
Virtual network peerings per virtual network	500
Virtual network gateways (VPN gateways) per virtual network	1
Virtual network gateways (ExpressRoute gateways) per virtual network	1
DNS servers per virtual network	20
Private IP addresses per virtual network	65,536

RESOURCE	DEFAULT/MAXIMUM LIMIT
Private IP addresses per network interface	256
Private IP addresses per virtual machine	256
Public IP addresses per network interface	256
Public IP addresses per virtual machine	256
Concurrent TCP or UDP flows per NIC of a virtual machine or role instance	500,000
Network interface cards	65,536
Network Security Groups	5,000
NSG rules per NSG	1,000
IP addresses and ranges specified for source or destination in a security group	4,000
Application security groups	3,000
Application security groups per IP configuration, per NIC	20
IP configurations per application security group	4,000
Application security groups that can be specified within all security rules of a network security group	100
User-defined route tables	200
User-defined routes per route table	400
Point-to-site root certificates per Azure VPN Gateway	20
Virtual network TAPs	100
Network interface TAP configurations per virtual network TAP	100

Public IP address limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Public IP addresses[1]	10 for Basic.	Contact support.
Static Public IP addresses[1]	10 for Basic.	Contact support.
Standard Public IP addresses[1]	10	Contact support.
Public IP Prefixes	limited by number of Standard Public IPs in a subscription	Contact support.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Public IP prefix length	/28	Contact support.

[1]Default limits for Public IP addresses vary by offer category type, such as Free Trial, Pay-As-You-Go, CSP. For example, the default for Enterprise Agreement subscriptions is 1000.

Load balancer limits

The following limits apply only for networking resources managed through Azure Resource Manager per region per subscription. Learn how to view your current resource usage against your subscription limits.

Standard Load Balancer

RESOURCE	DEFAULT/MAXIMUM LIMIT
Load balancers	1,000
Rules per resource	1,500
Rules per NIC (across all IPs on a NIC)	300
Frontend IP configurations	600
Backend pool size	1,000 IP configurations, single virtual network
High-availability ports	1 per internal frontend
Outbound rules per Load Balancer	20

Basic Load Balancer

RESOURCE	DEFAULT/MAXIMUM LIMIT
Load balancers	1,000
Rules per resource	250
Rules per NIC (across all IPs on a NIC)	300
Frontend IP configurations	200
Backend pool size	300 IP configurations, single availability set
Availability sets per Load Balancer	150

The following limits apply only for networking resources managed through the classic deployment model per subscription. Learn how to view your current resource usage against your subscription limits.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Virtual networks	100	100
Local network sites	20	50

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
DNS servers per virtual network	20	20
Private IP addresses per virtual network	4,096	4,096
Concurrent TCP or UDP flows per NIC of a virtual machine or role instance	500,000, up to 1,000,000 for two or more NICs.	500,000, up to 1,000,000 for two or more NICs.
Network Security Groups (NSGs)	200	200
NSG rules per NSG	1,000	1,000
User-defined route tables	200	200
User-defined routes per route table	400	400
Public IP addresses (dynamic)	500	500
Reserved public IP addresses	500	500
Public VIP per deployment	5	Contact support
Private VIP (internal load balancing) per deployment	1	1
Endpoint access control lists (ACLs)	50	50

ExpressRoute limits

RESOURCE	DEFAULT/MAXIMUM LIMIT
ExpressRoute circuits per subscription	10
ExpressRoute circuits per region per subscription, with Azure Resource Manager	10
Maximum number of routes advertised to Azure private peering with ExpressRoute Standard	4,000
Maximum number of routes advertised to Azure private peering with ExpressRoute Premium add-on	10,000
Maximum number of routes advertised from Azure private peering from the VNet address space for an ExpressRoute connection	200
Maximum number of routes advertised to Microsoft peering with ExpressRoute Standard	200
Maximum number of routes advertised to Microsoft peering with ExpressRoute Premium add-on	200

RESOURCE	DEFAULT/MAXIMUM LIMIT
Maximum number of ExpressRoute circuits linked to the same virtual network in the same peering location	4
Maximum number of ExpressRoute circuits linked to the same virtual network in different peering locations	4
Number of virtual network links allowed per ExpressRoute circuit	See the Number of virtual networks per ExpressRoute circuit table.

Number of virtual networks per ExpressRoute circuit

CIRCUIT SIZE	NUMBER OF VIRTUAL NETWORK LINKS FOR STANDARD	NUMBER OF VIRTUAL NETWORK LINKS WITH PREMIUM ADD-ON
50 Mbps	10	20
100 Mbps	10	25
200 Mbps	10	25
500 Mbps	10	40
1 Gbps	10	50
2 Gbps	10	60
5 Gbps	10	75
10 Gbps	10	100
40 Gbps*	10	100
100 Gbps*	10	100

**100 Gbps ExpressRoute Direct Only*

> **NOTE**
> Global Reach connections count against the limit of virtual network connections per ExpressRoute Circuit. For example, a 10 Gbps Premium Circuit would allow for 5 Global Reach connections and 95 connections to the ExpressRoute Gateways or 95 Global Reach connections and 5 connections to the ExpressRoute Gateways or any other combination up to the limit of 100 connections for the circuit.

Virtual WAN limits

RESOURCE	LIMIT
Virtual WAN hubs per region	1
Virtual WAN hubs per virtual wan	Azure regions
VPN (branch) connections per hub	1,000

RESOURCE	LIMIT
VNet connections per hub	500
Point-to-Site users per hub	10,000
Aggregate throughput per Virtual WAN VPN gateway	20 Gbps
Throughput per Virtual WAN VPN connection (2 tunnels)	2 Gbps with 1 Gbps/IPsec tunnel
Aggregate throughput per Virtual WAN ExpressRoute gateway	20 Gbps

Application Gateway limits

The following table applies to v1, v2, Standard, and WAF SKUs unless otherwise stated.

RESOURCE	DEFAULT/MAXIMUM LIMIT	NOTE
Azure Application Gateway	1,000 per subscription	
Front-end IP configurations	2	1 public and 1 private
Front-end ports	100[1]	
Back-end address pools	100[1]	
Back-end servers per pool	1,200	
HTTP listeners	100[1]	
HTTP load-balancing rules	100[1]	
Back-end HTTP settings	100[1]	
Instances per gateway	V1 SKU - 32 V2 SKU - 125	
SSL certificates	100[1]	1 per HTTP listener
Maximum SSL certificate size	V1 SKU - 10 KB V2 SKU - 16 KB	
Authentication certificates	100	
Trusted root certificates	100	
Request timeout minimum	1 second	
Request timeout maximum	24 hours	
Number of sites	100[1]	1 per HTTP listener
URL maps per listener	1	

RESOURCE	DEFAULT/MAXIMUM LIMIT	NOTE
Maximum path-based rules per URL map	100	
Redirect configurations	100[1]	
Concurrent WebSocket connections	Medium gateways 20k Large gateways 50k	
Maximum URL length	32KB	
Maximum header size for HTTP/2	4KB	
Maximum file upload size, Standard	2 GB	
Maximum file upload size WAF	V1 Medium WAF gateways, 100 MB V1 Large WAF gateways, 500 MB V2 WAF, 750 MB	
WAF body size limit, without files	128 KB	
Maximum WAF custom rules	100	
Maximum WAF exclusions	100	

[1] In case of WAF-enabled SKUs, we recommend that you limit the number of resources to 40 for optimal performance.

Network Watcher limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT	NOTE
Azure Network Watcher	1 per region	1 per region	Network Watcher is created to enable access to the service. Only one instance of Network Watcher is required per subscription per region.
Packet capture sessions	10,000 per region	10,000	Number of sessions only, not saved captures.

Private Link limits

The following limits apply to Azure private link:

RESOURCE	LIMIT
Number of private endpoints per virtual network	1000
Number of private endpoints per subscription	64000
Number of private link service per subscription	800
Number of IP Configurations on a private link service	8 (This number is for the NAT IP addresses used per PLS)

RESOURCE	LIMIT
Number of private endpoints on the same private link service	1000

Traffic Manager limits

RESOURCE	DEFAULT/MAXIMUM LIMIT
Profiles per subscription	200
Endpoints per profile	200

Azure Bastion limits

RESOURCE	DEFAULT LIMIT
Concurrent RDP connections	25*
Concurrent SSH connections	More than 50**

*May vary due to other on-going RDP sessions or other on-going SSH sessions.
**May vary if there are existing RDP connections or usage from other on-going SSH sessions.

Azure DNS limits

Public DNS zones

RESOURCE	DEFAULT LIMIT
Public DNS Zones per subscription	250 [1]
Record sets per public DNS zone	10,000 [1]
Records per record set in public DNS zone	20
Number of Alias records for a single Azure resource	20
Private DNS zones per subscription	1000
Record sets per private DNS zone	25000
Records per record set for private DNS zones	20
Virtual Network Links per private DNS zone	1000
Virtual Networks Links per private DNS zones with auto-registration enabled	100
Number of private DNS zones a virtual network can get linked to with auto-registration enabled	1
Number of private DNS zones a virtual network can get linked	1000

RESOURCE	DEFAULT LIMIT
Number of DNS queries a virtual machine can send to Azure DNS resolver, per second	500 [2]
Maximum number of DNS queries queued (pending response) per virtual machine	200 [2]

[1]If you need to increase these limits, contact Azure Support.

[2]These limits are applied to every individual virtual machine and not at the virtual network level. DNS queries exceeding these limits are dropped.

Azure Firewall limits

RESOURCE	DEFAULT LIMIT
Data throughput	30 Gbps[1]
Rules	10,000. All rule types combined.
Maximum DNAT rules	299
Minimum AzureFirewallSubnet size	/26
Port range in network and application rules	0-64,000. Work is in progress to relax this limitation.
Public IP addresses	100 maximum (Currently, SNAT ports are added only for the first five public IP addresses.)
Route table	By default, AzureFirewallSubnet has a 0.0.0.0/0 route with the NextHopType value set to **Internet**. Azure Firewall must have direct Internet connectivity. If your AzureFirewallSubnet learns a default route to your on-premises network via BGP, you must override that with a 0.0.0.0/0 UDR with the **NextHopType** value set as **Internet** to maintain direct Internet connectivity. By default, Azure Firewall doesn't support forced tunneling to an on-premises network. However, if your configuration requires forced tunneling to an on-premises network, Microsoft will support it on a case by case basis. Contact Support so that we can review your case. If accepted, we'll allow your subscription and ensure the required firewall Internet connectivity is maintained.

[1]If you need to increase these limits, contact Azure Support.

Azure Front Door Service limits

RESOURCE	DEFAULT/MAXIMUM LIMIT
Azure Front Door Service resources per subscription	100
Front-end hosts, which includes custom domains per resource	100

RESOURCE	DEFAULT/MAXIMUM LIMIT
Routing rules per resource	100
Back-end pools per resource	50
Back ends per back-end pool	100
Path patterns to match for a routing rule	25
Custom web application firewall rules per policy	10
Web application firewall policy per subscription	100
Web application firewall match conditions per custom rule	10
Web application firewall IP address ranges per match condition	600
Web application firewall string match values per match condition	10
Web application firewall string match value length	256
Web application firewall POST body parameter name length	256
Web application firewall HTTP header name length	256
Web application firewall cookie name length	256
Web application firewall HTTP request body size inspected	128 KB
Web application firewall custom response body length	2 KB

Timeout values

Client to Front Door

- Front Door has an idle TCP connection timeout of 61 seconds.

Front Door to application back-end

- If the response is a chunked response, a 200 is returned if or when the first chunk is received.
- After the HTTP request is forwarded to the back end, Front Door waits for 30 seconds for the first packet from the back end. Then it returns a 503 error to the client.
- After the first packet is received from the back end, Front Door waits for 30 seconds in an idle timeout. Then it returns a 503 error to the client.
- Front Door to the back-end TCP session timeout is 30 minutes.

Upload and download data limit

	WITH CHUNKED TRANSFER ENCODING (CTE)	WITHOUT HTTP CHUNKING
Download	There's no limit on the download size.	There's no limit on the download size.

	WITH CHUNKED TRANSFER ENCODING (CTE)	WITHOUT HTTP CHUNKING
Upload	There's no limit as long as each CTE upload is less than 2 GB.	The size can't be larger than 2 GB.

Other limits

- Maximum URL size - 8,192 bytes - Specifies maximum length of the raw URL (scheme + hostname + port + path + query string of the URL)
- Maximum Query String size - 4,096 bytes - Specifies the maximum length of the query string, in bytes.

Notification Hubs limits

TIER	FREE	BASIC	STANDARD
Included pushes	1 million	10 million	10 million
Active devices	500	200,000	10 million
Tag quota per installation or registration	60	60	60

For more information on limits and pricing, see Notification Hubs pricing.

Role-based access control limits

RESOURCE	LIMIT
Role assignments for Azure resources per Azure subscription	2,000
Role assignments for Azure resources per management group	500
Custom roles for Azure resources per tenant	5,000
Custom roles for Azure resources per tenant (specialized clouds, such as Azure Government, Azure Germany, and Azure China 21Vianet)	2,000

Service Bus limits

The following table lists quota information specific to Azure Service Bus messaging. For information about pricing and other quotas for Service Bus, see Service Bus pricing.

QUOTA NAME	SCOPE	NOTES	VALUE
Maximum number of Basic or Standard namespaces per Azure subscription	Namespace	Subsequent requests for additional Basic or Standard namespaces are rejected by the Azure portal.	100

QUOTA NAME	SCOPE	NOTES	VALUE
Maximum number of Premium namespaces per Azure subscription	Namespace	Subsequent requests for additional Premium namespaces are rejected by the portal.	100
Queue or topic size	Entity	Defined upon creation of the queue or topic. Subsequent incoming messages are rejected, and an exception is received by the calling code.	1, 2, 3, 4 GB or 5 GB. In the Premium SKU, and the Standard SKU with partitioning enabled, the maximum queue or topic size is 80 GB.
Number of concurrent connections on a namespace	Namespace	Subsequent requests for additional connections are rejected, and an exception is received by the calling code. REST operations don't count toward concurrent TCP connections.	NetMessaging: 1,000. AMQP: 5,000.
Number of concurrent receive requests on a queue, topic, or subscription entity	Entity	Subsequent receive requests are rejected, and an exception is received by the calling code. This quota applies to the combined number of concurrent receive operations across all subscriptions on a topic.	5,000
Number of topics or queues per namespace	Namespace	Subsequent requests for creation of a new topic or queue on the namespace are rejected. As a result, if configured through the Azure portal, an error message is generated. If called from the management API, an exception is received by the calling code.	10,000 for the Basic or Standard tier. The total number of topics and queues in a namespace must be less than or equal to 10,000. For the Premium tier, 1,000 per messaging unit (MU). Maximum limit is 4,000.
Number of partitioned topics or queues per namespace	Namespace	Subsequent requests for creation of a new partitioned topic or queue on the namespace are rejected. As a result, if configured through the Azure portal, an error message is generated. If called from the management API, the exception **QuotaExceededException** is received by the calling code.	Basic and Standard tiers: 100. Partitioned entities aren't supported in the Premium tier. Each partitioned queue or topic counts toward the quota of 1,000 entities per namespace.
Maximum size of any messaging entity path: queue or topic	Entity	-	260 characters.

QUOTA NAME	SCOPE	NOTES	VALUE
Maximum size of any messaging entity name: namespace, subscription, or subscription rule	Entity	-	50 characters.
Maximum size of a message ID	Entity	-	128
Maximum size of a message session ID	Entity	-	128
Message size for a queue, topic, or subscription entity	Entity	Incoming messages that exceed these quotas are rejected, and an exception is received by the calling code.	Maximum message size: 256 KB for Standard tier, 1 MB for Premium tier. Due to system overhead, this limit is less than these values. Maximum header size: 64 KB. Maximum number of header properties in property bag: **byte/int.MaxValue**. Maximum size of property in property bag: No explicit limit. Limited by maximum header size.
Message property size for a queue, topic, or subscription entity	Entity	The exception **SerializationException** is generated.	Maximum message property size for each property is 32,000. Cumulative size of all properties can't exceed 64,000. This limit applies to the entire header of the BrokeredMessage, which has both user properties and system properties, such as SequenceNumber, Label, and MessageId.
Number of subscriptions per topic	Entity	Subsequent requests for creating additional subscriptions for the topic are rejected. As a result, if configured through the portal, an error message is shown. If called from the management API, an exception is received by the calling code.	2,000 per-topic for the Standard tier.
Number of SQL filters per topic	Entity	Subsequent requests for creation of additional filters on the topic are rejected, and an exception is received by the calling code.	2,000

QUOTA NAME	SCOPE	NOTES	VALUE
Number of correlation filters per topic	Entity	Subsequent requests for creation of additional filters on the topic are rejected, and an exception is received by the calling code.	100,000
Size of SQL filters or actions	Namespace	Subsequent requests for creation of additional filters are rejected, and an exception is received by the calling code.	Maximum length of filter condition string: 1,024 (1 K). Maximum length of rule action string: 1,024 (1 K). Maximum number of expressions per rule action: 32.
Number of SharedAccessAuthorizationRule rules per namespace, queue, or topic	Entity, namespace	Subsequent requests for creation of additional rules are rejected, and an exception is received by the calling code.	Maximum number of rules per entity type: 12. Rules that are configured on a Service Bus namespace apply to all types: queues, topics.
Number of messages per transaction	Transaction	Additional incoming messages are rejected, and an exception stating "Cannot send more than 100 messages in a single transaction" is received by the calling code.	100 For both **Send()** and **SendAsync()** operations.
Number of virtual network and IP filter rules	Namespace		128

Site Recovery limits

The following limits apply to Azure Site Recovery.

LIMIT IDENTIFIER	DEFAULT LIMIT
Number of vaults per subscription	500
Number of servers per Azure vault	250
Number of protection groups per Azure vault	No limit
Number of recovery plans per Azure vault	No limit
Number of servers per protection group	No limit
Number of servers per recovery plan	50

SQL Database limits

For SQL Database limits, see SQL Database resource limits for single databases, SQL Database resource limits for elastic pools and pooled databases, and SQL Database resource limits for managed instances.

SQL Data Warehouse limits

For SQL Data Warehouse limits, see SQL Data Warehouse resource limits.

Storage limits

The following table describes default limits for Azure general-purpose v1, v2, and Blob storage accounts. The *ingress* limit refers to all data from requests that are sent to a storage account. The *egress* limit refers to all data from responses that are received from a storage account.

RESOURCE	DEFAULT LIMIT
Number of storage accounts per region per subscription, including both standard and premium accounts	250
Maximum storage account capacity	2 PiB for US and Europe, and 500 TiB for all other regions (including the UK)[1]
Maximum number of blob containers, blobs, file shares, tables, queues, entities, or messages per storage account	No limit
Maximum request rate[1] per storage account	20,000 requests per second
Maximum ingress[1] per storage account (US, Europe regions)	25 Gbps
Maximum ingress[1] per storage account (regions other than US and Europe)	5 Gbps if RA-GRS/GRS is enabled, 10 Gbps for LRS/ZRS[2]
Maximum egress for general-purpose v2 and Blob storage accounts (all regions)	50 Gbps
Maximum egress for general-purpose v1 storage accounts (US regions)	20 Gbps if RA-GRS/GRS is enabled, 30 Gbps for LRS/ZRS[2]
Maximum egress for general-purpose v1 storage accounts (non-US regions)	10 Gbps if RA-GRS/GRS is enabled, 15 Gbps for LRS/ZRS[2]
Maximum number of virtual network rules per storage account	200
Maximum number of IP address rules per storage account	200

[1]Azure Storage standard accounts support higher capacity limits and higher limits for ingress by request. To request an increase in account limits for ingress, contact Azure Support. For more information, see Announcing larger, higher scale storage accounts.

[2] If your storage account has read-access enabled with geo-redundant storage (RA-GRS) or geo-zone-redundant storage (RA-GZRS), then the egress targets for the secondary location are identical to those of the primary location. Azure Storage replication options include:

- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)

- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

> **NOTE**
> Microsoft recommends that you use a general-purpose v2 storage account for most scenarios. You can easily upgrade a general-purpose v1 or an Azure Blob storage account to a general-purpose v2 account with no downtime and without the need to copy data. For more information, see Upgrade to a general-purpose v2 storage account.

If the needs of your application exceed the scalability targets of a single storage account, you can build your application to use multiple storage accounts. You can then partition your data objects across those storage accounts. For information on volume pricing, see Azure Storage pricing.

All storage accounts run on a flat network topology and support the scalability and performance targets outlined in this article, regardless of when they were created. For more information on the Azure Storage flat network architecture and on scalability, see Microsoft Azure Storage: A Highly Available Cloud Storage Service with Strong Consistency.

For more information on limits for standard storage accounts, see Scalability targets for standard storage accounts.

Storage resource provider limits

The following limits apply only when you perform management operations by using Azure Resource Manager with Azure Storage.

RESOURCE	DEFAULT LIMIT
Storage account management operations (read)	800 per 5 minutes
Storage account management operations (write)	1200 per hour
Storage account management operations (list)	100 per 5 minutes

Azure Blob storage limits

RESOURCE	TARGET
Maximum size of single blob container	Same as maximum storage account capacity
Maximum number of blocks in a block blob or append blob	50,000 blocks
Maximum size of a block in a block blob	100 MiB
Maximum size of a block blob	50,000 X 100 MiB (approximately 4.75 TiB)
Maximum size of a block in an append blob	4 MiB
Maximum size of an append blob	50,000 x 4 MiB (approximately 195 GiB)
Maximum size of a page blob	8 TiB
Maximum number of stored access policies per blob container	5

RESOURCE	TARGET
Target request rate for a single blob	Up to 500 requests per second
Target throughput for a single page blob	Up to 60 MiB per second
Target throughput for a single block blob	Up to storage account ingress/egress limits[1]

[1] Throughput for a single blob depends on several factors, including, but not limited to: concurrency, request size, performance tier, speed of source for uploads, and destination for downloads. To take advantage of the performance enhancements of high-throughput block blobs, upload larger blobs or blocks. Specifically, call the Put Blob or Put Block operation with a blob or block size that is greater than 4 MiB for standard storage accounts. For premium block blob or for Data Lake Storage Gen2 storage accounts, use a block or blob size that is greater than 256 KiB.

Azure Files limits

For more information on Azure Files limits, see Azure Files scalability and performance targets.

RESOURCE	STANDARD FILE SHARES	PREMIUM FILE SHARES
Minimum size of a file share	No minimum; pay as you go	100 GiB; provisioned
Maximum size of a file share	100 TiB*, 5 TiB	100 TiB
Maximum size of a file in a file share	1 TiB	1 TiB
Maximum number of files in a file share	No limit	No limit
Maximum IOPS per share	10,000 IOPS*, 1,000 IOPS	100,000 IOPS
Maximum number of stored access policies per file share	5	5
Target throughput for a single file share	up to 300 MiB/sec*, Up to 60 MiB/sec ,	See premium file share ingress and egress values
Maximum egress for a single file share	See standard file share target throughput	Up to 6,204 MiB/s
Maximum ingress for a single file share	See standard file share target throughput	Up to 4,136 MiB/s
Maximum open handles per file	2,000 open handles	2,000 open handles
Maximum number of share snapshots	200 share snapshots	200 share snapshots
Maximum object (directories and files) name length	2,048 characters	2,048 characters
Maximum pathname component (in the path \A\B\C\D, each letter is a component)	255 characters	255 characters

* Available in most regions, see Regional availability for the details on available regions.

Azure File Sync limits

RESOURCE	TARGET	HARD LIMIT
Storage Sync Services per region	20 Storage Sync Services	Yes
Sync groups per Storage Sync Service	100 sync groups	Yes
Registered servers per Storage Sync Service	99 servers	Yes
Cloud endpoints per sync group	1 cloud endpoint	Yes
Server endpoints per sync group	50 server endpoints	No
Server endpoints per server	30 server endpoints	Yes
File system objects (directories and files) per sync group	100 million objects	No
Maximum number of file system objects (directories and files) in a directory	5 million objects	Yes
Maximum object (directories and files) security descriptor size	64 KiB	Yes
File size	100 GiB	No
Minimum file size for a file to be tiered	V9: Based on file system cluster size (double file system cluster size). For example, if the file system cluster size is 4kb, the minimum file size will be 8kb. V8 and older: 64 KiB	Yes

NOTE

An Azure File Sync endpoint can scale up to the size of an Azure file share. If the Azure file share size limit is reached, sync will not be able to operate.

Azure Queue storage limits

RESOURCE	TARGET
Maximum size of a single queue	500 TiB
Maximum size of a message in a queue	64 KiB
Maximum number of stored access policies per queue	5
Maximum request rate per storage account	20,000 messages per second, which assumes a 1-KiB message size
Target throughput for a single queue (1-KiB messages)	Up to 2,000 messages per second

Azure Table storage limits

RESOURCE	TARGET
Maximum size of a single table	500 TiB
Maximum size of a table entity	1 MiB
Maximum number of properties in a table entity	255, which includes three system properties: PartitionKey, RowKey, and Timestamp
Maximum total size of property values in an entity	1 MiB
Maximum total size of an individual property in an entity	Varies by property type. For more information, see **Property Types** in Understanding the Table Service Data Model.
Maximum number of stored access policies per table	5
Maximum request rate per storage account	20,000 transactions per second, which assumes a 1-KiB entity size
Target throughput for a single table partition (1 KiB-entities)	Up to 2,000 entities per second

Virtual machine disk limits

You can attach a number of data disks to an Azure virtual machine. Based on the scalability and performance targets for a VM's data disks, you can determine the number and type of disk that you need to meet your performance and capacity requirements.

> **IMPORTANT**
> For optimal performance, limit the number of highly utilized disks attached to the virtual machine to avoid possible throttling. If all attached disks aren't highly utilized at the same time, the virtual machine can support a larger number of disks.

For Azure managed disks:

The following table illustrates the default and maximum limits of the number of resources per region per subscription. There is no limit for the number of Managed Disks, snapshots and images per resource group.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Standard managed disks	50,000	50,000
Standard SSD managed disks	50,000	50,000
Premium managed disks	50,000	50,000
Standard_LRS snapshots	50,000	50,000
Standard_ZRS snapshots	50,000	50,000
Managed image	50,000	50,000

- **For Standard storage accounts:** A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not

exceed this limit.

You can roughly calculate the number of highly utilized disks supported by a single Standard storage account based on the request rate limit. For example, for a Basic tier VM, the maximum number of highly utilized disks is about 66, which is 20,000/300 IOPS per disk. The maximum number of highly utilized disks for a Standard tier VM is about 40, which is 20,000/500 IOPS per disk.

- **For Premium storage accounts:** A Premium storage account has a maximum total throughput rate of 50 Gbps. The total throughput across all of your VM disks should not exceed this limit.

For more information, see Virtual machine sizes.

Managed virtual machine disks

Standard HDD managed disks

STANDARD DISK TYPE	S4	S6	S10	S15	S20	S30	S40	S50	S60	S70	S80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 1,300	Up to 2,000	Up to 2,000
Throughput per disk	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 300 MiB/sec	Up to 500 MiB/sec	Up to 500 MiB/sec

Standard SSD managed disks

STANDARD SSD SIZES	E1*	E2*	E3*	E4	E6	E10	E15	E20	E30	E40	E50	E60	E70	E80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 120	Up to 120	Up to 120	Up to 120	Up to 240	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 2,000	Up to 4,000	Up to 6,000
Throughput per disk	Up to 25 MiB/sec	Up to 25 MiB/sec	Up to 25 MiB/sec	Up to 25 MiB/sec	Up to 50 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 400 MiB/sec	Up to 600 MiB/sec	Up to 750 MiB/sec

*Denotes a disk size that is currently in preview, for regional availability information see New disk sizes: Managed and unmanaged.

Premium SSD managed disks: Per-disk limits

PREMIUM SSD SIZES	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	120	120	120	120	240	500	1,100	2,300	5,000	7,500	7,500	16,000	18,000	20,000
Throughput per disk	25 MiB/sec	25 MiB/sec	25 MiB/sec	25 MiB/sec	50 MiB/sec	100 MiB/sec	125 MiB/sec	150 MiB/sec	200 MiB/sec	250 MiB/sec	250 MiB/sec	500 MiB/sec	750 MiB/sec	900 MiB/sec
Max burst IOPS per disk**	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500						
Max burst throughput per disk**	170 MiB/sec	170 MiB/sec	170 MiB/sec	170 MiB/sec	170 MiB/sec	170 MiB/sec	170 MiB/sec	170 MiB/sec						
Max burst duration**	30 min	30 min	30 min	30 min	30 min	30 min	30 min	30 min						
Eligible for reservation	No	No	No	No	No	No	No	No	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year

*Denotes a disk size that is currently in preview, for regional availability information see New disk sizes: Managed and unmanaged.

**Denotes a feature that is currently in preview, see Disk bursting for more information.

Premium SSD managed disks: Per-VM limits

RESOURCE	DEFAULT LIMIT
Maximum IOPS Per VM	80,000 IOPS with GS5 VM
Maximum throughput per VM	2,000 MB/s with GS5 VM

Unmanaged virtual machine disks

Standard unmanaged virtual machine disks: Per-disk limits

VM TIER	BASIC TIER VM	STANDARD TIER VM
Disk size	4,095 GB	4,095 GB
Maximum 8-KB IOPS per persistent disk	300	500
Maximum number of disks that perform the maximum IOPS	66	40

Premium unmanaged virtual machine disks: Per-account limits

RESOURCE	DEFAULT LIMIT
Total disk capacity per account	35 TB
Total snapshot capacity per account	10 TB
Maximum bandwidth per account (ingress + egress)[1]	<=50 Gbps

[1]*Ingress* refers to all data from requests that are sent to a storage account. *Egress* refers to all data from responses that are received from a storage account.

Premium unmanaged virtual machine disks: Per-disk limits

PREMIUM STORAGE DISK TYPE	P10	P20	P30	P40	P50
Disk size	128 GiB	512 GiB	1,024 GiB (1 TB)	2,048 GiB (2 TB)	4,095 GiB (4 TB)
Maximum IOPS per disk	500	2,300	5,000	7,500	7,500
Maximum throughput per disk	100 MB/sec	150 MB/sec	200 MB/sec	250 MB/sec	250 MB/sec
Maximum number of disks per storage account	280	70	35	17	8

Premium unmanaged virtual machine disks: Per-VM limits

RESOURCE	DEFAULT LIMIT
Maximum IOPS per VM	80,000 IOPS with GS5 VM
Maximum throughput per VM	2,000 MB/sec with GS5 VM

StorSimple System limits

LIMIT IDENTIFIER	LIMIT	COMMENTS
Maximum number of storage account credentials	64	
Maximum number of volume containers	64	
Maximum number of volumes	255	
Maximum number of schedules per bandwidth template	168	A schedule for every hour, every day of the week.
Maximum size of a tiered volume on physical devices	64 TB for StorSimple 8100 and StorSimple 8600	StorSimple 8100 and StorSimple 8600 are physical devices.
Maximum size of a tiered volume on virtual devices in Azure	30 TB for StorSimple 8010 64 TB for StorSimple 8020	StorSimple 8010 and StorSimple 8020 are virtual devices in Azure that use Standard storage and Premium storage, respectively.
Maximum size of a locally pinned volume on physical devices	9 TB for StorSimple 8100 24 TB for StorSimple 8600	StorSimple 8100 and StorSimple 8600 are physical devices.
Maximum number of iSCSI connections	512	
Maximum number of iSCSI connections from initiators	512	
Maximum number of access control records per device	64	
Maximum number of volumes per backup policy	24	
Maximum number of backups retained per backup policy	64	
Maximum number of schedules per backup policy	10	
Maximum number of snapshots of any type that can be retained per volume	256	This amount includes local snapshots and cloud snapshots.
Maximum number of snapshots that can be present in any device	10,000	

LIMIT IDENTIFIER	LIMIT	COMMENTS
Maximum number of volumes that can be processed in parallel for backup, restore, or clone	16	• If there are more than 16 volumes, they're processed sequentially as processing slots become available. • New backups of a cloned or a restored tiered volume can't occur until the operation is finished. For a local volume, backups are allowed after the volume is online.
Restore and clone recover time for tiered volumes	<2 minutes	• The volume is made available within 2 minutes of a restore or clone operation, regardless of the volume size. • The volume performance might initially be slower than normal as most of the data and metadata still resides in the cloud. Performance might increase as data flows from the cloud to the StorSimple device. • The total time to download metadata depends on the allocated volume size. Metadata is automatically brought into the device in the background at the rate of 5 minutes per TB of allocated volume data. This rate might be affected by Internet bandwidth to the cloud. • The restore or clone operation is complete when all the metadata is on the device. • Backup operations can't be performed until the restore or clone operation is fully complete.

LIMIT IDENTIFIER	LIMIT	COMMENTS
Restore recover time for locally pinned volumes	<2 minutes	• The volume is made available within 2 minutes of the restore operation, regardless of the volume size. • The volume performance might initially be slower than normal as most of the data and metadata still resides in the cloud. Performance might increase as data flows from the cloud to the StorSimple device. • The total time to download metadata depends on the allocated volume size. Metadata is automatically brought into the device in the background at the rate of 5 minutes per TB of allocated volume data. This rate might be affected by Internet bandwidth to the cloud. • Unlike tiered volumes, if there are locally pinned volumes, the volume data is also downloaded locally on the device. The restore operation is complete when all the volume data has been brought to the device. • The restore operations might be long and the total time to complete the restore will depend on the size of the provisioned local volume, your Internet bandwidth, and the existing data on the device. Backup operations on the locally pinned volume are allowed while the restore operation is in progress.
Thin-restore availability	Last failover	
Maximum client read/write throughput, when served from the SSD tier*	920/720 MB/sec with a single 10-gigabit Ethernet network interface	Up to two times with MPIO and two network interfaces.
Maximum client read/write throughput, when served from the HDD tier*	120/250 MB/sec	
Maximum client read/write throughput, when served from the cloud tier*	11/41 MB/sec	Read throughput depends on clients generating and maintaining sufficient I/O queue depth.

*Maximum throughput per I/O type was measured with 100 percent read and 100 percent write scenarios. Actual throughput might be lower and depends on I/O mix and network conditions.

Stream Analytics limits

LIMIT IDENTIFIER	LIMIT	COMMENTS
Maximum number of streaming units per subscription per region	500	To request an increase in streaming units for your subscription beyond 500, contact Microsoft Support.
Maximum number of inputs per job	60	There's a hard limit of 60 inputs per Azure Stream Analytics job.
Maximum number of outputs per job	60	There's a hard limit of 60 outputs per Stream Analytics job.
Maximum number of functions per job	60	There's a hard limit of 60 functions per Stream Analytics job.
Maximum number of streaming units per job	192	There's a hard limit of 192 streaming units per Stream Analytics job.
Maximum number of jobs per region	1,500	Each subscription can have up to 1,500 jobs per geographical region.
Reference data blob MB	300	Reference data blobs can't be larger than 300 MB each.

Virtual Machines limits

Virtual Machines limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Virtual machines per cloud service[1]	50	50
Input endpoints per cloud service[2]	150	150

[1]Virtual machines created by using the classic deployment model instead of Azure Resource Manager are automatically stored in a cloud service. You can add more virtual machines to that cloud service for load balancing and availability.

[2]Input endpoints allow communications to a virtual machine from outside the virtual machine's cloud service. Virtual machines in the same cloud service or virtual network can automatically communicate with each other. For more information, see How to set up endpoints to a virtual machine.

Virtual Machines limits - Azure Resource Manager

The following limits apply when you use Azure Resource Manager and Azure resource groups.

RESOURCE	DEFAULT LIMIT
VMs per subscription	25,000[1] per region.
VM total cores per subscription	20[1] per region. Contact support to increase limit.
Azure Spot VM total cores per subscription	20[1] per region. Contact support to increase limit.
VM per series, such as Dv2 and F, cores per subscription	20[1] per region. Contact support to increase limit.

RESOURCE	DEFAULT LIMIT
Availability sets per subscription	2,000 per region.
Virtual machines per availability set	200
Certificates per subscription	Unlimited[2]

[1]Default limits vary by offer category type, such as Free Trial and Pay-As-You-Go, and by series, such as Dv2, F, and G. For example, the default for Enterprise Agreement subscriptions is 350.

[2]With Azure Resource Manager, certificates are stored in the Azure Key Vault. The number of certificates is unlimited for a subscription. There's a 1-MB limit of certificates per deployment, which consists of either a single VM or an availability set.

> **NOTE**
> Virtual machine cores have a regional total limit. They also have a limit for regional per-size series, such as Dv2 and F. These limits are separately enforced. For example, consider a subscription with a US East total VM core limit of 30, an A series core limit of 30, and a D series core limit of 30. This subscription can deploy 30 A1 VMs, or 30 D1 VMs, or a combination of the two not to exceed a total of 30 cores. An example of a combination is 10 A1 VMs and 20 D1 VMs.

Shared Image Gallery limits

There are limits, per subscription, for deploying resources using Shared Image Galleries:

- 100 shared image galleries, per subscription, per region
- 1,000 image definitions, per subscription, per region
- 10,000 image versions, per subscription, per region

Virtual machine scale sets limits

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Maximum number of VMs in a scale set	1,000	1,000
Maximum number of VMs based on a custom VM image in a scale set	600	600
Maximum number of scale sets in a region	2,000	2,000

See also

- Understand Azure limits and increases
- Virtual machine and cloud service sizes for Azure
- Sizes for Azure Cloud Services
- Naming rules and restrictions for Azure resources