# Introduction to the Dell NativeEdge Software Platform

White Paper

H19628.6

**Abstract**

This white paper introduces Dell NativeEdge, as enabled through Dell Automation Platform, and describes the value proposition and architecture of the software.

**Dell Solutions**

November 2025

DELL Technologies

## Notes, cautions, and warnings

**NOTE:** A NOTE indicates important information that helps you make better use of your product.

**CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

**WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

# Contents

# 1

# Executive summary

Dell NativeEdge, an outcome of Dell Automation Platform, is an edge operations software platform that offers fleet management and application orchestration to the edge, core data centers, and cloud. With NativeEdge, customers can simplify edge operations, optimize edge investments, and secure the edge.

**Topics:**



## Overview

Dell NativeEdge, as enabled through Dell Automation Platform, offers edge operations, fleet management and application orchestration to the edge, core data centers, and cloud. With NativeEdge, customers can simplify edge operations, optimize edge investments, and secure the edge.

## Audience

This document is intended for IT administrators, Operations Technicians (OT), solution architects, partners, Dell Technologies employees, and individuals who may evaluate, acquire, manage, operate, or design an edge environment using NativeEdge.

## Terminology

**Table 1. Terminology**

| Term | Definition |
|---|---|
| Blueprint | A YAML file with definitions of resources and connections between them (based on the TOSCA specification), that is used to templatize application deployment. |
| Cluster | A group of interconnected, identical endpoints working together to improve performance, scalability, and fault tolerance in a network environment. |
| Deployments | Applications or Solutions that are deployed from blueprints downloaded from the catalog. |
| FIDO Device Onboard (FDO) | The main technology used to provide Secure Device Onboarding with FDO. For more information, see FIDO Device Onboard Specification 1.1. |
| Dell Automation Platform catalog | A curated library of validated blueprints and plugins for use across the entire platform, enabling utilities and solutions for all industries. |
| NativeEdge endpoint | A component that automates application and infrastructure workload orchestration and life cycle management across AI, edge, and private cloud environments. |
| Dell Automation Platform orchestrator | A management component built into the edge platform that provides hierarchical security, orchestration, and life cycle management of vertical solutions distributed across the edge, core, and edge local deployments. |
| Dell Automation Platform portal | The entry point for the Dell Automation Platform used for onboarding assets, identity management, and connecting to an orchestrator. |
| NativeEdge OS | A combination of a Linux-based operating system, KVM hypervisor, and an orchestrator agent that enable the devices to work with the NativeEdge platform. |

**Table 1. Terminology (continued)**

| Term | Definition |
|---|---|
| Onboarding Service | A support service for FIDO Device Onboard protocols to bind the endpoint to the Dell Automation Platform orchestrator and allow the orchestrator to provision the device. |
| Rendezvous Service | A networking service that runs inside the Dell Automation Platform orchestrator that determines how the newly powered-on NativeEdge endpoint connects to the Dell Automation Platform orchestrator. |

# We value your feedback

Dell Technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team by email.

**Author**: Jonathan Tang

**Contributor**: Jesela Cantu

**NOTE:** For links to additional documentation for this topic, see Dell Technologies Info Hub for NativeEdge Solutions.

# 2

# Business challenge

In recent years, there has been a significant shift towards the edge, with more companies deploying devices that demand increased data and analytics. Deploying devices to the edge reduces latency, improves the speed of data processing, and enhances security. It also helps reduce bandwidth consumption and minimizes the costs associated with transmitting large amounts of data to the cloud. As a result, edge deployment has become a crucial component of modern technology infrastructure, improving operational efficiency and customer experience.

However, unique challenges require a new approach to the edge. The diversity of hardware and environments makes testing, integrating, deploying, and managing hardware and associated software a critical design point. Edge application workloads must support diverse use cases, such as computer vision in manufacturing or inventory management in retail. Large-scale geo-distributed locations, like retail stores and distribution centers, elevate business-level concerns surrounding security, support, and efficient distributed systems operations. The installation of these systems must prioritize simplicity and be zero touch once plugged in and powered on. Secure operations require the ability to bring edge endpoints into an environment with zero-trust security in mind. Multiple solutions for specific use cases can lead to technology silos, creating operational challenges.

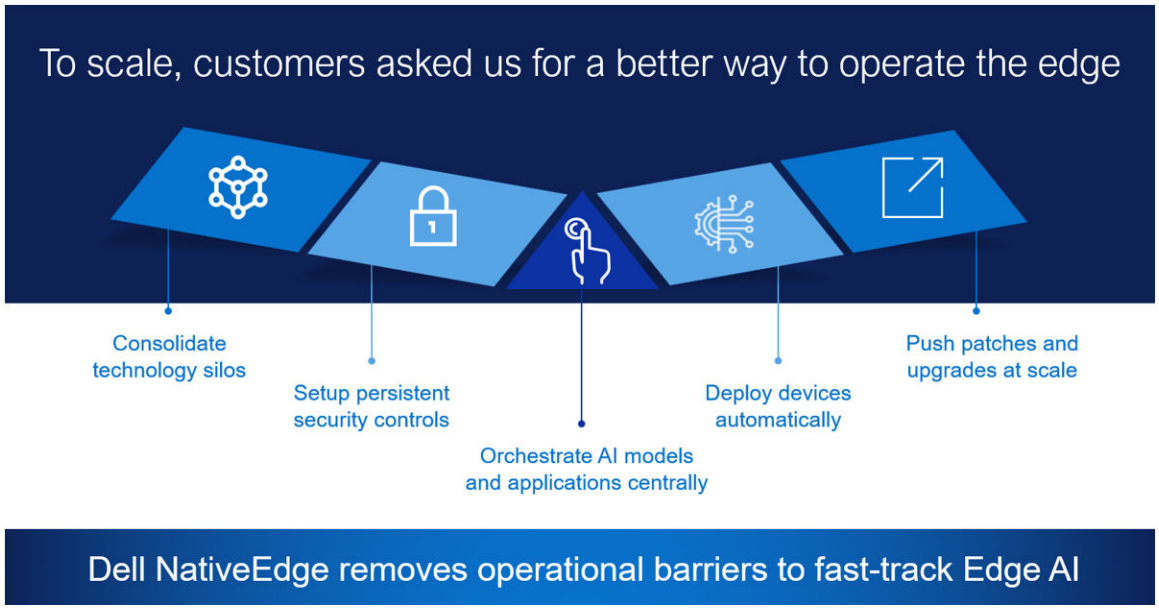


**Figure 1. Challenges at the edge**

NativeEdge addresses the complexities of modern edge operations by reimagining how edge environments are deployed and managed. As a fully automated solution, it eliminates the need for on-site skilled resources—users simply plug in and power on the device, and the rest is handled seamlessly. With built-in secure device onboarding and a zero-trust security model that spans from manufacturing through deployment to device retirement, NativeEdge ensures robust protection across the entire lifecycle. This platform empowers organizations to scale edge operations with confidence, speed, and security.

NativeEdge supports a wide range of protocols and networking configurations, accommodating unpredictable network services or isolated designs. NativeEdge also has the flexibility to start small, operating with a single device, and expand within the same location or across multiple sites. Moreover, it is designed for multicloud workloads that can be centrally monitored and managed, allowing for the deployment of applications from the edge, core, and any cloud of choice.

# 3

# About NativeEdge

NativeEdge is a solution that enables organizations to securely deploy and manage edge infrastructure, supporting various endpoints and utilizing zero-trust principles, factory integration, and application orchestration for a secure environment. It offers scalability from a single device and can be globally deployed regardless of network connectivity, technology staffing, or specific environment.

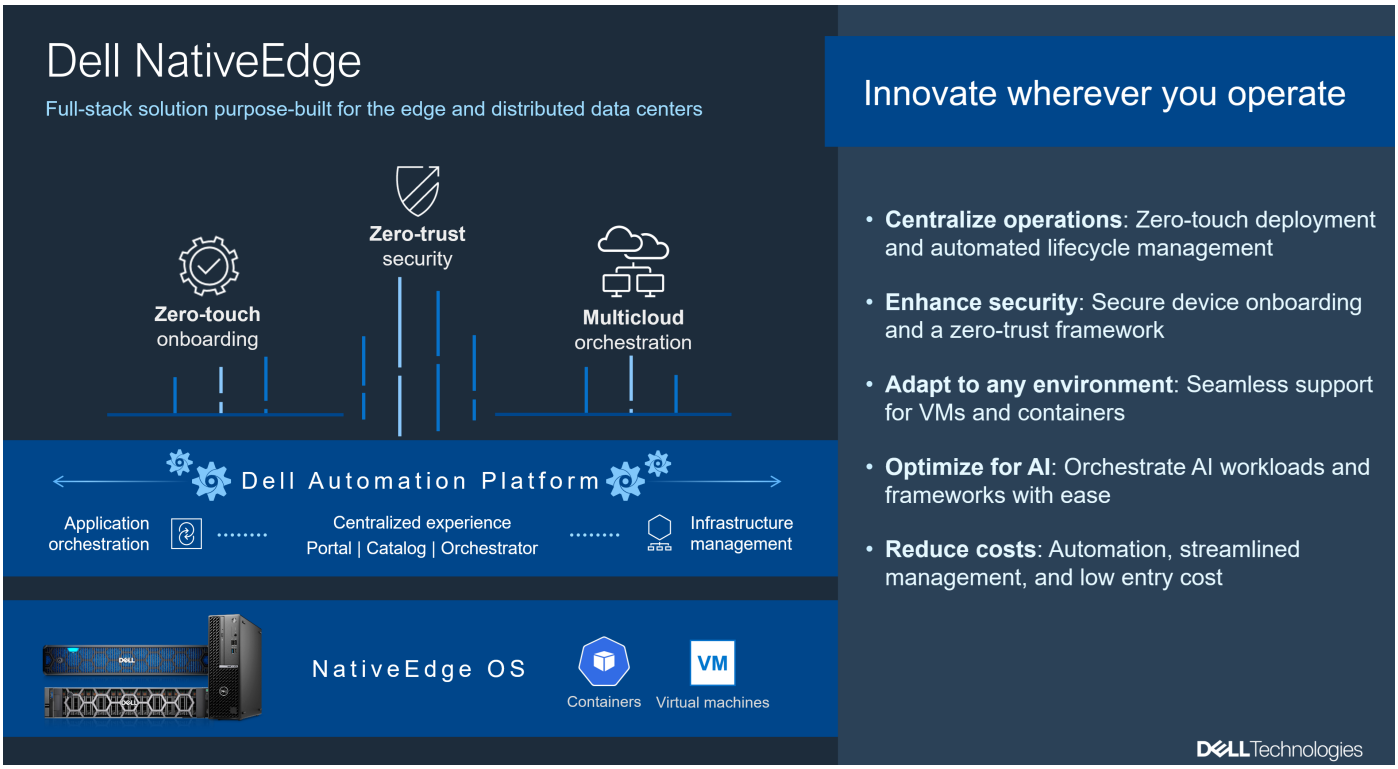


**Figure 2. Dell NativeEdge**

4

# Dell Automation Platform orchestrator

NativeEdge is a key outcome of the Dell Automation Platform, designed to extend its automation capabilities across AI, edge, and private cloud environments. Central to the platform is the orchestrator—a flexible, centralized control plane that enables application orchestration, fleet management, and lifecycle management across distributed infrastructures. It can be deployed using Helm charts on Kubernetes clusters (bare-metal or virtual machines) or as an OVA in VMware environments.

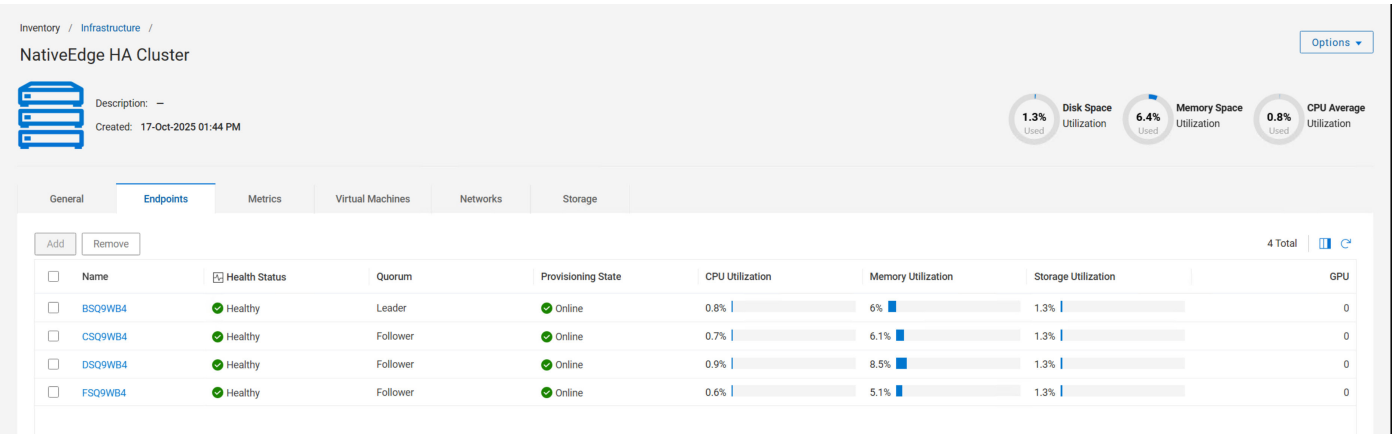


**Figure 3. The different components of NativeEdge**

NativeEdge stands out as a fully integrated solution for secure, automated edge operations. Through the orchestrator, customers can seamlessly onboard NativeEdge endpoints using secure device onboarding and zero-touch provisioning—eliminating the need for local skilled resources. This flexibility empowers organizations to tailor their edge strategies while maintaining centralized control and operational consistency.

**Topics:**



# Secure device onboarding with FDO

Traditionally, installing edge devices has been laborious and time-consuming, often involving retail store or factory managers who may lack the expertise for complex installations. This underscores the importance of making edge devices user-friendly and easy to deploy.

To address this need, NativeEdge simplifies the deployment of NativeEdge endpoints while ensuring robust security with zero-trust and zero-touch capabilities. With secure device onboarding capabilities, anyone can set up an endpoint by plugging in a network cable, powering on the device, and stepping away. Dell has partnered with Intel and the Fast Identity Online (FIDO) Alliance to streamline this process, leveraging the FIDO Device Onboarding specification 1.1.

During manufacturing, a digital record called an ownership voucher is created for each NativeEdge endpoint. This voucher, a public key based on a hash, is stored in the device's Trusted Platform Module (TPM). After Dell manufactures the devices, customers can access their ownership vouchers through Dell My Account. For example, if a customer orders 50 Dell PowerEdge servers, 50 ownership vouchers are stored in their Dell My Account. Keeping these vouchers allows customers to validate the endpoint throughout the supply chain.

# Dell Automation Platform portal

After successfully deploying the orchestrator, customers can upload vouchers from the Dell Automation Platform portal. There are two options for uploading vouchers, as shown in the following figure. The first method, referred to as "Non-Air-Gapped," involves establishing an Internet connection between the portal and Dell My Account. Through a one-time security exchange, vouchers are automatically downloaded from Dell My Account and integrated into the orchestrator.

Alternatively, for environments with firewalls or physical network separations that prevent direct access to Dell My Account, users can opt for the "Air-Gapped" method. In this approach, customers manually download the vouchers to their local laptop or workstation, then upload them to the orchestrator once they are within the confines of their secure network.

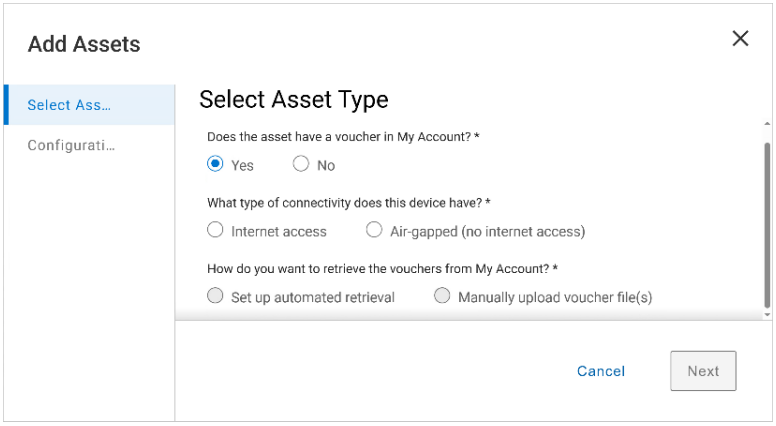


**Figure 4. Add Assets**

After uploading vouchers to the portal, an asset is automatically created and can then be assigned to an orchestrator. Once assigned, the asset is registered with an internal rendezvous service running on the orchestrator. This process completes the Transfer Ownership 0 (TO0) step as defined in the FDO Specification 1.1. To view the list of vouchers in the portal, go to **Assets**, as shown in the following figure:

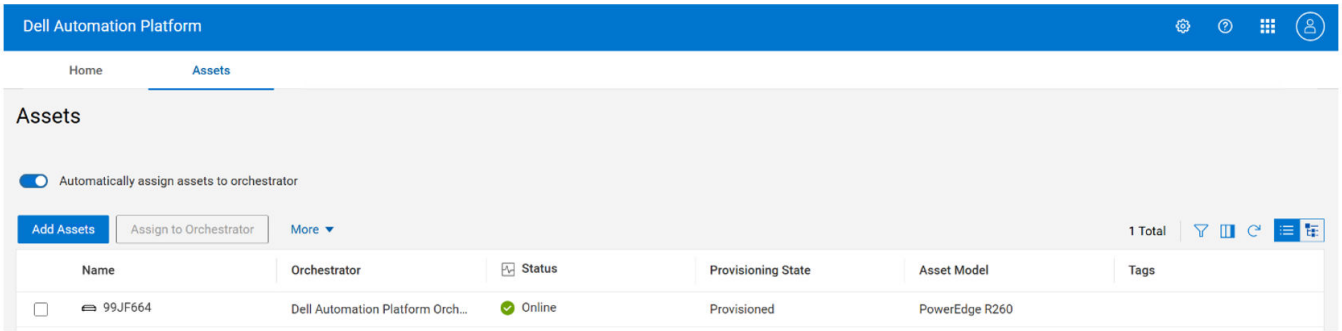


**Figure 5. Assets page**

When a customer receives the endpoint and powers it on, the endpoint automatically starts looking for the rendezvous service. It attempts to cycle through a set of preprogrammed addresses (“rv.local.edge,” “rv1.local.edge” “rv6.local.edge”) until it finds the voucher that matches the endpoint. The rendezvous service then returns information about the onboarding service within the orchestrator. When this step is completed, the Transfer Ownership (TO1) is completed as part of the FDO specification 1.1. If there is no voucher match, the device automatically attempts a reonboard after some time. Customers need to preconfigure their DNS servers and point these FQDN addresses to the IP address of their orchestrator. Customers without a DHCP or DNS server can manually configure the IP address and rendezvous service using the service console on a local VM or workstation.

**NOTE:** For more information about how to configure DNS mapping, see the *Dell Automation Platform Administration Guide* **Manuals & Documents** tab of the Dell Automation Platform Support Site.

The final onboarding step is connecting to the onboarding service, establishing secure communication between the endpoint and the orchestrator over port 443. During this step, mTLS credentials are established and stored in the TPM of the device. This is the final step known as Transfer Ownership 2 (TO2) as part of the FDO specification 1.1. The endpoint then automatically downloads, installs, and reboots into the NativeEdge OS. Users can load different versions of the NativeEdge OS by setting profiles for various device families (PowerEdge, OptiPlex, and Precision).

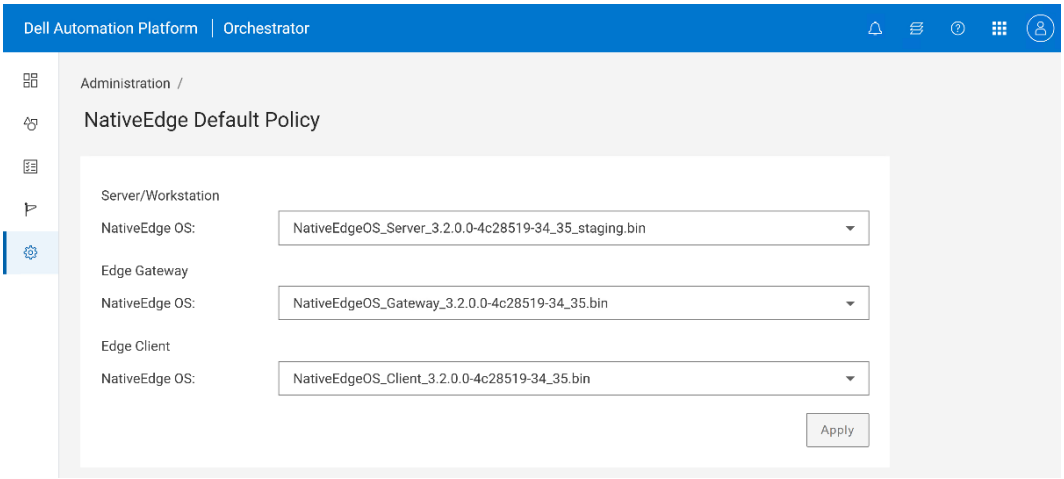


**Figure 6. NativeEdge OS onboarding Default Policy**

Users can access the global rendezvous service by going to **Administration** > **System Settings**. Here, they can enable the **Use Global Rendezvous Server** option. For backup purposes, the voucher is also registered with the local rendezvous service. Once NativeEdge endpoints have been drop-shipped to edge locations, during initial boot-up, the devices attempt to be onboarded to a global rendezvous service using the web address "rv.dell.com." If the global onboarding service fails, the onboarding process reverts to local rules. It continues to retry both global and local methods until successful onboarding.

# Fleet management

Dell NativeEdge is a comprehensive solution that enables fleet management for customers of all sizes. Using a centralized platform, customers can start with a few edge endpoints and expand as their business grows. Once NativeEdge endpoints are added, administrators can manage inventory, configure settings, monitor alarms and events, service and troubleshoot devices, and handle lifecycle tasks like OS upgrades and firmware updates. For more information about how to manage a NativeEdge endpoint, see the *Dell NativeEdge Administration Guide* on the **Manuals & Documents** tab of the NativeEdge Support Site.

# External connection

Dell Automation Platform orchestrator facilitates management of NativeEdge, VMware, and Kubernetes environments, streamlining operations and enhancing infrastructure efficiency. The orchestrator integrates with VMware and Kubernetes clusters, allowing administrators to import detailed information such as hosts and virtual machines, monitor host metrics like CPU and memory utilization, and manage VMs by starting, stopping, or rebooting them. To deploy new VMs in a VMware environment, users can select a solution blueprint with a vSphere deployment target.

For environments looking to migrate workloads, NativeEdge supports automated VM import from VMware through integration with vCenter Server. The orchestrator can automatically discover all VMs within the vCenter environment, enabling users to select multiple VMs for import, specify the target NativeEdge endpoint, choose a datastore, and assign a virtual network segment. This streamlined process facilitates efficient migration with minimal manual intervention. Once imported, VMs can be centrally managed and integrated into solution blueprints, supporting consistent policy enforcement and optimized resource utilization across hybrid environments.

# REST API

The REST API is an application programming interface that uses common HTTP operations like GET, PATCH, POST, and DELETE. It follows specific architectural constraints, ensuring consistent principles across different REST implementations, simplifying application development for developers. REST APIs are popular in data centers for standardizing management across appliances, regardless of vendor.

The orchestrator supports REST API, providing an additional method to manage NativeEdge and automate various tasks. The REST API offers the same functionalities as the orchestrator and uses JSON notation for communications. Users can employ scripting languages like Perl and PHP to send REST API requests and manage NativeEdge, allowing for flexible management and more complex scripted operations.

For more information about the Dell Automation Platform REST API, see the Dell Technologies Developer site.

# 5

# NativeEdge endpoints

NativeEdge offers a wide range of supported models, with form factors ranging from OptiPlex towers, Precision tower workstations, and PowerEdge servers.

After the user powers on the device at their site, the Dell NativeEdge OS is automatically installed on each endpoint device. This OS acts as a Linux-based KVM hypervisor, enabling support for VM and container based applications. The NativeEdge endpoint also has a secure and encrypted communication channel to the orchestrator using SSL or TLS protocols over HTTPS.

NativeEdge also offers comprehensive support for hardware upgrades such as adding additional network cards, additional storage devices, memory, CPU, and other components. These upgrades are limited to products sourced from Dell and approved for compatibility.

**Table 2. NativeEdge supported endpoints**

| Dell Edge Gateway | OptiPlex | Precision | PowerEdge |
|---|---|---|---|
| EGW-3200<br>EGW-5200 | XE4 Small Form Factor | 7960R<br>7960XL R<br>7960T<br>5860T | XR4510c<br>XR4520c<br>XR5610<br>XR7620<br>XR8610t<br>XR8620t<br>R260<br>R360<br>R660<br>R660xs<br>R760xa<br>R760xs<br>R770<br>T160<br>T360<br>T560 |

## Topics:

# Secure boot

Edge devices face security risks due to their deployment in remote and less secure locations, making them vulnerable to physical tampering. During shipment, devices may encounter multiple parties, including potential malicious actors. To mitigate these risks, Dell secures and locks down every shipment of NativeEdge endpoints from the manufacturing plant through the following steps:

- Secure Boot enabled in BIOS—Only Dell NativeEdge images, such as Factory OS, NativeEdge OS, and factory reset images, can boot successfully.
- BIOS password protection and lockout
- Boot order lockdown
- Secure Component Validation (for PowerEdge models)
- iDRAC disabled during onboarding (for PowerEdge models)
- Single network port available during onboarding

# Factory OS

The Factory OS is a lightweight, immutable operating system installed on the NativeEdge endpoint during manufacturing. It serves as a staging OS and is not intended for end-user use. Each boot-up of the Factory OS is identical, as it cannot be modified.

Designed with high security, the Factory OS provides no console access. For troubleshooting, users can use a Service Console loaded onto a laptop or workstation to set IPs, DNS addresses, and collect logs. For more details, see the *Dell NativeEdge Administration Guide* on the **Manuals & Documents** tab of the NativeEdge Support Site.

Upon boot-up, the Factory OS runs the following services:

- Service Console Listener
- Secure Component Validation (for PowerEdge models)
- FIDO Device Onboard Client
- Automated download and installation of the NativeEdge OS

# NativeEdge OS

The NativeEdge OS, installed automatically on the NativeEdge endpoint after onboarding, is based on an open-source Linux operating system. It supports virtual machines, containers, and solution blueprints for edge applications. Like the Factory OS, it is fully immutable. With this OS, all network ports, including iDRAC for PowerEdge models, are enabled, but the service console is disabled.

# Datastores

Datastores are a logical construct within NativeEdge that allow customers to store applications deployed on a NativeEdge endpoint. Datastores are encrypted using hardware-based encryption if self-encrypting drives (SEDs) are available; otherwise, software encryption is used. The NativeEdge OS automatically creates datastores, ensuring optimal performance and high availability to protect applications if there is disk loss.

If there is no RAID storage controller, the system creates datastores based on factors such as the drive protocol (NVMe or SCSI), speed (for example, 7200 RPM or 5400 RPM), and size (for example, 2 TB or 1 TB). To view datastores, select a name on **Inventory** > **Infrastructure**, go to **Hardware** > **Storage**, and select **Volumes/Datastores**.

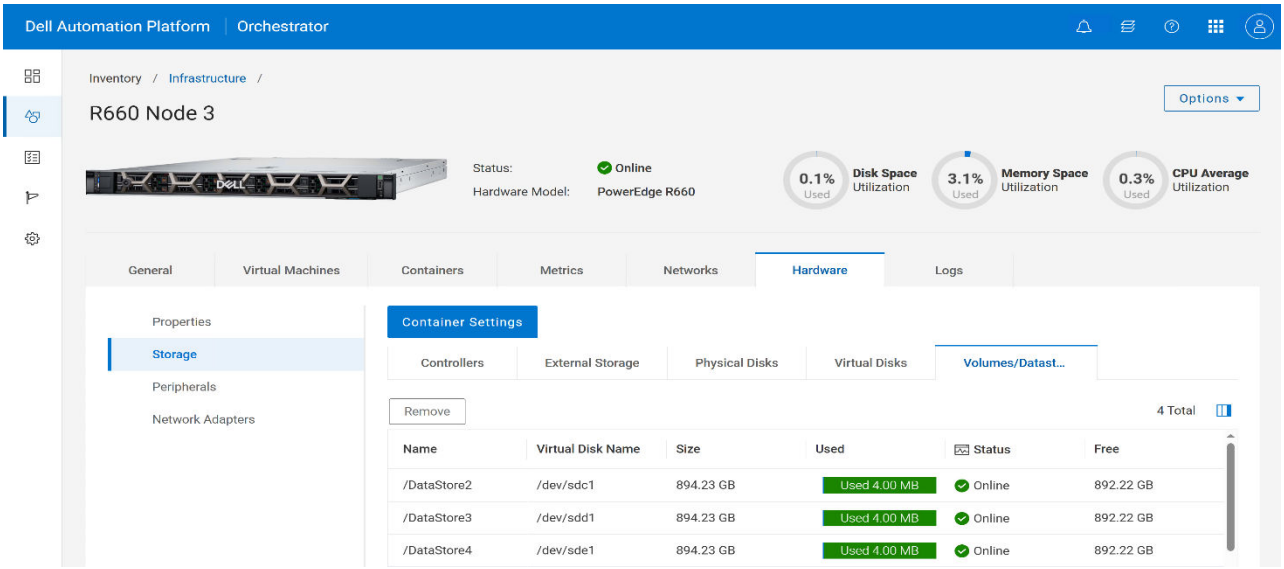


**Figure 7. Datastores**

# Networks

NativeEdge supports two types of networks: host networks and virtual network segments. Host networks manage communication between the NativeEdge endpoint and the Dell Automation Platform orchestrator. Users can create, modify, and delete host networks, except for the default network that is automatically created by the system. Host networks can also be used by customer application VMs when deploying applications with the NAT virtual network segment type and port forwarding enabled.

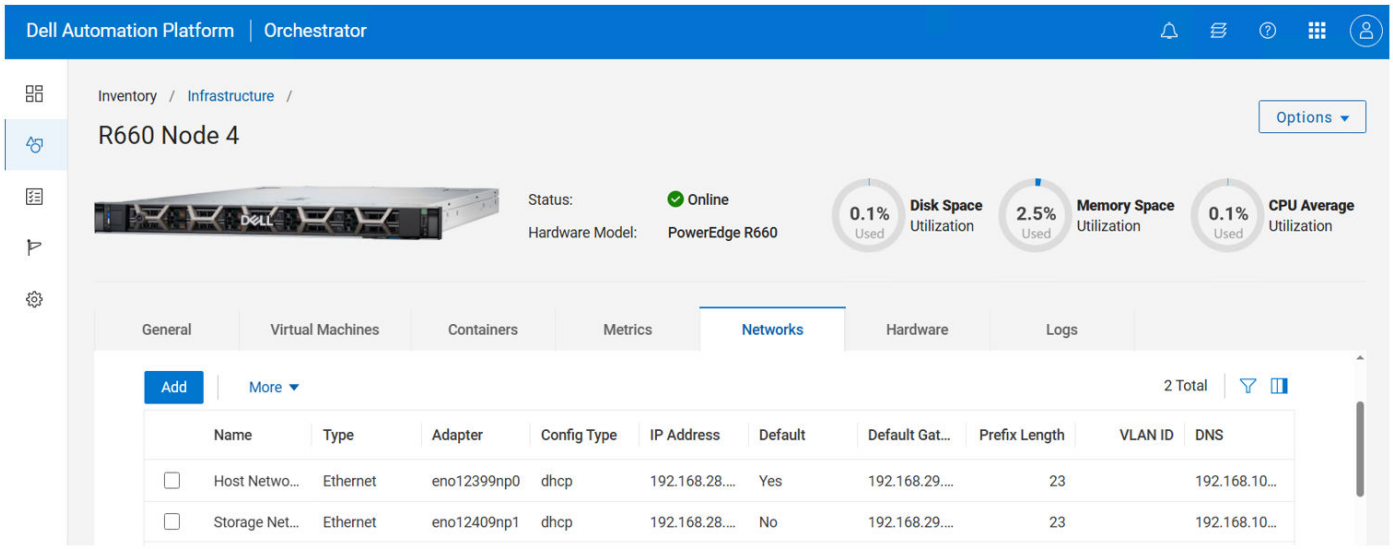


**Figure 8. Host networks**

Customers can also create virtual network segments for their applications, with NativeEdge supporting multiple segments on a single Ethernet port. There are three types of virtual network segments:

- Network Address Translation (NAT)
- Air-gapped (no Internet connection)
- Bridged

NAT virtual network segments have their own DHCP, DNS, and IP management scheme. By default, they do not have any visibility outside this network unless source NAT and port forwarding rules are set up, allowing VMs to connect to external devices through the host network.

Air-gapped virtual network segments are similar to NAT segments, providing their own DHCP, DNS, and IP management, but lacking external network connectivity. This scenario is useful for testing or development where isolated VMs must interact.

Bridged virtual network segments integrate with the customer's existing network environment. For example, if a VM needs access to an existing DHCP and DNS server, it can be assigned to a bridged network. Bridged networks also support VLANs in both access and trunk mode configurations.

# Brownfield devices

Many organizations today find themselves with a growing inventory of existing hardware—devices that were once cutting-edge but now sit underutilized or disconnected from modern IT strategies. These brownfield assets often represent significant capital investments, yet customers are unsure how to integrate them into newer, cloud-native or edge-native architectures. The challenge lies in bridging the gap between legacy infrastructure and the agility of modern edge computing.

NativeEdge addresses this challenge head-on by enabling customers to extend the value of their existing hardware. Through its support for non-NativeEdge and third-party devices, NativeEdge empowers organizations to bring these assets into the fold of a unified edge operations strategy. The only prerequisite is that these devices must be running Ubuntu 22.04, a widely adopted and stable Linux distribution.

Once Ubuntu 22.04 is in place, NativeEdge can generate a Hardware Enablement Kit (HEK) for each device. The HEK collects detailed hardware metadata—including manufacturer, model, serial number, CPU specifications, storage drives, and more—allowing the orchestrator to accurately discover and manage the device.

With the device now visible to the orchestrator, customers can deploy applications and monitor performance just as they would with native NativeEdge hardware. This seamless integration not only protects prior investments, but also accelerates time-to-value by eliminating the need for rip-and-replace strategies. For more information about how to configure brownfield devices, see the *Dell NativeEdge Administration Guide* on the **Manuals & Documents** tab of the NativeEdge Support Site.

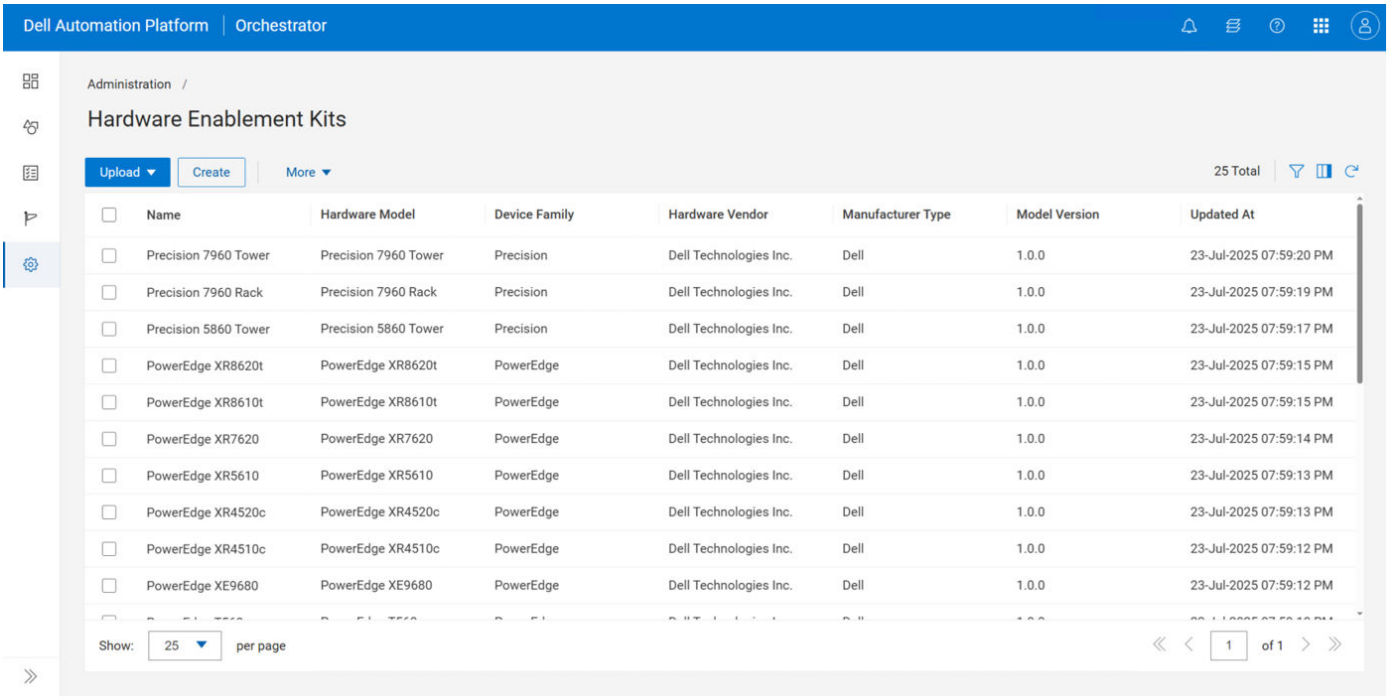


**Figure 9. Hardware enablement kits**

# 6

# Clustering NativeEdge endpoints

Clustering NativeEdge endpoints is designed to deliver robust fault tolerance and high availability, making it ideal for supporting demanding edge workloads. By distributing applications across multiple endpoints, the cluster ensures continuous operation even in the event of hardware failures. If one node goes offline, others in the cluster automatically take over, minimizing service disruption. This architecture not only enhances operational resilience, but also allows organizations to scale their deployments as needed, ensuring consistent performance and reliability in dynamic edge environments.

To establish a NativeEdge cluster, several key requirements must be met. Clusters must include three to four endpoints of the same model to ensure compatibility and consistent performance. All endpoints should be connected to the same Host Network, with cluster communication and VM traffic that is ideally separated across different physical ports. Additionally, shared datastores are required to create a unified storage pool, enabling synchronized access to data and supporting high availability.

NativeEdge clustering also incorporates a quorum system to maintain stability and prevent split-brain scenarios. One endpoint is designated as the leader, coordinating the cluster and making critical decisions, while the others act as followers. Shared storage further enhances resilience by pooling local datastores and maintaining redundant copies of data across endpoints, ensuring business continuity even during node failures.

Advanced migration capabilities—such as live, offline, autoload-balancing, and failover migration—allow VMs to move between nodes with minimal or no disruption. High availability groups provide administrators with fine-grained control over VM placement, ensuring workloads run on the most suitable endpoints and automatically shift to prioritized alternatives when needed. These features collectively deliver a robust, flexible, and scalable edge infrastructure.

For detailed guidance on setup, configuration, and best practices, see the Best Practices for Virtualization and Clustering of NativeEdge Endpoints White Paper.

# 7

# Data protection

**Topics:**

- VM snapshots
- Backups

## VM snapshots

In today's digital landscape, data protection and snapshots are crucial for ensuring the security, integrity, and availability of information. Data protection strategies, such as encryption and firewalls, safeguard sensitive data from breaches and cyber threats, ensuring compliance with regulations and maintaining stakeholder trust. VM snapshots capture the state of a VM at a specific point in time, enabling quick recovery from errors and facilitating agile development processes. Together, these measures support both regulatory compliance and technological innovation in an increasingly complex and interconnected world.

NativeEdge supports VM snapshots using copy-on-write technology, which copies original data to a separate area before any changes are made, ensuring that the original data remains intact and unaltered. This approach conserves storage space by only saving changes rather than duplicating entire datasets, allowing for quick and reliable recovery of VMs to their previous states if there are errors or failures. Additionally, managing snapshots through the orchestrator enables users to create, revert, and delete VM snapshots with ease. This provides a comprehensive and user-friendly solution for maintaining data integrity, enhancing the overall efficiency of virtual environments. For more information about using VM snapshots, see the *Dell NativeEdge Administration Guide* on the **Manuals & Documents** tab of the NativeEdge Support Site.

The following image displays a list of snapshots in a VM:

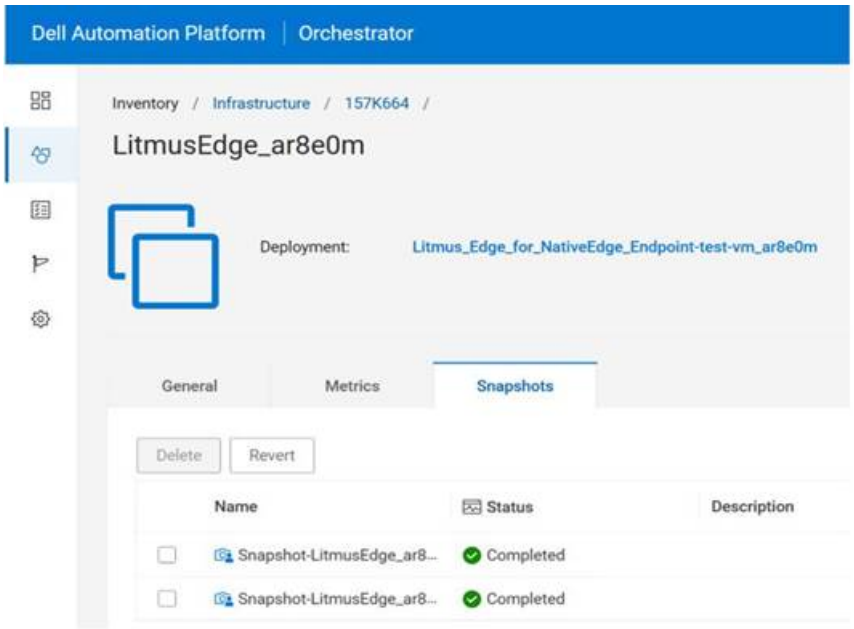


**Figure 10. A list of snapshots in a VM**

## Backups

In addition to snapshots, NativeEdge provides robust support for VM backups using APIs, enabling organizations to implement reliable and automated data protection workflows. These backups are crash-consistent, meaning they capture the state of a VM's storage device at a specific moment without requiring the VM to be shut down. This ensures that data is preserved even in the event of unexpected failures, while minimizing disruption to running workloads.

NativeEdge supports both full and incremental backups, allowing users to optimize storage usage and backup performance. Full backups capture the entire contents of a VM's storage, while incremental backups only record changes made since the last backup. This tiered approach enables efficient data protection strategies that balance speed, storage, and recovery needs.

Restoration of VMs from backups is also supported using API, providing flexibility and control for administrators to recover systems quickly and reliably. Whether restoring a full VM or applying incremental changes, NativeEdge ensures that recovery operations are streamlined and consistent with enterprise-grade reliability. These capabilities make NativeEdge a powerful platform for maintaining business continuity and resilience in virtualized environments.

For more information about how to use VM backups, see the Dell Automation Platform REST API, see the Dell Technologies Developer site.

# 8

# NativeEdge catalog

Deploying applications at the edge can be challenging for OT personnel, such as retail store managers or factory plant managers, who may lack the skills to configure complex application solutions. In addition, these users may be unaware of lifecycle management and patch applications that may be vulnerable to security risks.

NativeEdge offers a catalog that enables customers to download blueprints to the orchestrator and centrally manage applications for their entire edge environment. An application could be a virtual machine, container, or solution blueprint that is deployed to a NativeEdge endpoint after the installation of the NativeEdge OS.

**Topics:**



## Blueprints

A blueprint is a YAML-based configuration file that automates the provisioning, configuring, deploying, and validating of your edge solution. This saves time, effort, and resources. It also ensures consistency and compliance across the edge estate. With blueprints, users define application settings, infrastructure resources, network configurations, workflows, and scripts in a single file. Developers or IT operators can help develop blueprints to help simplify edge solutions across multiple locations. For more information about developing NativeEdge Blueprints, see the *Dell Automation Platform Blueprint Quick Start Guide* on the **Manuals & Documents** tab of the Dell Automation Platform Support Site.

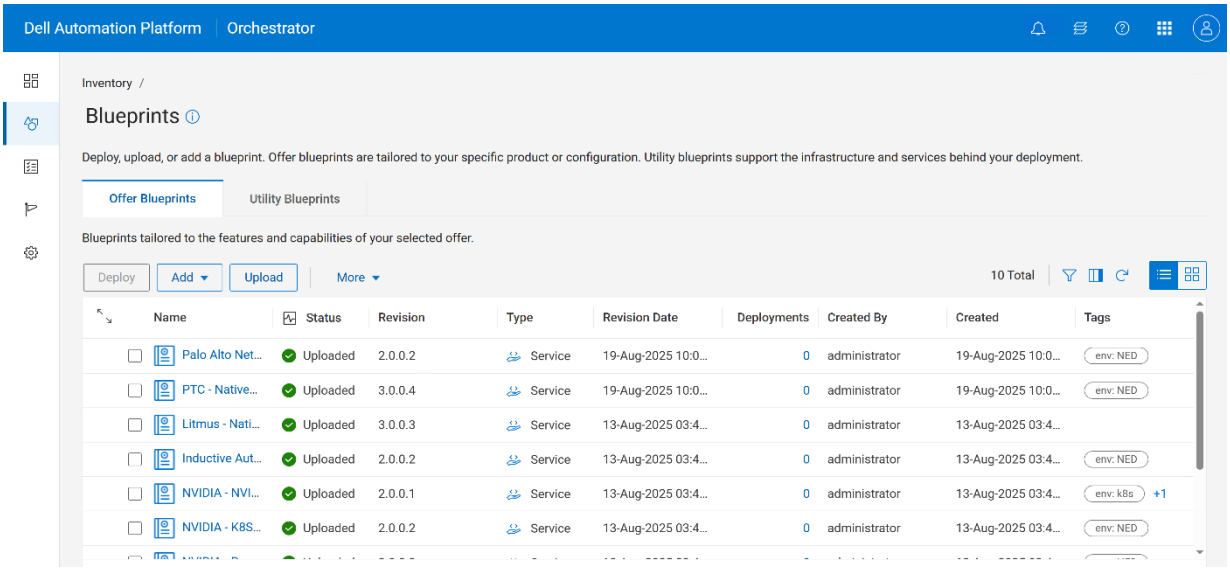


**Figure 11. Blueprints**

To help users get started, NativeEdge provides a wide range of different solutions that include common retail, manufacturing, energy, and smart city solutions. These blueprints have already been uploaded to the Dell Automation Platform catalog.

## Virtual machines

NativeEdge allows customers to centrally manage virtual machine images across their entire edge environment, supporting formats like raw, ISO, qcow2, VDI, VHD, and VMDK. Customers can upload images in two ways:

- **Local Upload**—Supports images up to 50 GB from an image stored on a local workstation.
- **External Upload**—For images larger than 50 GB, use an HTTP repository.

**NOTE:** The orchestrator automatically creates a VM blueprint for a virtual machine image that is uploaded to the orchestrator.

When adding virtual machine images, users can set certain compute constraints based on CPU, memory, and storage requirements of the application. Setting these limits allows users to have a filtered list of eligible NativeEdge endpoints to be shown at the time of deployment. Users can also set virtual network interfaces and select passthrough devices such as serial, USB, GPU, and video.

In certain scenarios, custom configurations may be necessary during the initial boot-up of applications on NativeEdge. NativeEdge offers the capability of passing custom parameters such as strings, numeric, or passwords as optional keys or value pairs that are available to the virtual machine upon first boot. Scripts and utilities running inside the virtual machine can then use these variables for customization. For example, an application may accept a STORE_LOCATION environment variable to set up configuration for a specific store.

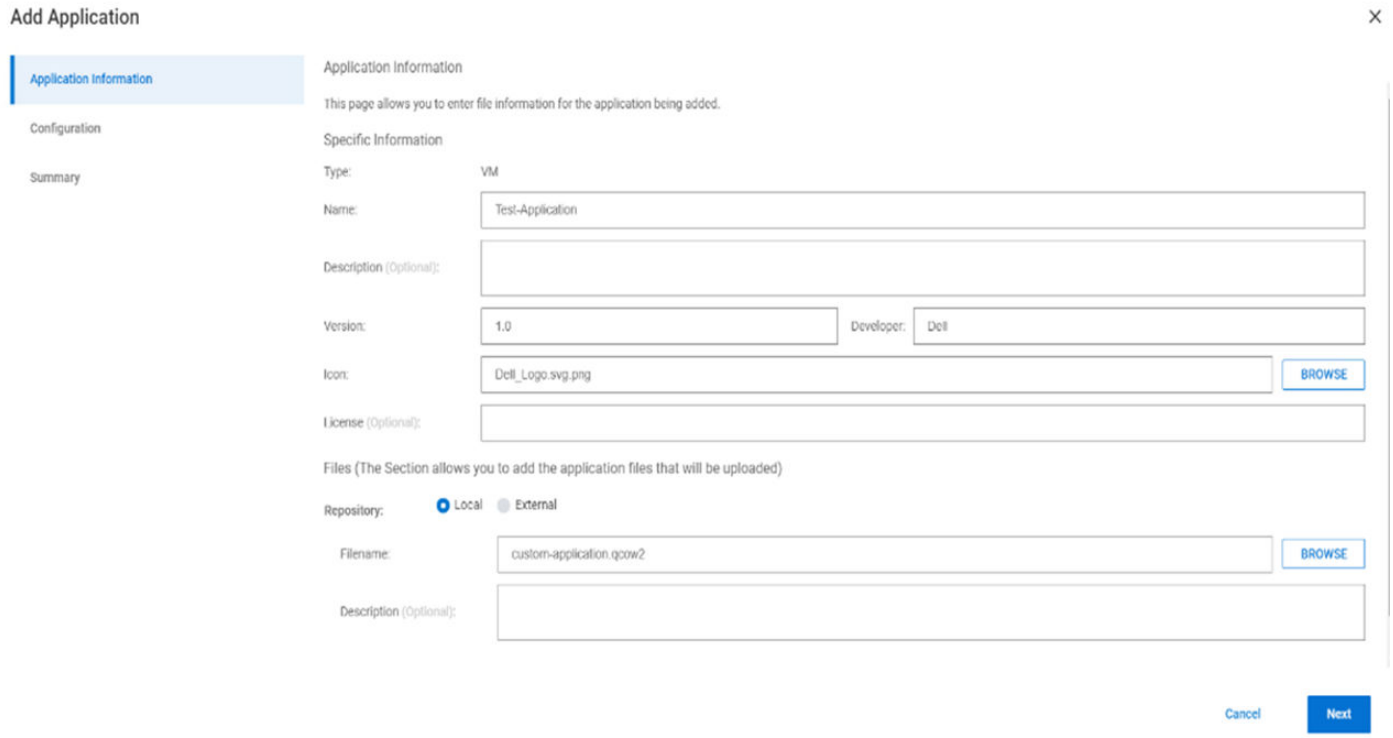


**Figure 12. Add Application**

# Containers

NativeEdge supports deploying bare-metal containers onto endpoints using a blueprint that references a customer-supplied docker-compose file. Upon deployment, NativeEdge automatically generates a NAT-type Virtual Network Segment, facilitating communication among containers within their designated network. If the docker-compose file requires persistent volumes, NativeEdge creates them and makes them accessible by going to the **Inventory** > **Infrastructure** page, clicking on an endpoint, and then and clicking: **Hardware** > **Storage** > **Volumes/Datastores**.

# Deploying blueprints

To deploy blueprints, users start on the **Inventory** > **Blueprints** page, select the checkmark next to the blueprint and click the **Deploy** button. The Deployment Targets tab prompts the administrator to select the endpoints on which to deploy the blueprint. Users can select a 1:1 deployment or one to many deployments. Next, the **Configuration** tab lists the required inputs, which can be modified.

In some situations, a blueprint requires secrets. NativeEdge provides a secret management system that helps store sensitive information such as passwords, SSH key pairs, certificates, or binary images. Secrets can be created on the **Administration** >

**Security** > **Secrets** tab or on the **Configuration** during blueprint deployment. Secrets play a crucial role in modern software development and deployment. NativeEdge provides a centralized storage for sensitive information, ensuring compliance and integrating with DevOps practices.

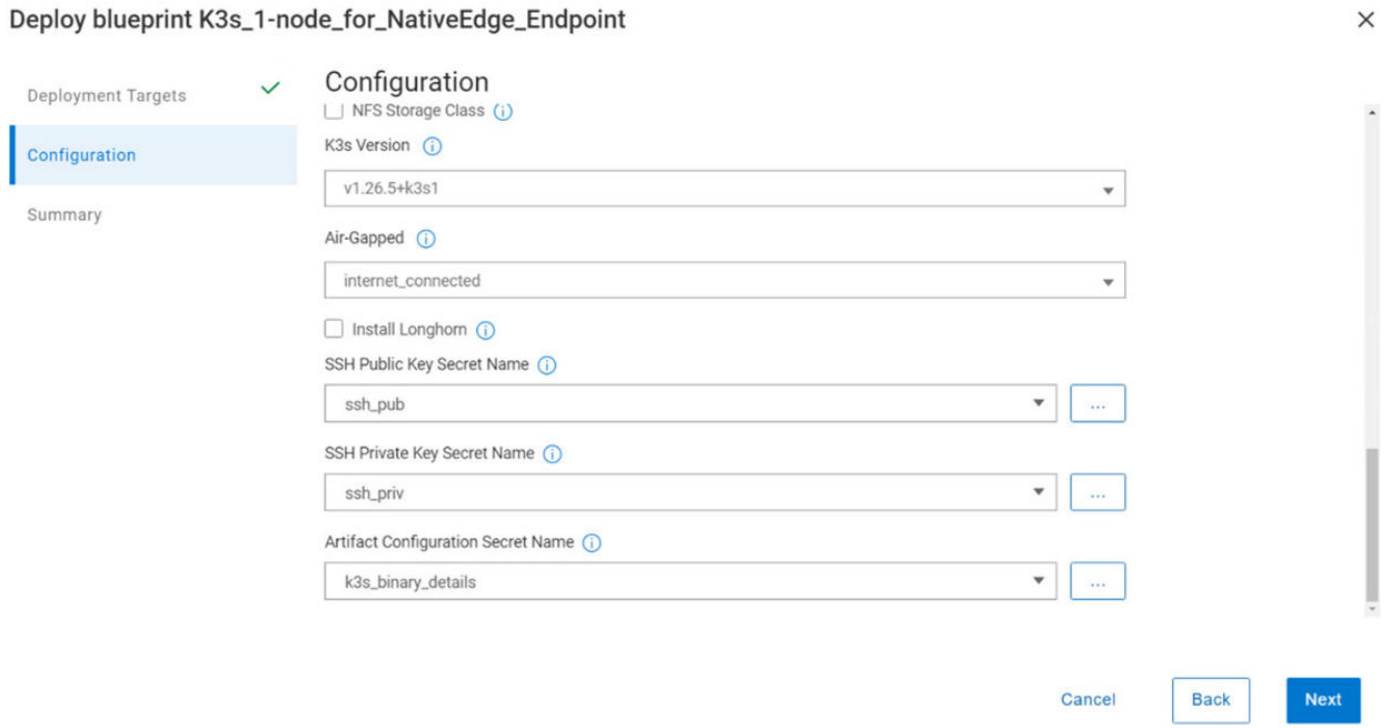


**Figure 13. Configuration tab**

# 9

# Conclusion

Dell NativeEdge helps customers simplify their edge operations. It enables data processing and analytics closer to the source, reduces latency, and minimizes the need for data to be processed in the cloud. Using NativeEdge, customers can simplify their edge operations with secure device onboarding and zero-touch provisioning. Also, the NativeEdge software platform offers a set of features to support the robust ecosystem that is required to address the challenges of the modern era.

# 10

# Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

On the **Manuals & Documents** tab of the Dell Automation Platform Support Site:

- Dell Automation Platform—Administration Guide
- Dell Automation Platform—Pre-deployment Guide
- Dell Automation Platform—Deployment Guide
- Dell Automation Platform—Security Configuration Guide
- Dell Automation Platform—Release Notes
- Dell Automation Platform—Simple Support Matrix
- Dell Automation Platform Event Codes—Reference Guide
- Dell Automation Platform Blueprint—Quick Start Guide

On the **Manuals & Documents** tab of the NativeEdge Support Site:

- Dell NativeEdge—Administration Guide
- Dell NativeEdge—Security Configuration Guide
- Dell NativeEdge—Service Manual
- Dell NativeEdge—Release Notes

On the Dell NativeEdge Info Hub Page:

- Developer documentation
- White papers
- Blogs, videos, briefs

Related references:

- Dell.com - My Account
- PowerEdge Servers
- OptiPlex Desktop Computers
- Precision Fixed Workstations
- Dell Edge Gateways
- Dell ECS Enterprise Object Storage