Connectivity for enterprise systems

Table of contents

General feature highlights continued

16. What happens to secure connect gateway features when ProSupport Enterprise Suite or ProSupport One for Data Center coverage on my monitored system expires?
17. Does secure connect gateway allow me to set email notification preferences?
18. What languages are supported for the secure connect gateway on-premise connectivity management dashboard?
19. Where do I view dispatch notifications when my devices are connected?
20. What gateway technology has remote support capabilities? Also, what products have remote access capabilities that are being managed by secure connect gateway?
21. What is the policy manager for the secure connect gateway?
22. How do I get started with REST APIs?

Feature highlights: PowerEdge servers OpenManage Enterprise environment

23. Which systems are supported by the connectivity plugin for OpenManage Enterprise?
24. What are the prerequisites for connectivity monitoring of PowerEdge devices?
25. How does connectivity for services compliment data center management lifecycle monitoring by OpenManage Enterprise?

Security information

26. Where can I find more information about the security architecture of the connectivity technology?

General Information

1. **What is the secure connect gateway 5.x technology? Does it replace the SupportAssist Enterprise and Secure Remote Services solutions?**

   The secure connect gateway 5.x technology is the next generation consolidated connectivity solution from Dell Technologies Services. It replaces the legacy solutions – SupportAssist Enterprise and Secure Remote Services – whose capabilities are integrated into the secure connect gateway technology.

   Our secure connect gateway 5.x technology is remote IT support and monitoring software that is delivered as an appliance and a stand-alone application**.** It provides a single solution for your entire Dell portfolio supporting servers, networking, data storage, data protection, hyper-converged, and converged solutions. In addition, this version 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
   - Single installation and registration for the data center
   - 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

   This technology is available to new and current Dell Technologies connectivity customers with a warranty or a contract for a service level of ProSupport Enterprise Suite.

   Update on legacy connectivity platforms:

   - **SupportAssist Enterprise 2.x and 4.x** were retired on July 31, 2022.
   - **Secure Remote Services v3.x – Virtual and Docker editions:** **End of service life update** Transition to full retirement of this solution commences June 15, 2023, and wraps up on January 31, 2024.

   Current customers using Secure Remote Services 3.x are strongly encouraged to proactively upgrade their enterprise connectivity prior to January 31, 2024 to avoid disruptions in automated, intelligent support for systems. **See Q3 for end-of-service-life details for legacy solutions and Q6 for guidance on upgrades.**

2. **Are there other ways to connect besides using secure connect gateway?**

   Yes. 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.

   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.

3. **Can I continue to use SupportAssist Enterprise and Secure Remote Services technology? When will these solutions be retired?**

   If you are new to support technology, download and use the appropriate next-gen secure connect gateway solution.

   SupportAssist Enterprise 2.x and 4.x were retired on July 31, 2022.

   The transition to the full retirement of Secure Remote Services v3.x – Virtual and Docker editions – commences June 15, 2023, and wraps up on January 31, 2024.

In transition to full retirement:	Recap of legacy solution
Secure Remote Services (SRS) version 3.x (Formerly ESRS)	For storage, data protection and CI/HCI products. Deployed as a virtual appliance or containerized system. No direct upgrade path from Secure Remote Services to SupportAssist Enterprise 4.x. **End of service life update**

- Note: For customers with PowerStore and Unity products that utilize direct connect, we will retire Secure Remote Services-based technology at a date to be announced.

- On the effective date, all versions of the specified connectivity solution will reach their end of service life. As a result, support (including remediation and mitigation of security vulnerabilities) for the solution will be discontinued.
  - Learn more about support for limited functionality between June 15, 2023, and January 31, 2024.

- **The replacement solution is the new secure connect gateway.**
  - *Note: The proactive and predictive capabilities of legacy connectivity for Dell products will be discontinued unless the upgrade to the replacement technology is in place.*

As the end-of-service-life date for a solution approaches, Dell Technologies Services will send a notification email to the affected customers announcing the end of support and maintenance.

For those using Secure Remote Services 3.x – upgrade before January 31, 2024:

In-place upgrade paths make it easy to adopt secure connect gateway 5.x technology with minimal disruption. Get started from the upgrade links in the gateway management dashboard.

Resources: Interactive demo | Technical videos – Application | Virtual Appliance editions

4. **What is the right secure connect gateway deployment option for my environment?**

Use the table to select 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 hardware and software supported below.

Connect via gateway technology to monitor all devices in one place

Integrated gateway solutions	Hardware and software supported
Secure Connect Gateway 5.x – Virtual Appliance Edition *VMware* *Microsoft HyperV* *Container packages: Docker, Podman, Kubernetes*	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
- Appropriate for heterogeneous deployment of multiple Dell hardware products
- Connect directly to Dell Technologies or via the secure connect gateway server

5. **What software is recommended for my environment and what are the minimum requirements?**

   Secure Connect Gateway - Virtual edition:
   There are versions for:
   - VMware environment
   - Microsoft HyperV environment
   - Container packages: Docker, Podman, Kubernetes (Now available)

   Review minimum requirements for installing and using secure connect gateway software. 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)

   Review minimum requirements for installing and using the software. Download documentation and all resources from Dell.com/Support.

   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 provide a better support experience.
   - Get the right edition for your environment. During this step, you should create the authentication access key.

   Explore the technology:
   Hear from our experts in this Spiceworks Community event as they 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

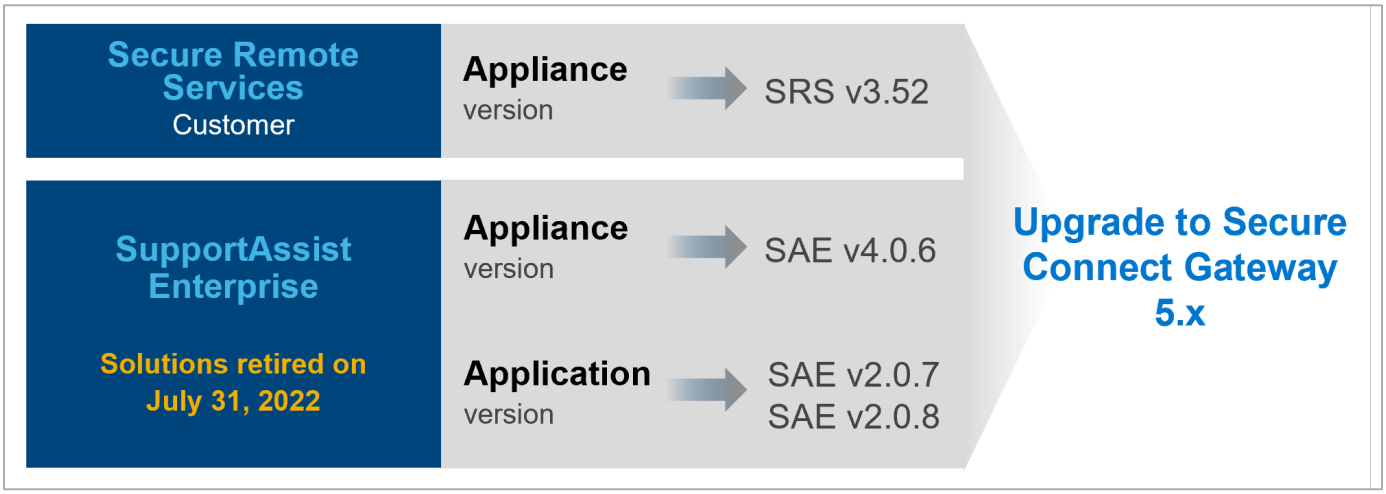
   Launch our interactive technical demo
   - *Covers new installations, enterprise business account set-up (included in Modules 1 & 2), upgrading from the legacy solution – Secure Remote Services, the gateway management dashboard features and the policy manager (Virtual edition only).*

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

6. **What version of SupportAssist Enterprise or Secure Remote Services should my system be running in order to upgrade to secure connect gateway 5.x?**

   SupportAssist Enterprise 2.x and 4.x were retired on July 31, 2022.

   You will need to ensure your Dell hardware or software are running the following version of Secure Remote Services. You will receive a prompt to upgrade to the secure connect gateway 5.x technology in your web user interface.



   Tip: Preview the steps to *Upgrade from Secure Remote Services 3.52* in the interactive demo

7. **What automated support features are available with ProSupport Enterprise Suite coverage?**

Features	Basic	ProSupport	ProSupport Plus
Automated issue detection & system state information collection	●	●	●
Proactive, automated case creation and dispatch notification		●	●
Predictive issue detection for failure prevention[1]			●

1. Predictive analysis failure detection includes server hard drives and backplanes when connected through secure connect gateway

   Learn more about our Support Services for IT Infrastructure.

8. **How does secure connect gateway technology save me time during troubleshooting?**

   Our connectivity technology automatically detects issues, captures system state information and initiates alerts and contact from Dell Technologies. You will eliminate time spent on collecting system state information, case creation and engaging with Dell Technologies. You can also use secure connect gateway to run automatic collections or on-demand collections, and to automatically send system state information to us for proactive case creation. Depending on the issue and your preferences, the gateway also can initiate remote resolution with remote access and secure, two-way communication between you and Dell Technologies.

9. **Do I have to register my secure connect gateway 5.x device with Dell Technologies?**

   Yes. To use the secure connect gateway and receive best-in-class security, you must register with Dell Technologies. 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 additional information about their organizations and products. The customer will be able to continue after undergoing the verification process.

10. **How do I get assistance deploying secure connect gateway technology?**

    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

    - *Covers new installations, enterprise business account set-up (included in Modules 1 & 2), upgrading from the legacy solution – Secure Remote Services, the gateway management dashboard features and the policy manager (Virtual edition only).*

    For those wanting assistance, the ProDeploy Enterprise suite of services include the enablement and configuration of the secure connect gateway. Customers with ProSupport Plus coverage are assigned a Service Account Manager (SAM) who can assist with installation and registration questions. Otherwise, as needed, you should contact Dell Technologies Support for help.

11. **If I experience any 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 Service Account Manager (if applicable).

General feature highlights

12. 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.

13. How do I see Dell automated alert data in my dashboard under *Connect and manage* in the TechDirect portal?

In the online dashboard for TechDirect under the *Connect and manage* tab, you can manage enterprise alerts and assets. Here, the IT admin can set rules to review automated alerts for support case creation or parts dispatch, and determine whether to forward to Dell Technologies.

Important connectivity requirement for data: The customer must integrate alert data to this dashboard as part of their on-premise gateway configuration. This is applicable to gateway editions and the plugin for OpenManage Enterprise environment.

Note: This feature is available for PowerEdge, iDRAC, PowerSwitch, Webscale, PeerStorage, EqualLogic, Compellent, Fluid File System (FluidFS), PowerVault and PowerStore systems that may use OpenManage Enterprise Services plugin, and/or secure connect gateway connectivity. Be sure to verify the required integration steps from the user or product installation guide.

Other: Alerts from devices connected to Secure Remote Services technology are not supported in this *Enterprise Assets and Alerts* dashboard in TechDirect.

14. What should I know about the credential management features of secure connect 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.

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

15. 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.

16. What happens to the secure connect gateway features when ProSupport Enterprise Suite or ProSupport One for Data Center coverage on my monitored system expires?

If your ProSupport Enterprise Suite or ProSupport One for Data Center service contract expires, the automatic case creation feature will be disabled. The secure connect gateway 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.

17. Does secure connect gateway 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.

18. What languages are supported for the secure connect gateway on-premise connectivity 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.

19. Where do I view dispatch notifications when my devices are connected?

From the dashboard for managing enterprise assets and alerts under *Connect and manage* in the TechDirect portal:

- You can review your dispatch preferences for eligible Dell servers, networking and storage systems.
- Important connectivity requirement for data: The customer must integrate alert data to this dashboard as part of their on-premise gateway configuration. This is applicable to gateway editions and the Services plugin for OpenManage Enterprise environment. Review Q13 in this document.

From the analytics dashboard in the MyService360 portal:

- You can view the dispatch notifications for eligible Dell storage, data protection, and CI/HCI devices

20. 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 is not available on the Application edition.

Data storage, data protection and 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.

21. What is the policy manager for secure connect gateway?

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

Tip: Preview these features for the *Virtual Edition – Policy Management* in the interactive demo and check out technical how-to videos for the Virtual Appliance edition.

22. How do I get started with REST APIs?

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

Feature highlights: PowerEdge server OpenManage Enterprise environment

23. Which systems are supported by the connectivity plugin for OpenManage Enterprise?

PowerEdge servers and chassis with iDRAC and Chassis Management Controller (CMC) as well as Linux servers are supported. Learn about the supported products and get technical resources.

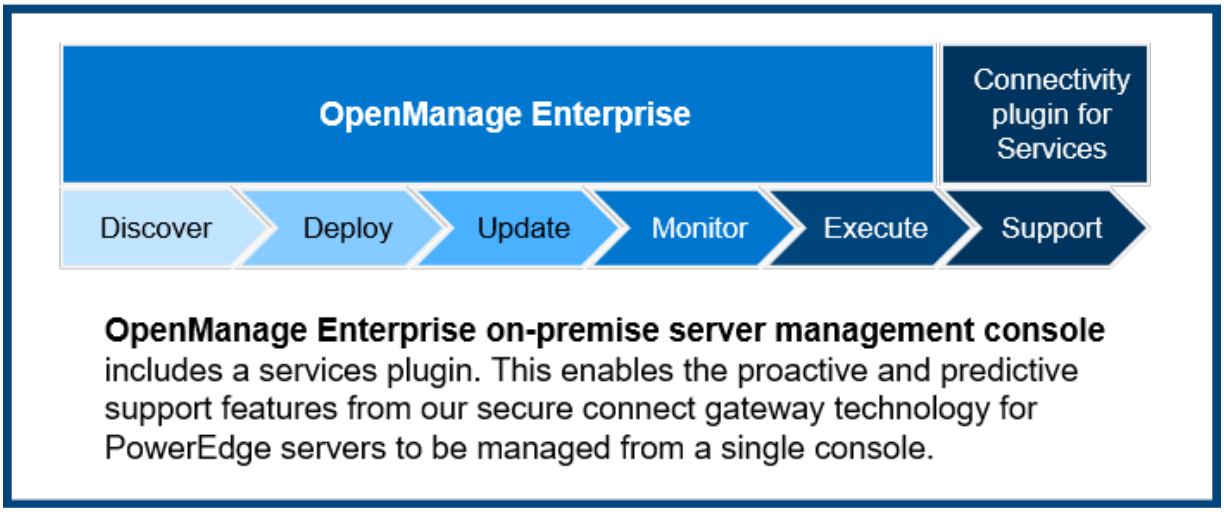
24. What are the prerequisites for connectivity monitoring of PowerEdge devices?

The plugin for OpenManage Enterprise and the gateway editions can monitor 12G and above PowerEdge servers out-of-band (when using iDRAC7, iDRAC8, and iDRAC9) as well as PowerEdge chassis. For additional information, refer to the support matrix for the specific device.

Alternatively, PowerEdge servers can be managed in-band with the prerequisite of the OpenManage Server Administrator (OMSA) agent being installed and running on the device. The recommended version of OMSA varies based on the operating system running on the device.

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 services for OpenManage Enterprise compliments the OpenManage Enterprise experience for the datacenter. This is currently available via the OpenManage Services plugin. Learn more and find resources.



Security information

26. Where can I find more information about the security architecture of the connectivity technology?

Download the security white 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.

Bonus: 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