Connectivity for Dell infrastructure systems

Table of contents

Table of contents continued

Introduction

1: What is the secure connect gateway technology platform?

Our secure connect gateway 5.x technology is the next generation connectivity software from Dell Technologies Services.

It provides **a single connectivity solution for managing your entire Dell infrastructure portfolio** i.e., servers, networking, data storage, data protection, converged and hyper-converged (CI/HCI) solutions. It also replaces the legacy software – SupportAssist Enterprise and Secure Remote Services – whose capabilities are integrated into this technology.

We provide **flexible deployment options which are customer installable and upgradeable**. With a gateway option (delivered as a virtual appliance, a standalone application, or a container edition), a direct connect option, and a plugin option, you can choose what's right for your environment.

Our technology **– also known as remote IT support and monitoring software –** provides:

- Insight into the most critical issues
- Accelerated issue resolution with remote access and secure, two-way communication between Dell Technologies and the customer's environment
- A continued focus on security with policy manager software with advanced auditing and control features, the best-in-class MQTT protocol and new development processes
- Improved performance and scalability with the gateway handling even more telemetry data and actions across your Dell enterprise environment
- An enhanced web UI experience for our on-premise connectivity management dashboard

Once you've purchased a Dell infrastructure product and it's bundled with a support services contract e.g., any service level of ProSupport Infrastructure Suite, you can set up this connectivity software at no cost. No license is needed.

Once our software is monitoring these systems, we provide you with our unique integration of smarter AI, automated support, and real-time analytics.

2: Are there other ways to connect besides using the gateway option?

Yes. The secure connect gateway technology has also been implemented as a direct connect version for select Dell hardware and a plugin.

Some Dell products can directly connect back to the Dell Technologies backend and are suitable for customers who do not want to set up separate software. Please consult your product documentation. *Read Q12 & Q29 for additional details.*

For customers in a PowerEdge data center who are utilizing OpenManage, you can now connect with our Services plugin for OpenManage Enterprise for alerting, auto-dispatch, and collection capabilities.

Explore the technology: Visit Dell.com to hear from our experts & for technical resources

Infographic with key links: Getting started with connectivity in the datacenter

3: Has the legacy software – SupportAssist Enterprise and Secure Remote Services – been retired?

The **Virtual and Docker editions of Secure Remote Services v3.x** were fully retired on January 31, 2024. Intelligent, automated support for the supported Dell storage, networking and CI/HCI systems has been discontinued.

- Note: For customers with **Dell PowerStore and Unity products that utilize direct connect**, their technology was retired on December 31, 2024. To avoid service disruptions, an operating environment update is made available prior to the end of service life.

SupportAssist Enterprise 4.x & 2.x were retired on July 31, 2022. Intelligent, automated support for Dell server, storage, networking and/or CI/HCI systems has been discontinued.

4: Is this customer installable and upgradeable software?

Yes. You can download and install our connectivity technology without assistance from Dell Technologies.

Visit the Dell Support site for the gateway and plugin software resources.

- **Tip:** Explore our interactive technical demo (English only) to preview installation, registration and use of the gateway editions and the policy manager software.
- **Tip:** Use the Services connectivity readiness template to quickly extract the details from Dell Support documentation to get your networks ready to connect. *See Q15.*

5: Do I need a license?

No software license is required. However, to download and register your software, you must be authenticated at Dell.com Support.

Technology features and value

6: How does the use of connectivity software provide more value from the Dell support experience?

The main reasons companies use our connectivity tools are to mitigate downtime in their environment, reduce the burden of monitoring critical issues, and identify and fix smaller issues before they become larger, costly ones.

Setting up connectivity enhances the support experience for Dell infrastructure products with support services coverage e.g., with any service level for ProSupport Infrastructure Suite. Once our secure connect gateway technology – implemented as a gateway, direct connect or plugin option – is monitoring these systems in your environment, we provide you with proactive, preventative and, in some cases, predictive support.

Data is the lifeblood of our connectivity technology. **We leverage system state data from customer environments. And correlate it with years of incident and engineering data** from field and tech support teams as well as component manufacturers. Using **sophisticated AI models, including machine learning**, our connectivity technology can find and apply patterns to the telemetry & event data to accurately detect the right issue to act on.

Our technology identifies hardware and software issues, **creates a case and initiates contact from us to begin resolving an issue before it becomes a costly problem.** Depending on the type of issue, the alert may also **initiate an automatic parts dispatch** which means faster receipt of hardware parts.

Another great feature is **remote support** included on most of our storage, data protection, converged and hyper-converged (CI/HCI) products. In that scenario – when a case is opened on our side – if we can troubleshoot thru remote support, the technology enables secure two-way communication for authorized technical support agents to remotely access managed devices to diagnose and resolve issues.

Also, by sending telemetry back to Dell, the **historical data for your system can help to reduce time to resolution** when Dell Support gets involved. For example, when an alert is sent back to Dell, a support technician can connect to the device (based on any policies the customer has set), then confirm what actions need to be taken and provide the customer with an action plan. For example, parts can be replaced before they actually fail and ultimately minimize the risk of downtime.

Another benefit from the remote support features is **remote upgrades.** This is a great example of how we utilize our secure connection. Many products can have upgrade code or security patches for the product sent directly for the customer to apply at their convenience. Or our remote change management teams can schedule and execute the upgrade from start to finish without being on-site.

Hear from our experts:

- Listen to podcast (English only): Maximizing datacenter uptime with intelligent support
- Listen to podcast (English only): Maximize PowerEdge uptime with proactive, predictive support

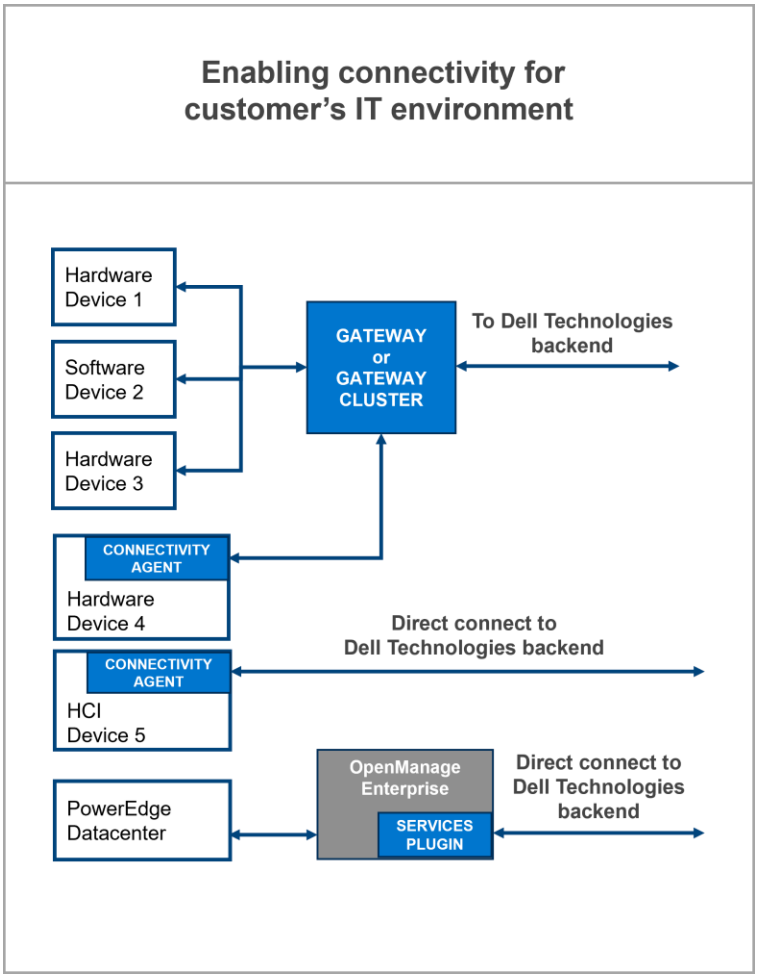
Watch short videos (English only)**:**

- Connectivity features and benefits
- Security architecture and features

Technology deployment options

7: What are the ways that you can deploy & configure the connectivity software in your environment?

You can choose what's right for your environment with our flexible installation options – a gateway option, a direct connect option and a plugin option. All are customer installable and upgradeable.



The secure connect **gateway option** allows you to connect your Dell systems to the gateway to communicate back to Dell Technologies Services. This simplifies your firewall / networking set up so that the gateway is the only thing connecting outbound over the internet.

For our gateway option, Dell provides a **virtual edition** for VMware, Microsoft Hyper-V & Linux KVM environments. We also have **container editions** for Docker, Podman, Kubernetes & OpenShift environments. For our smaller server customers, we provide an **application edition** with Windows / Linux versions. *See Q8-11.*

Customers looking for high availability and failover for their systems can set up multiple gateways, or a cluster that will provide redundancy in the event that one gateway is unavailable.

The **direct connect option** (enabled by integrating our connectivity technology into the Dell product's operating environment) is for smaller customers and non-traditional customers who might not want to set up additional software. *More in Q12 & Q29.*

Finally, for our compute centric customers, we've the **Services plugin for OpenManage Enterprise** for your PowerEdge server fleet for a single, secure direct connection. *More in Q13 & Q24-28.*

Infographic with key links: Getting started with connectivity in the datacenter

7 cont'd: What are the ways that you can deploy & configure the connectivity software in your environment?

Use the table below to identify the appropriate option for your environment. You should verify the product support matrix for secure connect gateway or visit the hardware product support page on Dell.com/Support. The application version is best for smaller customers who do not have a virtualized environment and use the supported Dell hardware and software.

Connect to monitor all devices in one place

Integrated solutions

Integrated solutions	Hardware and software supported
Secure Connect Gateway 5.x – Virtual Appliance Edition *For VMware, Microsoft HyperV, Linux KVM environments* *Container packages: Docker, Podman, Kubernetes, OpenShift*	Entire Dell product portfolio – data storage, servers, networking, CI/HCI and data protection
Secure Connect Gateway 5.x – Application Edition *Windows Enterprise management on servers* *Linux management on servers*	PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault
OpenManage Enterprise Services plug-in *For your OpenManage Enterprise environment*	PowerEdge servers

Direct connect for select Dell hardware

- Connectivity integration into Dell product's operating environment. Check Dell product support documentation to verify the specific product model and version.
- Appropriate for heterogeneous deployment of multiple Dell hardware products.
- Connect directly to Dell Technologies or via the secure connect gateway server.

Infographic with key links: Getting started with connectivity in the datacenter

8: What gateway software is recommended for my environment and what are the minimum requirements?

Gateway software	
Secure Connect Gateway - Virtual edition There are versions for: • VMware, Microsoft HyperV & Linux KVM environments • Container packages: Docker, Podman, Kubernetes, OpenShift Download documentation and all resources from Dell.com/Support.	Secure Connect Gateway - Application edition There are versions for: • Windows management server (monitors both Windows & Linux devices) • Linux management server (monitors Linux devices) Download documentation and all resources from Dell.com/Support.
Preview the interactive technical demo for technical tips on installation, registration, and use.	
Be sure to review the minimum requirements for installing and using secure connect gateway software	

Four steps for customers to get connected

1. **Prepare their site & verify account**
   Preview technical requirements and plan with network administrator. Prior to step 2, set up an enterprise business account at Dell.com/Support.
2. **Download**
   Sign in with account credentials at the product support page for secure connect gateway on Dell.com/Support.
   Get the right edition for their environment and create the authentication access key
3. **Install and provision**
   Deploy the virtual appliance or container template or install the application software. Complete initial registration steps.
4. **Connect their devices**
   Configure and enable communications between their Dell products and the gateway server

Tips for new users when getting started:

- New users must first set up an enterprise business account at Dell.com/Support. You will be prompted from the secure connect gateway download page to sign in and complete this step.
- Once completed, sign in with your account credentials at the secure connect gateway product support page on Dell.com/Support.
- Be sure to input the site location for software installation. This helps us to provide a better support experience.
- Get the right edition for your environment. During this step, you should create the authentication access key.

Note: *For those connecting for the first time ever, site preparation will require the most time. From days to potentially months, depending on the complexity of your network and security policies. Your security and networking teams may ask for a product review before implementation.* Get our security paper.

Explore the technology: Visit Dell.com to hear from our experts & for technical resources.

Need help? Ask our experts anything on the Secure Connect Gateway Forum

9: Do I have to register my secure connect gateway device with Dell Technologies?

Yes. To use the secure connect gateway and receive best-in-class security, you must register with Dell Technologies.

> **Tip:** Learn how to set up an enterprise business account You are correctly authenticated when a black check mark appears next to your name at Dell.com/Support.

Use your enterprise business account to log in to the download page, generate an access key and pin, and then, use your access key and pin to activate your secure connect gateway.

Customers who do not have a business account will be asked for additional information about their organizations and products. The customer will be able to continue after undergoing the verification process.

10: What gateway technology has remote support capabilities? Also, what products have remote access capabilities that are being managed by secure connect gateway?

Remote support capabilities are only available on the Virtual and Container editions of secure connect gateway and *are not available on the Application edition*.

Data storage, data protection, converged and hyper-converged (CI/HCI) products have remote access capabilities. The PowerEdge and PowerSwitch products can also be enabled for remote support in the on-premise gateway management user interface via Device Overview.

Authorized tech support agents use a required two-factor authentication to remotely access managed devices to troubleshoot and resolve issues. All remote sessions are audited, and the details can be accessed from the on-premise gateway management console for the secure connect gateway, under the Audit section.

For additional control and advanced auditing capabilities, customers can set up a policy management server which allows the flexibility to block or allow all remote access sessions.

11: What is the policy manager software and how is it used for the gateway option?

The policy manager for secure connect gateway is separate and complimentary external software that can be installed for advanced auditing and remote control capabilities.

With the policy manager, you can set up policies for remote support, file transfer and/or remote actions for the products that support one or more of these remote access capabilities.

Note: *The policy manager is only for use with the Virtual and Container editions of the gateway. It is not available for the Application edition.*

> **Tips:** Preview policy management module in the interactive demo. Check out technical how-to videos for the Virtual Appliance edition.

12: What products are enabled for direct connect? Can I use direct connect with a gateway as well?

In some instances, our connectivity technology is integrated into the Dell product's operating environment and allows for direct connection to our Services backend. This is what is meant by 'direct connect'.

You will be prompted to enable connectivity services while setting up your Dell hardware and software products.

However, at any time, you can switch your direct connect enabled Dell product to connect via a gateway. Your company's security and networking policies will influence your configuration decisions.

Dell infrastructure products enabled for direct connect *Always verify the most up-to-date list of supported products at Dell.com/Support*
Appsync | APEX AIOps Infrastructure Observability Collector | CMS – VxBlock software Data Backup / Avamar | Data Domain | Data Domain Management Console | Edge Orchestrator Elastic Cloud Storage | Metro Node Appliances | ObjectScale PowerFlex Family – Appliance, Rack, Software PowerProtect - Data Manager, Data Manager Appliance, Scale out Appliance PowerScale | PowerStore | PowerVault | S5000 Series | SRM | Streaming Data | Unity | VxRail *Check your product support documentation to verify the specific product model and version with direct connect capabilities.*
PowerEdge: *Read Q29* for an update on the direct connect option for servers. *Note: Eligible devices only have an option to connect via the virtual appliance edition of a gateway.*

Note: *SupportAssist, SupportAssist Enterprise and Secure Remote Services software capabilities are now part of our next-gen connectivity software platform. These software references in your product's user interface will be updated accordingly over time.*

13: What is the Services plugin for OpenManage Enterprise?

The secure connect gateway technology has also been implemented as a plugin. For customers in a PowerEdge data center who are utilizing OpenManage, you can now connect with our Services plugin for OpenManage Enterprise for alerting, auto-dispatch, and collection capabilities. *Also see Q25, 26 & 28.*

Resources:

- Learn more about the plugin and get technical resources
- For supported products, view the product Support Matrix document on the OpenManage Enterprise Services product support page.

Hear from our experts:

- **Watch short video** (English only)**:** Services plugin for OpenManage Enterprise
- **Listen to podcast** (English only)**:** Maximize PowerEdge uptime with proactive, predictive support
- **Read:** Security paper

14: How do I get assistance deploying connectivity software?

Many customers download and install our connectivity technology without assistance from Dell Technologies. Visit our web page for all resources.

Tip: You can launch & explore our interactive technical demo

- *Preview the installation, registration and use of the gateway editions and the policy manager*

For those wanting assistance, the ProDeploy Infrastructure Suite of services include the enablement and configuration of the secure connect gateway.

Customers with ProSupport Plus coverage are assigned a Technical Customer Success Manager who can assist with installation and registration questions.

Otherwise, as needed, you should contact Dell Technologies Support for help.

15: I am ready to get connected. How can I make sure that my networking team has all of the right information before I try to connect my systems?

This Services Connectivity Readiness: Network Preparation template helps you to quickly extract the minimum network requirements, gateway and device-specific port requirements, and firewall rules exception details from Dell Support documentation to get your network ready to connect.

The template can be used to streamline network preparation for secure connect gateway technology deployed as gateway, direct connect and plugin options. Simply answer the questions about your Dell products and IT environment to generate the network requirements. Then, download the details as a ready-made report to share with your networking and security teams.

The template will guide you through net-new connectivity installation and product connectivity. It is also suitable when connecting new products within existing connectivity configurations.

Steps:

1. Download the zip file by clicking on the Services Connectivity Readiness: Network Preparation template link. **Note:** Always download and use the latest template from this link.
2. Extract the file to a new folder and launch the application to open the template.
3. Complete the form by responding to questions about the Dell products to be connected and your IT environment.
4. Save or export the completed results in an Excel format to share with your networking and security teams.

Note: This offline template will be periodically updated to stay current with Dell Support documentation.

16: If I experience issues, how do I contact Support?

If you are experiencing any issues with Dell.com Online Support or secure connect gateway, visit our Administrative Support page from this location to request help. Select the category most resembling your issue and fill in the details as prompted. If you need immediate assistance with a technical support issue, contact us here. Please contact your Technical Customer Success Manager (if applicable).

Security

17: Tell us more about this software in the customer's environment and the connection back to Dell. How is that secured?

The connection between your environment and Dell is secured through a mutual TLS tunnel & a certificate chain. In this type of configuration, your systems will connect to our software in your environment and those connections will only have to be internal port/networking changes. The software will be the only thing that connects outbound over the internet and back to Dell. It acts as an aggregation point for all of your connected systems for the event and telemetry data. This is the only system state information which is being sent.

All telemetry from the systems is transported using HTTPS TLS 1.3. We also provide remote support capabilities using the secure tunnel to access and troubleshoot your system which speeds up issue resolution and helps avoid downtime.

Learn more from our security paper.

18: How is remote support conducted? Who can access the system from Dell through a remote support session?

From Dell, our technical support engineers use a portal to create remote support sessions to access your systems for troubleshooting and for upgrade activities. They use multi-factor authentication to access this portal. These Dell team members must undergo rigorous training and require management sign off for access. We use the MQTT protocol – a widely accepted solution for enterprise connected systems – as our remote support agent.

19: With the focus on security, is this system state data event and telemetry information being audited? What is the role of the policy manager?

We audit all transactions, and, in the software, you can view this information in the user interface. All remote support sessions, event and telemetry transfers are available for you to view.

For those customers with more stringent security policies or with third-party auditors who require this information to be stored for an extended period of time, we recommend setting up our policy manager software. Our policy manager works with your secure connect gateway to provide advanced auditing and remote support control features. *Also see Q11.*

20: Where can I find more information about the security architecture of the connectivity technology?

Download the security paper to learn how secure connect gateway technology integrates data protection and threat prevention into a secure, automated support experience.

The paper covers:

- **Secure onsite data collection:** Learn how the secure connect gateway acts as a secure communications broker, allows customers to control authorization requirements, leverages two factor authentication protocols and much more.
- **Secure data transportation and communication:** Learn how secure connect gateway uses encryption and bilateral authentication to create a secure Transport Layer Security (TLS) tunnel for its heartbeat polling, remote notification and remote access functions.
- **Secure data storage, use and processes:** Read more about the array of measures implemented daily to protect your data including physical security, supply chain risk management and secure development processes.

Hear from our experts:

- **Listen to podcast** (English only)**:** Maximizing datacenter uptime with intelligent support
- **Read:** Security paper

Watch short videos (English only)**:**

- Security architecture and features
- Security configuration for large and small scale environments
- Security features for financial sector

Or watch the webinar (English only)**:** Hear from our experts in this Spiceworks Community event who cover:

- How secure connect gateway integrates privacy, data protection and threat prevention
- How to flexibly deploy connectivity across small, large and non-traditional environments
- Why automated support helps to prevent and mitigate issues for connected systems

Configuration scenarios

21: What are the considerations for deploying and configuring connectivity technology for your company's needs?

The first items to consider are the **types of products – compute, storage, data protection, converged and hyper-converged (CI/HCI) –** that you will be configuring for connectivity, and **your current environment** such as

- Are your data centers networked together or not?
- Do you manage compute or storage (including data protection, CI/HCI products) *separately or together*?

You'll also want to consider the **security and networking policies** of the company. In addition, **whether your teams want to manage all products together or prefer to segment them by geo-location or product type.**

Essentially, you must think through how things are wired together, how teams work together and how to minimize network complexity. This will allow you to design the most effective architecture based on the varied deployment options.

Read and share our connectivity configuration considerations overview which covers:

1. What's the recommended configuration for a larger security-conscious company?
2. What are the configuration and deployment options for a mid-sized to small organization?
3. What if I'm a large to mid-sized company with a compute centric environment? How do I decide which tool to use?
4. What if I have ~ 1 – 50 PowerEdge servers and I don't have a virtualized environment. What are my gateway options?
5. What if I have Dell products with direct connect availability? What are some typical use cases?
6. What is the right configuration for my company?

Tip: Download and use the **Services connectivity readiness template** to generate a report for your networking and security teams with the specific port & firewall requirements for network set up. ***See Q15.***

Support services

22: How is connectivity relevant to the value of the support services contract on my Dell infrastructure products?

In a nutshell, you get more value from your active support contracts on Dell systems by deploying our connectivity software in your environment and connecting your Dell devices to be monitored by this software. It is free software – no license needed. We support over 90+ Dell infrastructure products – hardware and software. You will benefit from our unique integration of smarter AI, automated support, and real-time analytics.

Customers with ProSupport Infrastructure Suite services receive great value across all levels.

- Learn more: ProSupport and ProSupport Plus coverage for Dell infrastructure systems
    - Learn more: Lifecycle Extension with ProSupport or ProSupport Plus
- Note: Dell systems with Basic Hardware Support (Next Business Day) also benefit from our proactive, automated issue detection, case creation and notification features when monitored by our connectivity software. When an issue is detected, Basic Support customers will receive an email with the case number and are prompted to contact Dell Support in a timely manner to confirm that they want Dell assistance with troubleshooting and resolution.

In addition, explore our Specialty Support Services for Infrastructure

23: What happens to the automated support features when support services contract coverage e.g., with ProSupport Infrastructure Suite expires on my monitored system?

If your service contract for any level of ProSupport Infrastructure Suite expires, the automatic case creation feature will be disabled. The secure connect gateway technology deployed as a gateway, direct connect or plugin, will, however, continue to run automated system state collections. If you upgrade or extend your contract on a system (service tag), automatic case creation will be re-enabled automatically on that system.

Connectivity for PowerEdge

24: What are the best ways to deploy and configure this connectivity software for servers? How do you decide which tool to use?

In a nutshell, the Services plugin thru the OpenManage Enterprise solution is good for customers with compute centric environments while the gateway solution is the way to go when managing a variety of Dell infrastructure products.

Both solutions include our alerting, auto-case creation, auto-dispatch and telemetry collection capabilities for PowerEdge servers that have a support contract.

What you choose will depend on the type of environments you have, the networking between those environments, the device types being monitored and your preferences.

If you have or are thinking of setting up OpenManage Enterprise, the Services plugin is right for you! OpenManage Enterprise is Dell's infrastructure solution that facilitates lifecycle management of thousands of PowerEdge servers from a single console.

- If you're new to this, you would simply install Open Manage Enterprise in your environment, onboard your server products and then install our Services plugin – making sure that your firewall is configured correctly – so it starts sending the alerts and telemetry back to Dell.

For customers with a mix of Dell infrastructure products such as Powerstore, PowerMax, PowerScale, Data Domain, and VxRail, running alongside PowerEdge, we recommend setting up our secure connect gateway solution to manage those systems from a single UI.

Hear from our experts:

- **Listen to podcast** (English only)**:** Maximize PowerEdge uptime with proactive, predictive support
  - What's involved in connecting PowerEdge systems thru the OpenManage Enterprise solution and how this compares to connecting via a gateway solution
  - How to connect to the PowerEdge devices themselves
  - How you can easily scale the number of connected servers over time
  - Other configuration scenarios: Run both the plugin and gateway options

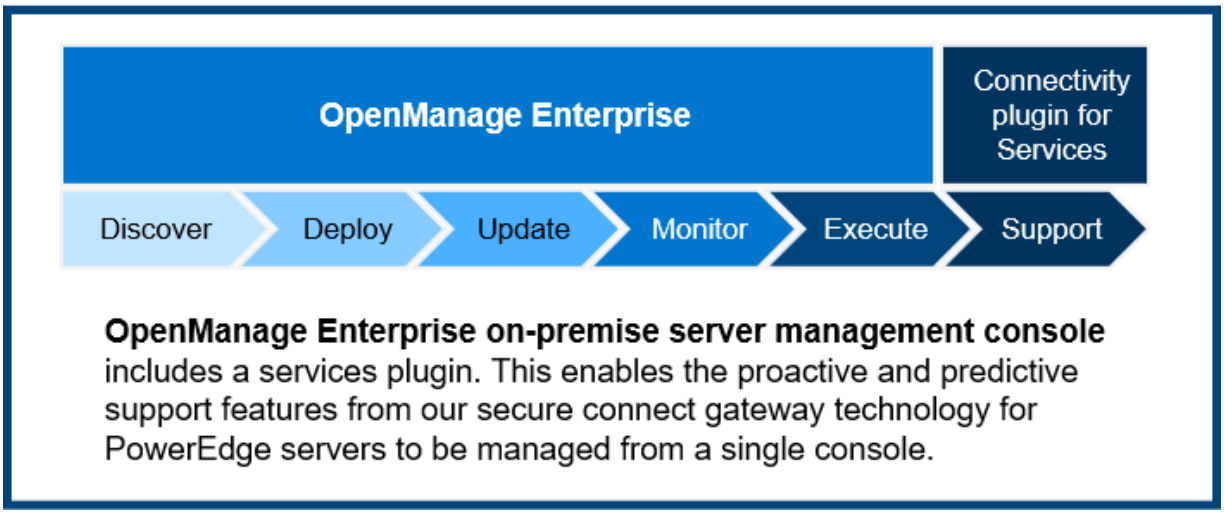
Update on the direct connect option for servers

- *Read Q29* for all details including product and region-specific details & guidance on connectivity considerations.

25: How does connectivity for services compliment data center management lifecycle monitoring by OpenManage Enterprise?

OpenManage Enterprise is a simple-to-use, one-to-many systems management console. It cost-effectively facilitates comprehensive lifecycle management for PowerEdge servers and chassis in one console.

See diagram below to understand how the connectivity plugin for OpenManage Enterprise compliments the OpenManage Enterprise experience for the data center.



This capability is currently available via the **Services plugin for OpenManage Enterprise.** This plugin enables the proactive and predictive support features from our secure connect gateway technology for PowerEdge servers to be managed from a single OpenManage Enterprise console. Learn more and find resources.

26: Which systems are supported for the Services plugin for OpenManage Enterprise?

PowerEdge servers and chassis with iDRAC and Chassis Management Controller (CMC) as well as Linux servers are supported.

To verify the specific supported products, visit the Dell.com/Support site and view the Support Matrix document on the OpenManage Enterprise Services product support page.

27: Does connectivity software for services allow me to perform data center lifecycle management tasks for PowerEdge servers, similar to OpenManage Enterprise?

No. Our connectivity software for Services ***does not*** transfer or orchestrate bios and firmware updates for standalone PowerEdge devices in a data center. Typically, compute-centric customers with standalone server environments install and use OpenManage Enterprise for these types of lifecycle management capabilities.

Note: Enabling the Services plugin for OpenManage Enterprise will activate our alerting, auto-case creation, auto-dispatch and telemetry collection capabilities for PowerEdge servers with an active support contract. However, the Services plugin ***does not*** enable upgrade code delivery and remote support access capabilities for the managed systems.

28: When should I use the Services plugin vs the AIOps plugin in my OpenManage Enterprise environment? Do I get automated, proactive support case creation with the AIOps plugin?

OpenManage Enterprise is Dell's infrastructure solution that facilitates lifecycle management of thousands of PowerEdge servers from a single console. The table below explains the use and capabilities of the Services plugin as compared to the AIOps plugin.

We recommend enabling ***both*** the Services plugin and AIOPs plugin to take full advantage of their respective capabilities from the OpenManage Enterprise console.

Overview of capabilities & use cases		
Plugin	OpenManage Enterprise **Services plugin**	OpenManage Enterprise **AIOps plugin**
When to use	Enable when you want **automated proactive support features**	Enable when you want **the capabilities of the Dell AIOps cloud-based dashboard**
Plugin capabilities	Provides alerting, auto-case creation, auto-dispatch of parts and telemetry collection capabilities	Enables health monitoring & predictive insights for capacity shortfalls, performance anomalies, cybersecurity risks and sustainability
Capabilities activated for	Assets with an active support contract including ProSupport and ProSupport Plus contracts. *See Q21.*	Assets with ProSupport and ProSupport Plus contracts
Secure connectivity set up explained	Note: The customer will enable one connection – not two – in their environment. There will be one secure mutual TLS connection ***between*** the OpenManage appliance in the customer's environment and Dell's backend based on secure connect gateway technology.	
Key takeaway	If you only enable the Services plugin, you don't get AIOps plugin capabilities. If you only enable the AIOps plugin, you don't get Services plugin capabilities. **Best practice recommendation: Enable both plugins.**	

29: What is the Dell Connectivity Client that appears on some of my PowerEdge systems? Is it compatible with secure connect gateway technology? Is it compatible with Dell AIOps?

Certain models of PowerEdge servers shipped with iDRAC include an integrated Dell Remote Access Controller (iDRAC) plugin called the Dell Connectivity Client. Read the FAQs for product and region-specific details. This client enables direct connection from the iDRAC to Dell backend services and provides streaming telemetry using the OpenTelemetry framework.

- **Note**: Customers must explicitly opt in to / opt out of the use of the Dell Connectivity Client during the Sales process since this PowerEdge product configuration is pre-enabled by Dell.

Compatibility with secure connect gateway technology:

The Dell Connectivity Client can be switched to connect via the virtual appliance edition of a secure connect gateway, starting with v5.32. The customer must explicitly opt in to the '*Streaming Telemetry Connection'* within the gateway to set up the connection to Dell for streaming telemetry.

- **Note:** On-premise audit and collection capabilities in the gateway are not supported for iDRAC models connecting via this client. Also, device status details in the gateway are limited and IPV6 is not supported.

When customers opt out, these iDRAC models will use the existing gateway connection in lieu of connecting via the Dell Connectivity Client. Thus, streaming telemetry is not enabled.

At this time, the Dell Connectivity Client does not have the ability to connect to the container or application editions of a secure connect gateway nor the Services plugin for OpenManage Enterprise.

Best practice recommendations:

If you are already using the secure connect gateway or the Services plugin for the PowerEdge systems in your environment:

- You can continue to use these existing configurations and *do not need* to connect these PowerEdge systems back to Dell via Dell Connectivity Client. However, *you must take action* to disable the Dell Connectivity Client for these PowerEdge systems. Read this guide to disabling the Dell Connectivity Client configuration.

If your company requires a single secure connection to comply with security policies such as a gateway connection, we recommend that:

- You download and install the appropriate version of the virtual, container or application editions for secure connect gateway or the Services plugin for OpenManage Enterprise.
- In addition, you must take action to disable the Dell Connectivity Client for these PowerEdge systems. You will then connect these systems to the gateway or via OpenManage Enterprise for monitoring per our technical guides. Learn more about these technology deployment options.

A note about telemetry for Dell AIOps:

For iDRAC models connecting with the Dell Connectivity Client – directly or via a gateway with an opt in for a streaming telemetry connection – no extra set up is needed to provide telemetry to the Dell AIOps platform.

However, the customer must access the Dell AIOps dashboard and onboard these models to enable Dell AIOps features & insights. Access to the dashboard is included with services for ProSupport or ProSupport Plus for Infrastructure services as well as ProSupport One for Data Center. Also see Q36.

Other general highlights

30: Where can I find information on the alert policies for secure connect gateway? When are predictive support cases opened for hardware failures?

Our Secure Connect Gateway Alert Policy provides information on the alerts that open cases with Dell Technologies technical support. Customers using the secure connect gateway will only receive automated predictive case creation for server hardware (hard disk, backplane and expanders) on systems with ProSupport Plus services. Predictive alerts are based on scheduled collections that are submitted to Dell Technologies.

31: What should I know about the credential management features of the gateway?

The secure connect gateway provides the flexibility to add multiple credential accounts and profiles. The credential accounts allow administrators to add authentication by product type. In addition, profiles allow multiple administrators who differ by function or region to manage their specific accounts. Products where credentials are needed include PowerEdge servers, iDRAC, Compellent, networking, PS series, MD series and Webscale systems.

We also offer credential vault integration. This is a great feature for customers with many devices as they can add systems and maintain the correct credentials without compromising security or increasing manual work. We're integrated with the market leader – CyberArk – with CyberArk Conjur APIs and CyberArk Credential Provider products currently supported. We also support Microsoft Azure Key Vault and HashiCorp credential vault. Additional vendors will be added. Check our support documentation for the most up to date list.

Tip: Preview these features in the *Device Management* module in the interactive demo

.

32: What are the key features of the maintenance mode?

An "event storm" happens when hardware alerts occur in quick succession, breaching a pre-defined count limit. In this scenario, the secure connect gateway will stop processing alerts for the specific devices that have triggered the event storm. All other devices will continue to be monitored by secure connect gateway for validated alerts that may create support cases.

In addition, users now have an option to manually enable maintenance on one or more devices from within the system. This can be used for planned maintenance and deployed when you do not want secure connect gateway to monitor those devices. Once the planned maintenance activities are completed, you can manually disable maintenance mode to signal the secure connect gateway to resume its monitoring.

33: Does the gateway option allow me to set email notification preferences?

Yes. Your email notification preferences can be tailored from the secure connect gateway user interface within the Settings tab. Check the user guide for details.

34: What languages are supported in the on-premise gateway management dashboard?

The secure connect gateway software interface is available in English, German, Brazilian Portuguese, French, Spanish, Simplified Chinese, and Japanese. However, customers may choose 1 of 28 languages for auto-email notifications sent at the time of a service request incident. Note: A few e-mail notifications will not be translated into local languages due to OS limitations.

35: How do I get started with REST APIs?

With the gateway option, customers are able perform and support their own custom scripting with REST APIs. Download the user guide for REST APIs from our documentation section.

36: How is this connectivity software used for the Dell AIOps portal?

Dell AIOps (formerly known as APEX AIOps Infrastructure Observability and CloudIQ) is a cloud-based, AI-driven observability and management solution designed to optimize Dell infrastructure.

It delivers real-time insights to maximize infrastructure performance, strengthen cybersecurity, enhance sustainability, and support proactive planning. Featuring an intuitive platform and a generative AI assistant, Dell AIOps helps you minimize risks, boost efficiency, and simplify IT operations.

- Key attributes include: Health status and cybersecurity risk assessments and recommendations for remediation; performance and capacity tracking, anomaly detection and forecasts; failure prediction; energy and emissions tracking and forecasting; and virtualization resource monitoring.

Our connectivity software is used solely for transmission of system and event data from the customer environment. The telemetry is securely transmitted back to the Dell backend where it is analyzed by the AI algorithms for Dell AIOps.

37: Can I see & manage my connected Dell infrastructure products with active support contracts in the TechDirect portal?

No, you cannot view or manage connected Dell infrastructure products in TechDirect. Our connectivity software is not integrated with TechDirect, so alert data and automated support cases for connected Dell systems are not supported or visible in the portal's dashboard.

However, you can access and manage automated support case details for Dell systems connected via the gateway, direct connect and plugin options at the Online Support site and in the MyService360 analytics dashboard.