

Secure Connect Gateway 5.x — Virtual Edition

User's Guide

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.

Chapter 1: Introduction.....	6
Version.....	6
Release history.....	6
Document purpose.....	7
Supported languages.....	7
Secure Connect Gateway capabilities available with Dell Technologies service contracts.....	7
Device types and supported features.....	8
Chapter 2: New and enhanced features.....	12
v5.30.00.14.....	12
v5.28.00.14.....	12
v5.26.00.20.....	13
5.26.00.18.....	13
v5.24.00.14.....	13
v5.22.00.18.....	14
v5.20.00.10.....	14
v5.18.00.20.....	15
v5.16.00.14.....	15
v5.14.00.10.....	16
v5.12.00.10.....	16
v5.10.00.10.....	17
Chapter 3: Dashboard.....	18
Network and service connectivity.....	18
Chapter 4: Devices.....	19
Methods of adding devices.....	21
Consolidated View.....	23
Add a chassis.....	24
Add an iDRAC.....	24
Add a networking device.....	25
Add a server or hypervisor.....	26
Add a software.....	27
Add a virtual machine.....	27
Add a converged or hyperconverged infrastructure appliance.....	28
Add a Web-Scale appliance.....	28
Add a data storage device.....	29
Add an EqualLogic or PowerVault MD3 or ME4 device.....	29
Add a Dell Compellent, Fluid FS device, or a Dell ML3 tape library.....	30
Add a direct liquid cooling device.....	30
Add a data protection device.....	31
Deep discovery.....	31
Maintenance mode overview.....	32
Inventory validation.....	33

Device correlation.....	33
Enable or disable remote access.....	33
Chapter 5: Device discovery rules.....	35
Create device discovery rule.....	35
Chapter 6: Adapters.....	37
Set up an OpenManage Enterprise adapter.....	37
Chapter 7: Device groups.....	39
Create a device group.....	39
Manage a device group.....	40
Enable group-level maintenance mode.....	40
Chapter 8: Device credentials and credential profiles.....	41
Device credentials.....	41
Add account credentials.....	41
Credential profiles.....	43
Create a credential profile.....	44
Assign a credential profile.....	44
Credential Vault.....	44
Add a credential vault.....	44
Edit or delete a credential vault.....	45
Chapter 9: Service requests.....	47
Chapter 10: Telemetry.....	48
Prerequisites to perform a collection.....	48
Telemetry collections.....	49
Analytics telemetry.....	49
View or download collections.....	50
Configuration viewer.....	50
Items reported in periodic collections from servers.....	50
Manually initiate a collection.....	52
Manually upload collection.....	53
Chapter 11: Extensions.....	54
Adapters.....	54
Set up an OpenManage Enterprise adapter.....	54
Chapter 12: Audits.....	56
Chapter 13: Configuring Secure Connect Gateway settings.....	57
Configure contact information.....	57
Configuring your environment.....	57
Configure SMTP server settings.....	58
Configure proxy server settings.....	59
Configure Policy Manager settings.....	60

Enable VMware tools.....	60
Manage Certificates.....	61
Configure SNMP v3 settings.....	61
Enable two-factor authentication.....	62
Enable custom Pre-login message.....	62
Configure telemetry settings.....	63
Configure email notifications.....	64
Types of email notifications.....	64
Request gateway health status through an email.....	66
Configure API settings.....	66
Configure alert delivery settings.....	67
Configure automated tasks.....	67
User Management and LDAP configuration.....	68
Local Users Management.....	68
LDAP Users Management.....	70
Configure update settings.....	71
Configure LDAP settings.....	72
Configure backup settings.....	73
Configuring Syslog Server for Secure Connect Gateway.....	74
Chapter 14: Configuring alert and event settings.....	77
Manually configure alert destination of a networking device.....	77
Manually configure alert destination using the script file for a server running Linux operating system.....	77
Install Net-SNMP on a server running Linux operating system.....	78
Manually configure alert destination by accessing the SNMP trap service for a server running Linux operating system.....	78
Chapter 15: Updating Secure Connect Gateway.....	79
Install hotfix updates.....	79
Update Host OS Patch update- when available.....	79
Upgrade to SUSE Linux Enterprise Server 15.....	79
Update Secure connect gateway for appliance.....	80
Update Secure connect gateway for Docker and Podman.....	80
Update Secure connect gateway for Kubernetes.....	81
Chapter 16: Secure Connect Gateway resources.....	82
Chapter 17: Contacting Dell Technologies.....	83

Introduction

Secure connect gateway is an enterprise monitoring technology that is delivered as an appliance and a stand-alone application. It monitors your devices and proactively detects hardware issues that may occur on your device. Depending on your service contract, it also automates support request creation for issues that are detected on the monitored devices. See [Secure Connect Gateway capabilities available with Dell Technologies service contracts](#).

Supported products include Dell server, storage, chassis, networking, data protection devices, virtual machines, and converged or hyperconverged appliances.

Based on the device type and model, secure connect gateway automatically collects the telemetry that is required to troubleshoot the issue that is detected. The collected telemetry helps technical support to provide a proactive and personalized support experience. For information about the telemetry collected, see the *Secure Connect Gateway 5.x — Virtual Edition Reportable Items* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

Version

The **Gateway version** displayed on the **About** page indicates the secure connect gateway version that is installed or deployed on the local system. The version number contains the following components—major release number, minor release number, service pack number, and build number.

For example, if the **Gateway version** displayed is 5.01.03.25:

- 5 indicates the major release number.
- 01 indicates the minor release number.
- 03 indicates the service pack number.
- 25 indicates the build number.

Release history

The following table lists the released secure connect gateway — virtual edition versions:

Table 1. Released versions

Version	Release date
5.30.00.14	June 24, 2025
5.28.00.14	February 24, 2025
5.26.00.20	November 7, 2024
5.26.00.18	October 15, 2024
5.24.00.14	June 10, 2024
5.22.00.18	February 26, 2024
5.20.00.10	November 6, 2023
5.18.00.20	September 18, 2023
5.16.00.14	May 23, 2023
5.14.00.16	February 13, 2023
5.14.00.12	December 6, 2022
5.14.00.10	November 8, 2022
5.12.00.10	July 25, 2022

Table 1. Released versions (continued)

Version	Release date
5.10.00.10	March 9, 2022

Document purpose

This document provides information about the minimum system and network requirements, and features available in secure connect gateway. For information about other documents available for secure connect gateway, see [Secure Connect Gateway resources](#).

In this document, the term local system refers to the secure connect gateway virtual appliance; remote device refers to device in your environment; backend refers to Dell Technologies.

Supported languages

The secure connect gateway user interface supports seven languages—Simplified Chinese, English, French, German, Japanese, Brazilian Portuguese, and Spanish.

However, secure connect gateway sends email notifications in the following languages: Arabic, Bahasa Indonesia, Simplified Chinese, Traditional Chinese, Czech, Danish, Dutch, English, Finnish, French, Canadian French, German, Greek, Hebrew, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Brazilian Portuguese, Russian, Slovak, Spanish, Latin American Spanish, Swedish, Thai, or Turkish.

Secure Connect Gateway capabilities available with Dell Technologies service contracts

The following table provides a comparison of the secure connect gateway capabilities available with the Basic Hardware, ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contracts.

Table 2. Secure connect gateway capabilities by service contract type

Capability	Description	Basic Hardware	ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center
Automated service request creation	For devices with Basic support contracts, a service request is created, and you are notified to contact technical support to initiate issue resolution. For all ProSupport contracts, when a failure is detected, a service request is automatically created with technical support. The technical support team contacts you for remote resolution.	Supported	Supported
Telemetry collections	System state telemetry that is required to troubleshoot issues is collected from managed devices and securely sent to Dell Technologies.	Supported	Supported
Proactive action from technical support	A technical support agent proactively contacts you about the service request and helps resolve the issue.	Not supported*	Supported
Proactive parts dispatch	If an issue is detected in your hardware and requires a replacement to resolve the issue, a service request is created for a replacement. The replacement part is dispatched based on your dispatch preferences.	Not supported	Supported

Table 2. Secure connect gateway capabilities by service contract type (continued)

Capability	Description	Basic Hardware	ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center
Predictive detection of hardware failures	Dell Technologies provides predictive detection of hardware failures for servers. If an issue is detected in your hardware and requires a replacement to resolve the issue, a service request is created for a replacement. The replacement part is dispatched based on your dispatch preferences.	Not supported	Supported

* If you have a Basic service contract, you receive an email notification containing case details when an issue occurs. To address the issue, you must contact Dell technical support. The email includes information about your service request and a reference number that you can provide during your call with support.

Device types and supported features

The following table provide information about the device types supported, features available, and tasks that can be performed using secure connect gateway.

Table 3. Device types and supported features

Device type or model	Products requiring credentials for device discovery	Devices supported through the adapter connection with OpenManage Enterprise	Auto-configuration of alert and event settings	Inventory devices through deep discovery	Uses Policy Manager for advanced control	Enable or disable device level maintenance mode	Automatic creation of service request	Initiate, upload, and configure telemetry collection
Server or hypervisor and iDRAC	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Chassis	Supported	Supported	Not supported	Supported	Not supported	Supported	Supported	Supported
PowerSwitch and Dell networking switches	Supported	Supported	Not supported	Supported	Supported	Supported	Supported	Supported
PowerConnect and Force10 switches	Supported	Supported	Not supported	Supported	Not supported	Supported	Supported	Supported
PowerSwitch with Enterprise SONiC	Supported	Not supported	Supported	Not supported	Supported	Supported	Supported	Supported
Brocade or Cisco switches	Supported	Not supported	Not supported	Supported	Supported	Not supported	Supported	Supported
Software	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
EqualLogic or PS series	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
PowerVault MD3 series	Not supported	Supported	Not supported	Supported	Not supported	Supported	Supported	Supported
PowerVault MD2400 series*	Supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported	Not supported
PowerVault ME4 series	Supported	Supported	Not supported	Not supported	Not supported	Supported	Supported	Supported
PowerVault ME5 series	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported	Not supported
Compellent or SC series	Supported	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Network Attached Storage (NAS)	Supported	Supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported
PowerVault tape libraries	Supported	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported

Table 3. Device types and supported features (continued)

Device type or model	Products requiring credentials for device discovery	Devices supported through the adapter connection with OpenManage Enterprise	Auto-configuration of alert and event settings	Inventory devices through deep discovery	Uses Policy Manager for advanced control	Enable or disable device level maintenance mode	Automatic creation of service request	Initiate, upload, and configure telemetry collection
Other supported data storage model. For example, PowerMax, Unity, PowerStore, XtremIO	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported	Not supported
WebScale	Supported	Supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported
Other supported Converged or Hyper-Converged Infrastructure appliances. For example, VxRail, PowerFlex, VxBlock	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported	Not supported
Virtual machine	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Data Protection	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported	Not supported
Direct Liquid Cooling	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Connectrix DS-7710B	Supported	Not supported	Not supported	Not supported	Supported	Supported	Supported	Supported

* These devices are discovered through the host server for all their operations.

New and enhanced features


This section provides information about the new and enhanced features in the current and previous releases of secure connect gateway.

v5.30.00.14


- Ability to create a custom pre-login message banner.
- Ability to integrate HashiCorp vault credentials with the gateway.
- Support updating friendly names for devices via the REST API.
- Retrieve user IDs from secure connect gateway using REST API.
- Introduced the option to download and install the previous version (N-1) in the gateway.
- Ability to store secure connect gateway proxy credentials in an external credential vault.
- Ability to view, solution based products in the Consolidated View page.
- Added support for:
 - iDRAC firmware version 7.10.20.05 with 15th and 16th generation PowerEdge servers.
 - iDRAC firmware version 7.10.20.50 with 15th and 16th generation PowerEdge servers.
 - iDRAC firmware version 7.20.10.05 on 15th and 16th generation PowerEdge servers.
 - DRAC firmware version 7.20.30.50 on 15th and 16th generation PowerEdge servers.
 - DRAC firmware version 1.20.25.00 on 17th generation PowerEdge servers.
 - iDRAC firmware version 7.10.90.00 on AX-660 and AX-760.
 - Enterprise SONiC operating system 4.4.1 on S5212F-ON, S5224F-ON, S5232F-ON, S5248F-ON, S5296F-ON, and S5448F-ON.
 - OpenManage Enterprise version 4.3.2, 4.2, and 4.1.

v5.28.00.14

- Ability to:
 - Integrate Syslog Server for a secure connect gateway.
 - Add Role Based Access management users which can integrate with your LDAP configuration.
 - Update SUSE Linux Enterprise Server 15 SP6 Host OS.

 **NOTE:** When upgrading to 5.28 for VMware, Microsoft Hyper-V, or KVM versions the SLES Linux Enterprise OS will be updated to version 15 SP6.

- Install on demand Host OS patch update.

 **NOTE:** More frequent SLES Host OS updates for Virtual Appliance customers running VMware, Microsoft Hyper-V, or KVM systems. This is not applicable for the container edition users.

- Automatically apply any available hotfixes when updating the gateway from a lower version to the latest version.
- Ability to deploy the gateway to an OpenShift platform.
- Ability to deploy the gateway as a Kernel-based Virtual Machine (KVM) hypervisor.
- Added support for:
 - Azure 23H2 OS version 7.10.30.00 on 15th generation AX nodes.
 - Azure 23H2 OS version 7.00.00.00 on 14th generation AX nodes.
 - iDRAC firmware version 7.10.70.00 on 15th and 16th generation PowerEdge servers.
 - iDRAC firmware version 7.10.90.00 on 15th and 16th generation PowerEdge servers.
 - iDRAC firmware version 7.00.00.174 on 14th generation PowerEdge servers.
 - iDRAC firmware version 7.10.77.00 on XE9680L.
 - iDRAC firmware version 7.10.50.07 and 7.10.70.00 on XE9680.

- Enterprise SONiC operating system 4.4.0 on S5296F.
 - Connectrix DS-7710B.
 - SNMP v3 Authentication type SHA512.
- Discontinued support for the account integration of TechDirect with secure connect gateway.

NOTE: If users have configured TechDirect in a previous version, they will notice that TechDirect is removed after they upgrade to version 5.26.00.18. As a result, the TechDirect account information is no longer available in the secure connect gateway system. However, PowerEdge servers continue to create cases and send parts for any issues that arise. During the upgrade, a banner appears to inform users about the removal of the TechDirect integration. For more information, click [here](#).

- Enhancements and bug fixes.

v5.26.00.20

- Resolves an issue in version 5.26.00.18 with Alert Delivery (Call Home) impacting products including Elastic Cloud Storage (ECS), XtremIO, and Switch-Brocade-B models. Click [here](#) for more details.
- Includes all enhancements for version 5.26.00.18, as detailed in the section titled V.5.26.00.18 below.

5.26.00.18

- Integrated secure connect gateway with the Azure credential vault.
- Support for **STARTTLS** for SMTP configuration to securely connect to secure connect gateway.
- Ability to backup credentials on the chosen credential vault.
- Enabled account lockout if the wrong RSA passcode is entered five times consecutively.
- Ability to change secure connect gateway username using a CLI script.
- Enabled device block capability for non-root Podman and Kubernetes containers to prevent spamming of secure connect gateway with data item service requests from the device.
- Added support for:
 - iDRAC9 firmware version 7.10.50.05 on XE9680.
 - iDRAC9 firmware version 7.10.50.00 on AX-760, AX-4510C, and AX-4520C.
 - iDRAC9 firmware version 6.10.85.00 on XC760-24N.
 - iDRAC9 firmware version 7.00.60.00 on XC4510c.
 - iDRAC9 firmware version 7.10.30.00 on XC4520c and XC760xd2.
 - iDRAC9 firmware version 7.10.50.00 on XC7625-24N.
 - iDRAC9 firmware version 7.10.30.00 on XR8610t and XR8620t.
 - Enterprise SONiC operating system 4.2.1 on E3248P-ON, E3248PXE-ON, and S5296F-ON PowerSwitch switches.
 - Firmware version GT280R014-01 for ME4012, ME4024, and ME4048.
- Discontinued support for:
 - SNMPv1 for alerts and events.
 - Port 8443 for inbound communication to secure connect gateway.
- Enhancements and bug fixes.


v5.24.00.14

- Integrated secure connect gateway with the credential vault, CyberArk Credential Provider.
- Two-factor authentication with RSA SecurID to log in to secure connect gateway.
- Ability to configure iSM for automatic case creation.
- Availability of hotfix updates for appliance, Docker, and Podman.
- Ability to run the container version of secure connect gateway on Microsoft Azure.
- Enabled notifications to inform customers that disk space is 90% full.
- Enabled device block capability to prevent spamming of secure connect gateway with data item service requests from the device.
- Added support for:

- iDRAC9 firmware version 7.10.50.00 on 15th and 16th generation PowerEdge servers.
- iDRAC9 firmware version 7.10.45.00 on T160 and R260.
- iDRAC9 firmware version 7.00.60.00 on XC760xa.
- iDRAC9 firmware version 7.10.30.00 on XC660xs.
- PowerVault MD2400.
- Operating system 10.5.6.1 for E3224F-ON PowerSwitch switch.
- Enterprise SONiC operating system 4.2.0 for E3248PXE PowerSwitch switch.
- Operating system 10.5.6.1 for MX9116n and MX5108n Dell Force10 switches.
- SUSE Linux Enterprise Server 15 SP6 operating system on managed devices.
- Red Hat Enterprise Linux versions 8.10 and 9.4 operating systems on managed devices.
- Ubuntu 24.04 operating system on managed devices.
- Enhancements and bug fixes.

v5.22.00.18

- Added support for Enterprise SONiC operating system for Dell PowerSwitch switches.
- Ability to integrate secure connect gateway with credential vault for remote support activities.
- Ability to enable or disable SNMP and Redfish listening services in alert delivery settings.
- Automatic deletion of Redfish subscription in iDRAC when iDRAC is deleted from secure connect gateway.
- Availability of the online update for Docker and Podman containers.

 **NOTE:** The online update is not available for non-root, IPV6 Podman containers.

- Discontinued support for TLS 1.0 and 1.1.
- Added support for:
 - iDRAC9 firmware version 7.10.30.00 on 14th and 15th generation PowerEdge servers.
 - iDRAC9 firmware version 2.85.85.85 on 13th generation PowerEdge server.
 - Azure 22H2 OS 7.00.00.00 on 14th generation AX nodes.
 - Azure 22H2 OS 7.00.30.00 on 15th generation AX nodes.
 - Operating system 10.5.6.0 for S and Z series PowerSwitch switches.
 - Enterprise SONiC operating system 4.2.0 for S and Z series PowerSwitch switches.
 - OpenManage Enterprise version 4.0.
 - Red Hat Enterprise Linux versions 8.9 and 9.3 operating systems on the managed devices.
 - ESXi 8.0 U2 and U3 operating systems on managed devices.
- Enhancements and bug fixes.

v5.20.00.10

- Integrated secure connect gateway with the credential vault, CyberArk with Conjur API.
- Enabled on-premise support for TLS 1.3 connections.
- Ability to schedule gateway health checks.
- Introduced the ability to bundle and download all log files for troubleshooting.
- Added support for CIFS share type in backup and restore feature.
- Added support for:
 - iDRAC9 firmware version 7.00.60.00 on 16th generation and 15th generation PowerEdge servers.
 - iDRAC9 firmware version 7.00.55.00 on C6615.
 - iDRAC9 firmware version 7.00.45.00 on R360 and T360.
 - iDRAC9 firmware version 7.00.30.00 on XE8640, XE9680, XR5610, XR8610t, and XR8620t.
 - Operating system 10.5.5.3 for S and Z series PowerSwitch switches.
 - Operating system 10.5.5.3 for N3248TE, S5448F, and Z9432F PowerSwitch switches.
 - Red Hat Enterprise Linux versions 8.7 operating system on the managed devices.
 - Dell Data Analytics Engine
- Discontinued support for NFS share type for MX7000 export and application logs.
- Enhancements and bug fixes.
- Includes the following fixes from the 5.18 Host OS patch update 10:

- PowerScale data items API calls show as failed after secure connect gateway upgrade to version 5.18.
- When the remote support on the **Remote access** tab remains unchanged or displays an incorrect value.

v5.18.00.20

- Enabled support for SNMP v3.
- Enabled a 24-hour lock period if the wrong username and password is entered in curl commands while resetting the password for security purposes.
- Backup and restore capability to schedule and create on-demand backup of secure connect gateway system information.
- Enabled automatic clearing of data collection tasks that were unresponsive for seven days.
- Added memory partitioning for containers to avoid out-of-memory conditions.
- Added support for:
 - iDRAC9 firmware version 7.00.30.00 on 16th generation and 15th generation PowerEdge servers.
 - iDRAC9 firmware version 7.00.00.00 on 16th generation, 15th generation, and 14th generation PowerEdge servers.
 - iDRAC9 firmware version 7.00.39.00 on XE9640.
 - iDRAC9 firmware version 7.00.35.00 on C6615.
 - iDRAC9 firmware version 6.10.85.00 on XR4510c and XR4520c.
 - iDRAC9 firmware version 6.10.43.00 on XR8620t.
 - iDRAC9 firmware version 6.10.39.00 on C6620, MX760c, R660, and R760.
 - iDRAC9 firmware version 6.00.49.00 on XR4510c and XR4520c.
 - Operating system 10.5.5 for S and Z series PowerSwitch switches.
 - Operating system 6.6.3.6 for PowerSwitch switch model N3224T-ON.
 - Red Hat Enterprise Linux versions 8.8, 9.1, and 9.2 operating systems on the managed devices.
 - SUSE Linux Enterprise Server 15 SP5 operating system on the managed devices.
 - Dell OpenManage Server Administrator version 11.0.1.
 - Direct liquid cooling device CHx80.
 - Port 8080 for APEX Navigator for Multicloud Storage
- Removed root access requirement for registration.
- Removed support for Skyline.
- Enhancements and bug fixes.
- Fixes available when you apply OS Patch: 10 on 5.18:
 - PowerScale data items API calls show as failed after secure connect gateway upgrade to version 5.18.
 - When the remote support on the **Remote access** tab remains unchanged or displays an incorrect value.

v5.16.00.14

- Support to deploy secure connect gateway using Docker, Podman, and Kubernetes containers.
- Complete support for IPV6.
- Improvements to error messages that may occur while configuring proxy server settings.
- Complete support for Dell ML3 tape libraries.
- Removed the option to enter a root password during the secure connect gateway registration.
- Added support for:
 - iDRAC9 firmware version 6.10.25.00 for XR5610 and XR7620.
 - iDRAC9 firmware version 6.10.29.05 for HS5610, HS5620, R660xs, and R760xs.
 - iDRAC9 firmware version 6.10.35.00 for XE9680.
 - iDRAC9 firmware version 6.10.39.00 for C6620.
 - iDRAC9 firmware version 6.10.47.00 for XE8640.
 - iDRAC9 firmware version 6.10.55.00 for R760xd2, R860, R960, and T560.
 - iDRAC9 firmware version 6.10.75.00 for R760xa.
 - Operating systems 10.5.3.x and 10.5.4.x for PowerSwitch switches.
 - ESXi 8.0 and Windows 2022 operating systems on managed devices.
 - Azure 22H2 OS node.
- Enhancements and bug fixes.

v5.14.00.10

- Enable or disable Dell technical support agent to remotely initiate collections on PowerEdge servers and PowerSwitch switches.
- Enable remote access only for PowerEdge servers and PowerSwitch switches from the secure connect gateway user interface.

NOTE: You can manually enable remote access only for PowerSwitch switches running OS 10.5.2 or lower. For PowerSwitch switches running OS 10.5.3.x or later, remote access is automatically enabled. Also, switches running OS 10.5.3.x or later must be added to secure connect gateway by configuring the device to connect to the Dell backend through a secure connect gateway instance unlike switches running OS 10.5.2 or lower that must be added from the secure connect gateway user interface.

- View the heartbeat status of the secure connect gateway virtual appliance through port 443.
- View banners on the secure connect gateway user interface to notify about new features, bug fixes, support for new device models or firmware, and so on.
- Delete a collection from the secure connect gateway user interface manually.
- View the metadata collected during periodic collections.
- Configure secure connect gateway to collect telemetry on a weekly basis.
- Schedule the interval in which the collected telemetry must be purged.
- Information about configured witness nodes on an iDRAC is included in a collection.
- The serial number of the secure connect gateway virtual appliance is automatically populated when you select **Customer Management Station** as the storage type.
- Added support for:
 - Dell OpenManage Server Administrator version 10.3.
 - Red Hat Enterprise Linux versions 8.5, 8.6, and 9.0 operating systems on the managed devices.
 - VMware ESXi 8.0 operating system on the managed devices.
 - Ubuntu 22.04 operating system on the managed devices.
 - iDRAC firmware versions 5.10.50.00 and 6.00.02.00.
 - S5000 series servers.
- Bug fixes.

v5.12.00.10

- Added support for:
 - FN410T, FN410S, and FN2210S switches.
 - iDRAC9 firmware versions 5.10.10.00 and 5.10.30.00 on 15th generation and 14th generation PowerEdge servers.
 - iDRAC8 with Lifecycle Controller version 2.83.83.83 on 13th generation PowerEdge servers.
 - Ubuntu 20.04.4 operating system on managed devices.
 - Dell ML3 tape libraries.


NOTE: Remote monitoring and service request creation capabilities are not available for Dell ML3 tape libraries.

- OpenManage Enterprise 3.9.
- Retired support for:
 - VMware vSphere ESXi 6.0
 - Disk Library Mainframe (DLm) series 1 and 2
 - DSSD
 - VMwCloudVxRail
 - Dell EMC Symphony
 - GeoNas
 - Invista
 - PowerOne Controller
- Ability to select the client TLS protocol for outbound TLS sessions from secure connect gateway to your devices or components, such as LDAP server, SMTP server, iDRAC devices and so on.
- Display information about other gateways in the cluster to which the virtual appliance is associated.

- Renamed **Cases** to **Service requests**.
- User interface improvements and bug fixes.

v5.10.00.10

- Display list of services and their running status and description on the **Network and service connectivity** page.
- Rebranded PowerVault to PowerVault MD3 and ME4.
- Receive alert and event information using Redfish protocol from iDRAC9 devices running firmware version 5.x or later.

 **NOTE:** If Redfish protocol is disabled, SNMP protocol is used to receive the alert and event information.


- Ability to configure security certificates to securely access secure connect gateway through port 5700.
- Ability to enable common name and certificate authority checks while setting up an adapter.
- Ability to update secure connect gateway.
- Ability to collect application logs from MX7000 devices.
- Added support for:
 - OpenManage Enterprise version 3.8.2 and 3.8.3
 - XC450 and XC7525 appliances
 - Firmware version 5.00.10.20
- Retired support for the following hypervisors:
 - ESX 4.0 and 4.1 U3
 - ESXi 4.0, 4.0 U3, 4.1, 4.1 U3, 5.0, 5.0 U3, 5.1, 5.5 U1, 5.5 U2, 5.5 U3, 6.0, 6.0 U1, 6.0 U2, and 6.0 U3
 - Citrix XenServer 6.0, 6.2, 6.5, 7.0, 7.1 LTSR CU2, and 7.2
- Retired support for the following operating systems running on the local system:
 - Windows 2008 Small Business Server
 - Windows 2011 Small Business Server
 - SUSE Linux Enterprise Server 12, 12 SP1, and 12 SP2
 - Debian 8.x and 9.x
- User interface and performance enhancements.
- Bug fixes.

Dashboard

After you deploy, register, and log in to secure connect gateway, you can start managing your devices on the user interface. For more information about deploying and registering secure connect gateway, see the *Secure Connect Gateway 5.x — Virtual Edition Deployment Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

When you log in to secure connect gateway, the dashboard is displayed. The dashboard provides an overall view of the health and connectivity status of your devices and environment. The dashboard contains the following panes or information:

- **Open service requests**—displays the number of open service requests for the devices in your environment. Click the number of requests to go to the **Service requests** page. See [Service requests](#).
- Percentage of memory and processor that is used and the amount of free space available in your server.
- **Device overview**—displays the total number of devices in **Managed**, **Staging**, **Inactive**, and **Not managed** states. To view the reason and resolution for the devices in the **Staging** state, click **Staging** and then click **Export** to save the information as a CSV file.
- Number of active remote sessions running on your devices.
- Overall connectivity status of secure connect gateway. If the status is displayed as **OFF**, see the *Secure Connect Gateway Virtual Edition Troubleshooting Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page, for steps to resolve the issue.
- **Network resources**—displays the number of connected and disconnected Enterprise servers, heartbeat connection status, and the configuration status of your SMTP server and Policy Manager. To test the heartbeat connection status through port 443 and verify the connectivity to the Enterprise servers, click **Test connection**.


 **NOTE:** By default, secure connect gateway verifies the heartbeat status every 24 hours.

To configure your SMTP server and Policy Manager, see [Configuring your environment](#).

- **Site inventory validation status**—displays the number of devices on which the connectivity capability, collection capability, and monitoring capability or heartbeat status of the devices were validated successfully or failed. See [Inventory validation](#). The **Others** column displays the following:
 - Number of devices on which validation was not performed.
 - Number of devices on which the validation is not supported.
 - Number of devices on which monitoring is disabled.
 - Number of devices inventoried through an adapter on which monitoring was successful.
 - Number of devices on which the capability could not be verified.
 - Number of devices that are offline.
- **Services**—displays the number of services that are running or stopped. Click **Stopped services** to view the names of the services that are not running.

Network and service connectivity

The **Network connections and services** page displays the connectivity status of the Global access and Enterprise servers and the heartbeat status of the secure connect gateway virtual appliance through port 443. The possible statuses are **Connected** and **Disconnected**. By default, secure connect gateway verifies the heartbeat status every 24 hours.

 **NOTE:** The heartbeat connection indicates the connectivity status between the secure connect gateway virtual appliance and the Dell backend.

To go to the page, click **Connectivity** in the header and then click **Network connections and services**. You can click **Test connection** to verify connectivity to the Global access servers, Enterprise servers, and the Dell backend.

The **Service status** section lists the names, running status, and description of the services running in the backend. If the **Stopped** status is displayed for a service, see the *Secure Connect Gateway Virtual Edition Troubleshooting Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page to resolve the issue.


Devices

The **Devices** page displays the following information about all the devices that are added in secure connect gateway:

- Name, hostname, or IP address depending on the information you have provided for the device.

NOTE: If the device supports remote access, but it is not enabled on the device, the IP address is not retrieved and a link to add a name is displayed.

- Model of the device, for example, PowerEdge M820
- Service Tag or serial number of the device
- Inventory validation status.
 - Success—displayed if connectivity, collection capability, monitoring capability, remote access enablement, as applicable are successful.
 - Success with warnings—displayed if remote access is disabled on the device.
 - Failed—displayed if connectivity, collection capability, or monitoring capability are unsuccessful.
 - Blocked—displayed if the device is blocked due to excessive Dataltem service request volume or API usage.

If a device and its associated devices are added in secure connect gateway,  is displayed beside the name or IP address of the primary device. Click the device to view the list of associated devices in the device overview pane.

After you add your devices, you can perform the following tasks from the **Devices** page:

- Filter the devices based on type, device group, mode in which the devices were added, and inventory validation status.
- Edit a device name and account credentials.
- Perform inventory validation. See [Inventory validation](#).
- Initiate a single or multiple device collection. See [Manually initiate a collection](#).
- Assign a credential profile to one or more devices. See [Assign a credential profile](#).
- Delete a device.


NOTE: Devices that are inventoried and added in secure connect gateway through an adapter cannot be deleted. Those devices are deleted automatically when either the adapter is deleted or the devices are removed from the systems management console. If you add a device to secure connect gateway using the RESTful protocol, you must disable it from the device user interface.

- Export the information that is displayed on the page as an XLS file.
- Clear System Event Logs (SEL) or hardware logs, also known as the Embedded System Management (ESM) logs that report potential hardware issues in PowerEdge servers. You can run this task when an error message is displayed on a server even after the problem is resolved or when an SEL full error message is displayed.


CAUTION: Clearing SEL removes the event history of the server.

NOTE: The **Clear System Event Logs** task is disabled if the device was added as a server or hypervisor and OMSA was not installed on the device.


- Check for service requests created for the device.
- Discover associated devices through deep discovery. See [Deep discovery](#).
- Enable or disable device-level maintenance mode. For more information about maintenance mode, see [Maintenance mode overview](#).
- Configure alert and event settings to set the alert destination of a device and ensure that the alerts from the device are forwarded to the local system. Secure connect gateway cannot automatically configure the alert and event settings of a device running the following operating system or hypervisor:
 - Oracle Enterprise Linux
 - VMware ESXi
 - Oracle Virtual Machine

 **NOTE:** If secure connect gateway does not support the configuration of alert and event settings on the device, the option is disabled.

- Enable or disable device monitoring.
- Manually enable or disable remote access. See [Enable or disable remote access](#).

 **NOTE:** You can manually enable or disable remote access only for PowerEdge servers and PowerSwitch switches from the secure connect gateway user interface.

- Enable iSM for automatic case creation. iSM can be used as a default case creation service for 14th generation PowerEdge servers or later.
- Unblock blocked devices. If the device is temporarily blocked, it is automatically unblocked after two hours. If the device is permanently blocked, you can unblock the device from the **Tasks** pane. You can enable email notifications to receive information about blocked devices on the **Email notifications** page.

 **NOTE:**

- The device block capability is available only for appliance, Docker, and Podman root devices.
- Devices that are temporarily blocked are highlighted in yellow in the **Status** column of the **Devices** page. Devices that are permanently blocked are highlighted in red in the **Status** column of the **Devices** page.


When you click a device in the **Name / IP Address** column, the device overview pane is displayed. Depending on the device type, the device overview pane displays the following information is displayed in the device overview pane:

- Hostname or IP address of the device
- Operating system running on the device
- Device model number
- Service Tag assigned to the device
- Connectivity status of the device. The following statuses may be displayed:
 - If remote access is supported on the device: **Connected** or **Disconnected**.
 - If remote access is not supported on the device: **Remote access not supported**.
- Heartbeat status of the device received through the `keepalive` service.
- Software or firmware version running on the device
- Display name configured for the device
- Device type
- iSM version
- iSM service status
- iSM prerequisites set
- Timestamp of the next scheduled collection
- Status of the previous job

The device overview pane also displays the collections that were performed on the device and enables you to perform the following tasks:

 **NOTE:** Only the tasks applicable for the device are enabled.

- Edit the device details.
- Delete the device.

 **NOTE:** Devices that are inventoried and added in secure connect gateway through an adapter cannot be deleted. Those devices are deleted automatically when either the adapter is deleted or the devices are removed from the systems management console. If you add a device to secure connect gateway using the RESTful protocol, you must disable it from the device user interface.

- Clear System Event Logs (SEL) or hardware logs, also known as the Embedded System Management (ESM) logs that report potential hardware issues in PowerEdge servers. You can run this task when an error message is displayed on a server even after the problem is resolved or when an SEL full error message is displayed.

 **CAUTION:** Clearing SEL removes the event history of the server.

NOTE: The **Clear System Event Logs** task is disabled if the device was added as a server or hypervisor and OMSA was not installed on the device.

- Check for service requests created for the device.
- Discover associated devices through deep discovery. See [Deep discovery](#).
- Enable or disable device-level maintenance mode. For more information about maintenance mode, see [Maintenance mode overview](#).
- Configure alert and event settings to set the alert destination of a device and ensure that the alerts from the device are forwarded to the local system. Secure connect gateway cannot automatically configure the alert and event settings of a device running the following operating system or hypervisor:
 - Oracle Enterprise Linux
 - VMware ESXi
 - Oracle Virtual Machine


NOTE: If secure connect gateway does not support the configuration of alert and event settings on the device, the option is disabled.


- Enable or disable device monitoring.
- Enable iSM for automatic case creation. iSM can be used as a default case creation service for 14th generation PowerEdge servers or later.

NOTE: Configuring iSM is not supported on devices that connect to secure connect gateway through an adapter.

- Manually enable or disable remote access. See [Enable or disable remote access](#).

NOTE: You can manually enable or disable remote access only for PowerEdge servers and PowerSwitch switches from the secure connect gateway user interface.

When a task is performed on a device,  is displayed beside the name or IP address of the device. You can initiate more than one task for a device. When you hover over the device, the task in progress is displayed.

Click  to view the number of active remote sessions running on your devices, number of active file transfers running for your devices, and the overall connectivity status secure connect gateway.

Methods of adding devices

You can add devices in secure connect gateway by using one of the following methods:

- Add each device individually by entering the details of the device.
- Add devices based on a specific IP address range. See [Device discovery rules](#).
- Inventory and add devices that are managed by system management consoles. See [Adapters](#).
- Configure the device to connect with secure connect gateway directly. After you configure, the device details are automatically displayed in secure connect gateway. For more information, see the device-specific documentation.

NOTE: If the SNMP and Redfish listener services are disabled, you cannot add device, device discovery rules, or adapters for servers and networking devices.

Some devices can be added from the secure connect gateway user interface or by configuring them to connect to secure connect gateway directly. If you add such a device from the secure connect gateway user interface, only limited capabilities are enabled for the device. For steps to configure the device, see the device-specific documentation.

The following table lists the device types or models by the method in which they can be added in secure connect gateway.

Table 4. Devices types or models and method of adding devices

Configure the device to connect to secure connect gateway through the device management software or using the CLI script	Add device from secure connect gateway user interface
AppSync	9th generation of PowerEdge servers and later
Avamar** (v19.10 and later)	Atmos
Cloud Array	Avamar** (versions earlier than 19.10)

Table 4. Devices types or models and method of adding devices (continued)

Configure the device to connect to secure connect gateway through the device management software or using the CLI script	Add device from secure connect gateway user interface
CloudBoost Virtual Appliance	Centera
CloudIQ Collector	Chassis
Connectrix** (v9.1.1 and later)	Connectrix** (versions earlier than 9.1.1)
Converged Management Software	Customer Management Station
Data Domain** (vDDOS6 and later)	Data Domain** (versions earlier than vDDOS6)
Data Protection Advisor	Data Computing Appliance
Data Protection Appliance	Dell Compellent
DatalQ	Dell Technologies Disk Library (EDL)
Dell Storage Resource Manager (SRM)	Disk Library (DL3D)
Dell InterConnect Fabric	Disk Library Mainframe (DLm) series 3
Dell ML3	EqualLogic
DellSvcs-Auth	Fluid File System
DellSvcs-Automate	HIT Kit/VSM for VMware
DellSVcs-Connector	iDRAC
DellSvcs-CPMS	Linux virtual machines
DellSvcs-Monitor	Networking
Elastic Cloud Storage (ECS)	PowerMAX/VMAX** (PowerMax 2000, PowerMax 8000, and VMAX3 series)
Enterprise Copy Data Management	PowerVault MD3 and ME4
Isilon or PowerScale	RecoverPoint
MetroNode or VPLEX	Switch Cisco
Networker	Symmetrix
ObjectScale	vCenter
PowerFlex Appliance	VNX
PowerFlex OS	VNXe
PowerFlex Rack	Web Scale
PowerMAX/VMAX** (PowerMax 2500 and PowerMax 8500)	XtremIO** (XMS code earlier than 6.4)
PowerMaxV4	-
PowerPath	-
PowerPath Management Appliance	-
PowerProtect Appliance	-
PowerProtect Data Manager	-
PowerScale SD	-
PowerStore*	-
PowerVault ME5	-
S5000 series servers	-
ScaleIO	-

Table 4. Devices types or models and method of adding devices (continued)


Configure the device to connect to secure connect gateway through the device management software or using the CLI script	Add device from secure connect gateway user interface
Streaming Data Platform	-
Switch Brocade	-
UCC	-
Unisphere	-
Unity	-
Unity VSA	-
VxRack SDDC	-
VxRail	-
XtremIO** (XMS code 6.4 and later)	-

*After the device is configured, enable remote access to manage the device using secure connect gateway. You can manage remote access permissions to the device using Policy Manager. For more information about the operations and configuration of Policy Manager, see the *Policy Manager for Secure Connect Gateway 5.x User's Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

Consolidated View


The **Consolidated View** page displays a grouped view of devices that share a common serial number, with or without a suffix. This view provides the following information for each group:

- **Name/IP Address and Service Tag/Serial Number:** Displays the group serial number that is used to associate the devices.
- **Device count:** The total number of devices in the group is shown in parentheses next to the serial number.
- **Expand/collapse icon:** A symbol (^) is provided to expand or collapse the list of grouped devices.
- **Status:** Shows a consolidated status based on the individual statuses of the devices in the group:
 - **Blocked (Red color):** Shown in red with status **Blocked**. This takes the highest priority and becomes the group status if any device is in a red **Blocked** state.
 - **Failed:** The group status is **Failed** if at least one device has a **Failed** status, unless a red **Blocked** status is present.
 - **Blocked (Yellow color):** Displayed in yellow with status **Blocked**. This becomes the group status if at least one device is in a yellow **Blocked** state and all other devices are either in **Warning** or **Success** status.
 - **Warning:** Group status is **Warning** if at least one device has **Warning** status and others are **Success**.
 - **Success:** Group status is **Success** if all devices have **Success** status.

 **NOTE:** The consolidated view is applicable to data storage and data protection devices.

The devices that are displayed in the Consolidated View show the following information:

- Name, hostname, or IP address depending on the information you have provided for the device.


 **NOTE:** If the device supports remote access, but it is not enabled on the device, the IP address is not retrieved and a link to add a name is displayed.

- Model of the device, for example, PowerEdge M820
- Service Tag or serial number of the device
- Inventory validation status.
 - Success—displayed if connectivity, collection capability, monitoring capability, remote access enablement, as applicable are successful.
 - Success with warnings—displayed if remote access is disabled on the device.
 - Failed—displayed if connectivity, collection capability, or monitoring capability are unsuccessful.
 - Blocked—displayed if the device is blocked due to excessive Data Item service request volume or API usage.


Add a chassis


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Chassis**.
3. Enter the hostname or IP address of the device.
4. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
5. To discover and add other devices that are associated with the primary device, select **Perform deep discovery**.
6. If the chassis is associated with iDRAC devices and you want the secure connect gateway to monitor these devices for hardware issues, and automatically configure their settings to receive alert traps or event subscriptions, select the **Enable and configure alerts** checkbox.
7. Perform one of the following steps:
 - If you enabled deep discovery, select a credential profile that you want to assign to the primary device and its associated devices. To create a new credential profile, click **Create profile**. See [Create a credential profile](#).
 - If you did not enable deep discovery, select an account credential that you want to assign to the device. To create an account credential, click **Create a new account**. See [Add account credentials](#).
8. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
9. If you do not want secure connect gateway to monitor the device for hardware issues, clear the **Enable monitoring** checkbox.

 **NOTE:** If monitoring is disabled, secure connect gateway does not create service requests for issues that are detected on the device. However, periodic collections are performed on the device.
10. Click **Next**.

Results


The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add an iDRAC

Prerequisites

- The device must be a 12th generation PowerEdge server or later (iDRAC7 or later).
- If the device connects to the Internet through a proxy server, ports 161 and 443 must be open on the proxy server firewall.
- For iDRAC7 or iDRAC8, Enterprise or Express license must be installed on the iDRAC.
- For iDRAC9, Basic, Enterprise, or Express license must be installed on the iDRAC.
- For iDRAC9 running firmware version 5.x or later, the Redfish protocol and port 5705 must be enabled on the device.

 **NOTE:** The Redfish protocol is used to receive the alert and event information from the device. However, if it is unable to configure using the Redfish protocol, SNMP is used to configure the settings.





- For iDRAC9 running firmware version 5.x or later, Redfish event notifications must be enabled on the device. For instructions on how to enable Redfish event notifications in the **Alerts configuration** section, see the *Integrated Dell Remote Access Controller User's Guide* available on the [iDRAC Manuals](#) page. You must enable all the individual component categories in the **Alerts configuration** section.

About this task


By default, SupportAssist is available on 14th generation PowerEdge servers. You can register SupportAssist on the server to receive the automated support capabilities of secure connect gateway. When you add an iDRAC in secure connect gateway,


the SupportAssist component is automatically disabled and automatic support capabilities are provided through secure connect gateway.

Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
 2. From the **Device type** list, select **iDRAC**.
 3. Enter the hostname or IP address of the device.
 4. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
 5. Select an account credential that you want to assign to the device. To create a new account credential, click **Create a new account**. See [Add account credentials](#).
-  **NOTE:** Create account credentials using an iDRAC user with Administrator user role.
6. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
 7. By default, **Enable and configure alerts and events** check box is selected. This enables secure connect gateway to monitor the device for hardware issues and automatically configure the device settings to receive the alert traps or event subscriptions. If you want to manually configure alert and event forwarding for the device, clear the **Enable and configure alerts and events** check box..
-  **CAUTION:** If the device alerts and event settings are not configured, secure connect gateway cannot monitor hardware issues that may occur on the device.
-  **NOTE:** On 15th generation PowerEdge servers, secure connect gateway configures the alert and event settings using the Redfish protocol. However, if it is unable to configure using the Redfish protocol, SNMP is used to configure the settings.
-  **NOTE:** If monitoring is disabled, secure connect gateway does not create service requests for issues that are detected on the device. However, periodic collections are performed on the device.
8. Click **Next**.

Results


The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.


Add a networking device


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Networking**.
3. Select one of the following from the **Operating System type** list:
 - Select **Enterprise SONiC** for SONiC operating system.

 **NOTE:** The minimum firmware version required to add Enterprise SONiC operating system is 4.2.0.


 - Select **Additional OS types** for all other operating systems.

 **NOTE:** To add the device Connectrix DS-7710B, choose **Device type** as **Networking** and Operating System type as **Additional OS types**.

 **NOTE:**


- To add Enterprise SONiC operating system on a PowerSwitch switch that is already discovered with OS10 on secure connect gateway, delete the PowerSwitch from secure connect gateway and add it again using SONiC OS credentials.
- If the PowerSwitch switch is not deleted and a manual or periodic inventory validation is run, the switch moves to staging.


4. Enter the hostname or IP address of the device.
5. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other devices that are associated with the primary device, select **Perform deep discovery**.
7. Perform one of the following steps:
 - If you enabled deep discovery, select a credential profile that you want to assign to the primary device and its associated devices. To create a new credential profile, click **Create profile**. See [Create a credential profile](#).
 - If you did not enable deep discovery, select an account credential that you want to assign to the device. To create an account credential, click **Create a new account**. See [Add account credentials](#).
8. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
9. If you do not want secure connect gateway to monitor the device for hardware issues, clear the **Enable monitoring** check box.

 **NOTE:** If monitoring is disabled, secure connect gateway does not create service requests for issues that are detected on the device. However, periodic collections are performed on the device.

10. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.


 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add a server or hypervisor

Prerequisites


- The device must be running a Linux, ESX, or ESXi operating system. For the list of supported Linux, ESX, and ESXi operating systems, see the *Secure Connect Gateway 5.x — Virtual Edition Support Matrix* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.
- If the device is running a Linux operating system, the unzip package must be installed on the local system.

About this task


 **NOTE:** If you want to add a 12th generation PowerEdge server or later with iDRAC7 or later installed, it is recommended that you add the device in secure connect gateway as an iDRAC device. See [Add an iDRAC](#).


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Server / Hypervisor**.
3. Enter the hostname or IP address of the device.
4. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
5. Select an account credential that you want to assign to the device. To create a new account credential, click **Create a new account**. See [Add account credentials](#).

 **NOTE:** You cannot add account credentials for a server or hypervisor running Windows operating system. For the list of supported operating systems, see the *Secure Connect Gateway 5.x — Virtual Edition Support Matrix* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.


6. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
7. By default, **Enable and configure alerts and events** check box is selected. This enables secure connect gateway to monitor the device for hardware issues and automatically configure the device settings to receive the alert traps or event subscriptions. If you want to manually configure alert and event forwarding for the device, clear the **Enable and configure alerts and events** check box.


 **CAUTION:** If the device alerts and event settings are not configured, secure connect gateway cannot monitor hardware issues that may occur on the device.

 **NOTE:** If monitoring is disabled, secure connect gateway does not create service requests for issues that are detected on the device. However, periodic collections are performed on the device.

8. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.


 **NOTE:** You can use other features in secure connect gateway during the device discovery process.


Add a software

Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Software**.
3. Select the type of software that you want to add in secure connect gateway.
4. Enter the hostname or IP address of the device.
5. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
6. Select an account credential that you want to assign to the device. To create a new account credential, click **Create a new account**. See [Add account credentials](#).
7. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
8. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.


Add a virtual machine


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **VirtualMachine**.

3. Enter the hostname or IP address of the device.
4. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
5. Select an account credential that you want to assign to the device. To create a new account credential, click **Create a new account**. See [Add account credentials](#).
6. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
7. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add a converged or hyperconverged infrastructure appliance


Prerequisites


Ensure that the device model can be added from secure connect gateway user interface. For information about the device models that can be added, see [Methods of adding devices](#).

Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Converged/Hyper-Converged Infrastructure**.
3. Select the appliance model.
4. If you selected Web Scale, see [Add a Web-Scale appliance](#).
5. If you selected any other model, perform the following steps. For information about the other hyperconverged infrastructure appliance models that can be added from secure connect gateway, see [Methods of adding devices](#).
 - a. Enter the IP address and serial number of the device.
 - b. Select the device extension.
 - c. Click **Next**.

The device is discovered, and then the **Devices** page is displayed with the device details.

 **NOTE:** You cannot use other features in secure connect gateway during the device discovery process.

 **NOTE:** To enable remote support and remote actions capabilities for these models, configure the settings using Policy Manager or contact Dell technical support.


Add a Web-Scale appliance


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Hyper-Converged Infrastructure**.
3. Select the appliance model as Web-Scale.
4. Enter the hostname or IP address of the device.
5. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other devices that are associated with the primary device, select **Perform deep discovery**.
7. If you enabled deep discovery, select a credential profile that you want to assign to the primary device and its associated devices. To create a new credential profile, click **Create profile**. See [Create a credential profile](#).

8. If you did not enable deep discovery, select an account credential that you want to assign to the device. To create an account credential, click **Create a new account**. See [Add account credentials](#).
9. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
10. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add a data storage device


Prerequisites


Ensure that the device model can be added from secure connect gateway user interface. For information about the device models that can be added, see [Methods of adding devices](#).

Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Data Storage**.
3. Select the storage type.
If you select the **Customer Management Station**, the secure connect gateway serial number is automatically displayed.
4. To add an EqualLogic or PowerVault MD3 or ME4 device, see [Add an EqualLogic or PowerVault MD3 or ME4 device](#).
5. To add a Dell Compellent, Fluid FS, or a Dell ML3 tape library, see [Add a Dell Compellent, Fluid FS device, or a Dell ML3 tape library](#).
6. If you selected any other storage type, perform the following steps. For information about the other data storage models that can be added from secure connect gateway user interface, see [Methods of adding devices](#).
 - a. Enter the IP address and serial number of the device.
 - b. Select the device extension.
 - c. Click **Next**.

The device is discovered, and then the **Devices** page is displayed with the device details.

 **NOTE:** You cannot use other features in secure connect gateway during the device discovery process.

 **NOTE:** To enable remote support and remote actions capabilities for these models, configure the settings using Policy Manager or contact Dell technical support.


Add an EqualLogic or PowerVault MD3 or ME4 device


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Data Storage**.
3. Select the storage type.
4. Enter the hostname or IP address of the device.
5. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other devices that are associated with the primary device, select **Perform deep discovery**.
7. If you enabled deep discovery, select a credential profile that you want to assign to the primary device and its associated devices. To create a new credential profile, click **Create profile**. See [Create a credential profile](#).

8. If you did not enable deep discovery, select an account credential that you want to assign to the device. To create an account credential, click **Create a new account**. See [Add account credentials](#).
9. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
10. Click **Next**.


Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.


 **NOTE:** You can use other features in secure connect gateway during the device discovery process.


Add a Dell Compellent, Fluid FS device, or a Dell ML3 tape library

Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Data Storage**.
3. Select the storage type.
 **NOTE:** Remote monitoring and service request creation capabilities are not available for Dell ML3 tape libraries.
4. Enter the hostname or IP address of the device.
5. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
6. Select an account credential that you want to assign to the device. To create a new account credential, click **Create a new account**. See [Add account credentials](#).
7. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
8. Click **Next**.

Results


The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add a direct liquid cooling device


Steps


1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Direct Liquid Cooling**.
3. Enter the hostname or IP address of the device.
4. Optionally, enter a name for the device that can be used to represent the device in secure connect gateway. If you do not enter a name, the IP address or hostname is used to represent the device.
5. To create a new account credential, click **Create a new account**. See [Add account credentials](#).
6. Select a custom group to which you want to assign the device. If you do not select a custom group, the device is automatically assigned to the default device group. To create a new custom group, click **Create group**. See [Create a device group](#).
7. If you do not want secure connect gateway to monitor the device for hardware issues, clear the **Enable monitoring** check box.

 **NOTE:** If monitoring is disabled, secure connect gateway does not create service requests for issues that are detected on the device. However, periodic collections are performed on the device.

8. Click **Next**.

Results

The **Devices** page is displayed. If the device is discovered successfully through Redfish, a success message is displayed and the device details are displayed on the **Devices** page. Click  on the **Devices** page to view the device discovery progress or the error message if the device discovery failed.

 **NOTE:** You can use other features in secure connect gateway during the device discovery process.

Add a data protection device

Prerequisites


Ensure that the device model can be added from secure connect gateway user interface. For information about the device models that can be added, see [Methods of adding devices](#).


Steps

1. Go to **Device management > Manage devices > Devices > Add device**.
2. From the **Device type** list, select **Data Protection**.
3. Select the device model.
4. Enter the IP address and serial number of the device.
5. Select the device extension.
6. Click **Next**.

Results

The device is discovered, and then the **Devices** page is displayed with the device details.

 **NOTE:** You cannot use other features in secure connect gateway during the device discovery process.

 **NOTE:** To enable remote support and remote actions capabilities for these models, configure the settings using Policy Manager or contact Dell technical support.


Deep discovery

The deep discovery feature enables you to discover and add other devices that are associated with a primary device. To perform deep discovery, you must assign a credential profile. You can choose to perform deep discovery while discovering the primary device or after the primary device is discovered.

The following table lists the primary device and its associated devices that are discovered by deep discovery.

Table 5. Primary device and its associated devices discovered by deep discovery

Primary device	Associated devices discovered by deep discovery
Chassis	<ul style="list-style-type: none">• iDRAC 7 or later on modular servers• Networking switches
Storage PS Series group	<ul style="list-style-type: none">• Storage PS Series members• Storage PS Series FluidFS
Storage MD Series Enclosure	<ul style="list-style-type: none">• JBODs
Networking - management switch	<ul style="list-style-type: none">• Member switches
Web-scale appliance	<ul style="list-style-type: none">• Controller VM• Node (iDRAC / ESX)

 **NOTE:** On deep discovery of a chassis, networking devices associated with the chassis are also discovered. However, you can collect telemetry only from networking devices that are supported by secure connect gateway. For the list of supported networking devices, see the *Secure Connect Gateway 5.x — Virtual Edition Support Matrix* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

Maintenance mode overview

The maintenance mode functionality suspends the alert processing and automatic service request creation capability of secure connect gateway. If secure connect gateway receives 10 or more valid hardware alerts within one hour from a device, it automatically enables maintenance mode for the device. You can also manually enable the maintenance mode for all the monitored devices, for a specific device, or for devices in a custom device group.

The maintenance mode applies only to the following devices:

- Server or hypervisor and iDRAC
- Chassis
- PowerSwitch and Dell networking switches
- PowerConnect and Force10 switches
- PowerVault MD3 and ME4 series

 **NOTE:** Secure connect gateway sends events to the backend during maintenance mode though there is no automatic service request creation.


Global-level maintenance mode

Global-level maintenance mode suspends alert processing and automatic service request creation capabilities for all the monitored devices. During this mode, a yellow **Maintenance Mode** banner is displayed on top of the user interface.


To manually enable global-level maintenance mode, on the secure connect gateway header, click **Connectivity**, click **Toggle maintenance mode**, and then click **Turn on**.

Device-level maintenance mode

Device-level maintenance mode suspends alert processing and automatic service request creation capabilities for a specific device. If secure connect gateway receives 10 or more valid hardware alerts within one hour from a device, it automatically enables maintenance mode for the device. The device remains in maintenance mode for 30 minutes, enabling you to resolve the issue without creating additional service requests for the device. An email notification is also sent to the primary and secondary

contacts, and  is displayed beside the device on the **Devices** page. After 30 minutes, the device is automatically removed from maintenance mode, enabling secure connect gateway to resume normal alert processing for the device. If required, you can resume the maintenance mode for the device or disable it before 30 minutes.

To manually enable maintenance mode for a specific device, from the **Tasks** list in the device overview pane, click **Enable maintenance mode** and then click **Yes**.

 **NOTE:** If maintenance mode is manually enabled for a device, the device remains in maintenance mode even if global-level maintenance mode is enabled and then disabled during that time. If maintenance mode is automatically enabled for a device, the device remains in maintenance mode for 30 minutes even if the global maintenance mode is enabled and then disabled during that time.

Group-level maintenance mode

Group-level maintenance mode suspends alert processing and automatic service request creation capabilities for all the devices in a custom device group. After you enable maintenance mode for all the devices in the group, you can disable maintenance mode for a specific device from the device overview pane.

To enable group-level maintenance mode, on the **Device groups** page, click  beside the group, click **Enable maintenance mode for devices in the group**, and then click **Yes, continue**.

Inventory validation

Site inventory validation verifies the following:

- Connectivity between secure connect gateway and the device. It also verifies if the required ports are open on the device and if account credentials for the device are available and valid.
- If the requirements to collect telemetry from the device are met.
- If the alert or event destination on servers running Linux operating system and on iDRAC devices are configured.

If the validation is successful, the device is moved to the **Default** group or to the assigned custom device group. If the validation fails, the device is moved to the **Staging** or **Inactive** group.

If the device is not reachable or the device is unable to connect to the required ports, the device is moved to the **Inactive** group. If the device is connected but secure connect gateway is unable to collect the required information for device discovery, the device is moved to the **Staging** group.

By default, inventory validation is scheduled on a randomly determined day of every month at 11 p.m. You can choose a specific day based on your requirement. For more information, see [Configure automated tasks](#). To manually perform an inventory validation, select one or more devices on the **Devices** page and click **Validate inventory**.

Device correlation

You can add a server in secure connect gateway by using the host operating system IP address and iDRAC IP address of the device. In such a case, the **Devices** page displays two separate listings for the same device. Secure connect gateway receives alerts from the device through both the operating system and the iDRAC. However, for operational purposes, the operating system IP address and iDRAC IP address are correlated and considered as a single device. For correlated devices:

- The alerts from the operating system and the iDRAC are correlated and a service request is created for the Service Tag of the device.
- When telemetry is collected, the **Devices** page displays the same status for both the listings.
- For a manually initiated collection, the telemetry is collected through the selected device listing on the **Devices** page. For example, if the operating system listing is selected, telemetry is collected only through the operating system. However, if secure connect gateway is unable to connect to the device by using the operating system IP address, the telemetry is collected through the iDRAC.
- During periodic collections and collections performed when a service request is created, the telemetry is collected through the operating system. However, if secure connect gateway is unable to connect to the device by using the operating system IP address, the telemetry is collected through the iDRAC.


Enable or disable remote access

Prerequisites

Ensure that **Success** status is displayed for the device.

About this task

Dell technical support engineers may need to access your device to troubleshoot the device or perform any device-specific actions. So, you can enable remote access for the device, if necessary. You can also disable remote access to the device after the remote session is complete.


 **NOTE:** You can manually enable or disable remote access only for PowerEdge servers and PowerSwitch switches from the secure connect gateway user interface.

Steps

1. On the **Devices** page, click  beside the device IP address or hostname, and click **Enable remote access**.

 **NOTE:** If **Failed** status is displayed for the device, the **Enable remote access** option is disabled.

2. Click **Yes** to confirm that you want to enable remote access for the device.
Remote access is enabled for the device.

3. After the remote session is complete, click  beside the device IP address or hostname, click **Disable remote access**, and then click **Yes** to confirm.
Remote access is disabled for the device.

Device discovery rules

A device discovery rule enables you to add devices in secure connect gateway based on IP address ranges or comma-separated hostname expressions or IP addresses.

The **Device discovery rule** page enables you to create, manage, and run single or multiple discovery rules. It also displays the name of the rule, date, and time when the rule was last run, and its status.

NOTE: If devices discovered by the discovery rule become unreachable later, they are moved to the **Inactive** state. If a device is in **Inactive** state even after the discovery rule is run for three consecutive times, the device is automatically deleted.

When you click a discovery rule in the **Name** column, the **Discovery rule details** window is displayed with the following details:

- IP range or hostname of the devices
- Discovery frequency that is assigned to the rule
- Status of the rule

NOTE: During discovery, all the devices in the IP range are pinged. A device is discovered and inventoried in secure connect gateway as and when the device replies to the ping.

- Date when the rule was last run
- Number of devices that were successfully added during the current and previous run cycle, and number of devices in **Staging**, **Inactive**, and **Failed** states.

Create device discovery rule

About this task

You can discover devices within an IP address range or using comma-separated hostname expressions or IP addresses using a device discovery rule.

Steps

1. Go to **Device management > Manage devices > Discovery rule > Create rule**.

The **Create a discovery rule** page is displayed.

2. Enter a name for the discovery rule.

3. To discover a specific device using the IP address or multiple devices within an IP address range, perform the following steps:

- a. Select **IP address/range**.
- b. Enter the IP address or range of the devices.
- c. Enter the subnet mask of the specified IP address range.
- d. Optionally, to add another IP address or range, click **Add** and enter the required details.

You can add up to five different IP address ranges in the following formats:

- 10.34.*.*
- 10.34.1-10.*
- 10.34.*.1-10
- 10.34.1-10.1-10
- 10.34.1.1/24

NOTE: For an IP address entered in Classless-Inter Domain Routing (CIDR) notation, for example 10.34.1.1/24, the subnet mask entry is not considered.

4. To discover devices by using the hostname or IP addresses:

- a. Select **Individual hostname / IP address**.

- b. Enter the hostname or IP address of the devices as comma-separated values in the following formats:
 - 10.34.10.2, 10.34.10.3, 10.34.10.22
 - hostname1, hostname2, hostname3
 - 10.34.10.22, hostname2, 10.34.10.24
5. Select one of the following discovery frequencies:
 - **Run now**—discover the devices immediately.
 - **Run later**—discover the devices on a specific date.
 - **Run multiple times**—discover the devices on a specific day and time on a monthly or quarterly basis.
6. Based on your preference, select or clear the following check boxes:
 - **Perform deep discovery**—discovers a device and its associated device types.
 - **Enable monitoring**—enables secure connect gateway to detect hardware issues on the discovered devices.
 - **Configure protocols to receive alerts and events from this device**—automatically configures the alert and event settings of the discovered device to forward alert traps or event subscriptions to secure connect gateway.
7. Click **Create rule**.

Results

The discovery rule is added and listed on the **Device discovery rules** page. If you selected **Run now**, discovery of devices is initiated.

Adapters

Adapters act as an interface between secure connect gateway and the systems management consoles. They enable secure connect gateway to inventory and retrieve alerts from supported devices that are managed by systems management console such as OpenManage Enterprise, instead of adding each device individually. After inventorying and adding the devices, secure connect gateway can monitor the devices for issues and also collect and upload telemetry to the backend.

From the **Adapter** page, you can set up, edit, or delete an adapter. The **Adapter** page also displays the name or IP address of the server on which the adapter is installed, system management console name and version, number of devices managed by the adapter, and the adapter status.

i NOTE: If OpenManage Enterprise Services plug-in is installed and enabled on the OpenManage Enterprise instance, the devices are not retrieved by secure connect gateway and **Inactive** status is displayed for the adapter in the secure connect gateway user interface. When you disable the plug-in and manually sync the adapter, or when secure connect gateway performs a periodic scan, **Connected** status is displayed and the devices are retrieved by secure connect gateway.

When you click the name or IP address of the adapter, the adapter overview pane is displayed with the following details:

- Adapter display name, if any.
- Hostname or IP address of the server on which the systems management console is installed.
- Name and version of the systems management console.
- Operating system type.
- Adapter status.
- Timestamp of when the adapter sync was performed.
- Number of devices added successfully.
- Number of devices in the Staging group.

In the Adapter Overview pane, click **Sync now** to verify and update the devices that are inventoried through the adapter.

Set up an OpenManage Enterprise adapter

Prerequisites


You must have administrator privileges on the server on which OpenManage Enterprise is installed.

About this task


Setting up an OpenManage Enterprise adapter enables you to inventory devices that are managed by OpenManage Enterprise. If OpenManage Enterprise Services plugin is installed and enabled on the OpenManage Enterprise instance, the devices are not retrieved by secure connect gateway and **Inactive** status is displayed for the adapter in secure connect gateway.


Steps

1. Go to **Device management > Manage devices > Adapter > Connect to an adapter**.
The **Connect to an adapter** page is displayed.
2. Enter the hostname or IP address of the server on which OpenManage Enterprise is installed.
3. Optionally, enter a name for the adapter.
4. Enter the username and password that is required to access the server on which OpenManage Enterprise is installed.
i NOTE: The password must not exceed 50 characters.
5. Optionally, enable the common name check.
i NOTE: You must enable the common name check only if you have entered hostname in step 2.
6. Optionally, to enable the certificate authority check, perform the following steps:

 **NOTE:** The certificate authority check enables secure connect gateway to securely access OpenManager Enterprise.

- a. Select the certificate authority check box.
 - b. Browse and upload the security certificate in CRT format.
7. If you have already created a credential profile for the devices, select the credential profile.

 **NOTE:** If account credentials for a device type are not available in the credential profile, the device is moved to **Staging** state.
8. If you do not have a credential profile, click **Create a new credential profile** and perform the following steps:
 - a. Enter a name for the credential profile.
 - b. Select the device types and associated account credentials that you want to include in the credential profile.

 **NOTE:** A device type is enabled only if an account credential exists for the device type.
 - c. To create an account credential, expand the **Add account credentials** section, enter the required details, and then click **Save**.
 - d. Click **Create**.
9. Select the frequency in which you want secure connect gateway to verify and update the devices inventoried through the adapter.
10. Click **Connect to an adapter**.

Results

If secure connect gateway connects to the adapter successfully, the **Adapter Overview** window is displayed and devices that are managed by OpenManage Enterprise are inventoried in secure connect gateway.

Device groups

All the devices that are inventoried in secure connect gateway are automatically assigned to the **Default** device group. Depending on your requirement, you can group your devices to manage them better. After you create a device group, you can perform the following tasks:

- Add or remove devices from the device group.
- Configure the contact information and parts dispatch information for the device group.
- Edit the device group details.
- Delete the device group.
- Enable or disable maintenance mode for all the devices in the group.

The **Device groups** page displays the list of device groups and the number of devices in each group. You can also create, edit, delete, manage device groups, and enable or disable maintenance mode for all devices in a custom group.

NOTE: Grouping of devices is available for the following device types:

- Server/Hypervisor
- iDRAC
- Chassis
- Fluid File System (Fluid FS)
- Networking
- PeerStorage(PS)/ Equallogic
- Storage Center(SC)/Compellent
- PowerVault (MD3 and ME4 Series)
- Software
- VirtualMachine
- Webscale
- Dell ML3
- Direct Liquid Cooling

Create a device group

About this task

All the devices that are inventoried in secure connect gateway are automatically assigned to the **Default** device group. Depending on your requirement, you can group your devices to manage them better.

Steps

1. Go to **Device management > Manage device groups > Create group**. The **Create group** page is displayed.
2. Enter a group name and description.
3. To provide primary or secondary contact details applicable for the devices in the group, select the **Contact Details** check box and then enter the required details. To copy the details provided on the **Preferred contact details** page, click the link that is displayed below the check box.
4. Click **Create group**.

Results

The device group is created and displayed on the **Device groups** page.

Manage a device group

About this task

After you create a device group, you can add or delete devices from the device group.

 **NOTE:** A device can be included in only one device group.

Steps


1. Go to **Device Management** > **Manage device groups** > **View**.
2. On the **Device groups** page, select the device group and click **Manage**.
The list of ungrouped devices and the devices in the device group are displayed.
3. Select and move the devices between the two panes and click **Save**.
When you add or remove devices, its associated devices are also migrated.

Enable group-level maintenance mode


About this task

Group-level maintenance mode suspends alert processing and automatic service request creation capabilities for all the devices in a custom device group. After you enable maintenance mode for the devices in the group, you can disable maintenance mode for a specific device from the device overview pane. In such cases, the total number of devices in the group and the number of devices in maintenance mode is shown in the **Total devices** column.

Steps

1. Go to **Device management** > **Manage device groups** > **View**.
2. Click  beside the device group and click **Enable maintenance mode for devices in the group**.
3. Click **Yes, continue**.

Results

Maintenance mode is enabled for the devices and  is displayed beside the devices on the **Devices** page.


Device credentials and credential profiles

Secure connect gateway requires device credentials to add devices and to collect telemetry. You can enter or assign credentials to a device when you add or edit the device details. You can also enter the credentials by assigning an account credential.

Device credentials

A device credential consists of the credentials of a specific device type. The credentials are used by secure connect gateway to connect to the device and collect telemetry. Depending on the devices in your environment, you may have to create one or more account credentials.

The **Device credentials** page enables you to add, edit, or delete an account credential. It also displays the name and associated device type.

 **NOTE:** If you installed secure connect gateway on a server or virtual machine running Linux operating system, you cannot create credential accounts for devices running a Windows operating system.

Add account credentials

About this task

Account or device credentials are required to add a device in secure connect gateway and to collect telemetry, if required. Depending on the devices in your environment, you can create one or more credential accounts for the same device type. However, at a time, only one account credential can be associated with a device type.

For authentication, after the username, you can either choose to enter the password of the device, or upload a key certificate and enter a passphrase. It is recommended to use the key certificate and passphrase method as it is more secure.


Authentication using key certificate includes the following process:


1. Creating an SSH key pair—a public key and a private key.
2. Copying the public key to the server.
3. Using the private key as the passphrase.

For more information about generating and using an SSH key pair, see [How to generate a new SSH key](#).

Steps

1. Go to **Device management > Manage credentials > Manage device credentials > Add credentials**. The **Add account credentials** window is displayed.
2. Enter a credential name.
3. Select the device type. The associated fields are displayed.
4. You can enter the credentials either manually or using a credential vault. Select one of the following options:
 - To store the credentials locally on the secure connect gateway device, select **Manually**.
 - To access credentials from the vault, select **Use a credential vault**. Select the correct vault from the dropdown list and enter the identifiers that the device has been configured with. If you select **CCP**, you must enter an **Account identifier**. If you select **Conjur** or **Azure Key Vault**, you must enter the **Username identifier** and **Password identifier**. If you select HashiCorp vault, you must enter the Secret path, Username identifier and Password identifier.

 **NOTE: Secret Path:** The specified location within the Vault for storing and retrieving secrets.

 **NOTE:** The identifier details for Conjur vault are available on the credential vault user interface and the format is as follows:

- Username identifier—Secret Name/username
- Password identifier—Secret Name/password

If you have not added a vault, click **Add a vault** and enter the required information. See [Add a credential vault](#).

5. Click **Add**.

6. Perform one of the following steps:

- If you select the device type as **Server / Hypervisor**, select the operating system, enter the username and either enter the password, or upload the key certificate and enter the passphrase.

NOTE: You cannot add account credentials for a server or hypervisor running the Windows operating system. For the list of supported operating systems, see the *Secure Connect Gateway 5.x — Virtual Edition Support Matrix* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

- If a device is running the Linux operating system, the credentials must have root or sudo user rights. If you provide the username and password of a sudo user, ensure that the sudo user is configured for secure connect gateway. See [Configure sudo access for Secure Connect Gateway on a server running Linux operating system](#).
- If the device is running ESX or ESXi, you can select the **Enable Common Name (CN) check** or **Enable Certificate Authority (CA) check** check boxes to perform additional security checks on the device. To perform a CA check, you can also upload certificates from the local system.
- If you select the device type as **iDRAC, Storage Center (SC) / Compellent, Dell ML3 or PowerVault**, enter the username and password of the device. Optionally, select the **Enable Common Name (CN) check** or **Enable Certificate Authority (CA) check** check boxes to perform additional security checks on the device. To perform a CA check, you can also upload certificates from the local system.
- If you select the device type as **Chassis**, enter the username and either enter the password, or upload the key certificate and enter the passphrase. Optionally, select the **Enable Common Name (CN) check** or **Enable Certificate Authority (CA) check** check boxes to perform additional security checks on the device. To perform a CA check, you can also upload certificates from the local system.
- If you select the device type as **Fluid File System (Fluid FS)**, enter the username and either enter the password, or upload the key certificate and enter the passphrase.
- If you select the device type as **Peer Storage (PS) / Equallogic**, select the software type. Enter the username and either enter the password, or upload the key certificate and enter the passphrase, and then enter the community string of the device.
- If you select the device type as **Software** and software type as **vCentre**, enter the username and password of the device. Optionally, select the **Enable Common Name (CN) check** or **Enable Certificate Authority (CA) check** check boxes to perform additional security checks on a vCenter. To perform a CA check, you can also upload certificates from the local system. If you select the software type as **HIT Kit / VSM for VMware**, enter the username and either enter the password, or upload the key certificate and enter the passphrase.
- If you select the device type as **Virtual Machine**, select the operating system, and enter the username and either enter the password, or upload the key certificate and enter the passphrase.
- If you select the device type as **Networking**, and the operating system type as **Additional OS types**, enter the username and either enter the password, or upload the key certificate and enter the passphrase. Enter the community string of the device. Click **Enable SNMP v3** if you have configured your networking device with SNMP v3 for traps. Enter the SNMP v3 details according to the security level. For details see [Configure SNMP v3 settings](#)

NOTE:

- If you are using a networking device that is running the operating system version 10 and later, ensure that you enter only the username and password for authentication and not the key certificate and passphrase. You must also use the same credentials for SSH or REST.
- If you have configured the device with **Enable password** and **Community string**, you must add **Enable password identifier** and **Community string identifier** when you select **Conjur** credential vault type. The community string is required only for Cisco devices, wireless controllers, and devices from the PowerConnect family 28xx and X series. The identifier details are available on the credential vault user interface and the format is as follows:
 - Enable Password identifier—Organization account name /Environment /Safe Name/Name + password
 - Community string identifier—Organization account name /Environment /Safe Name/Name + username

. If you select the device type as **Networking**, and the operating system type as **Enterprise SONiC**, enter the username and the password.

- If you select the device type as **Solution**, for **SSH Credentials**, enter the username and either enter the password, or upload the key certificate, and enter the passphrase. For **REST Credentials**, enter the username and password. Optionally, you can select the **Enable Common Name (CN) check** or **Enable Certificate Authority (CA) check** check boxes to perform additional security checks on the appliance. To perform a CA check, you can also upload certificates from the local system.
- If you select the device type as **Direct Liquid Cooling**, enter the credential name and then enter the community string of the device.
- If you select the device type as **Remote Support SSH**, use the credential vault and enter the username identifier and the password identifier. You cannot manually add the username and password for **Remote Support SSH**.

NOTE: Devices that have SSH remote support capabilities enabled can share credentials using **Remote Support SSH**. The supported device types are:

- Data storage devices other than Fluid File System (Fluid FS), PeerStorage(PS) / Equallogic, Storage Center(SC)/Compellent, PowerVault (MD3 and ME4 Series), Dell ML3.
- Converged/Hyperconverged Infrastructure other than Webscale.
- Data Protection.

For more information about device types that have SSH for remote support capabilities, see the *Secure Connect Gateway 5.x - Virtual Edition Support Matrix* available on the on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

7. Click **Add**.

Configure sudo access for Secure Connect Gateway on a server running Linux operating system

Prerequisites

Ensure that you are logged in to the device with root privileges.

About this task

In Linux operating systems, users with sudo access may be granted administrator privileges to run certain commands. If you have added a device in secure connect gateway using the credentials of a sudo user, you must perform the following steps to allow secure connect gateway to monitor and collect telemetry from the device.

Steps

1. Open the terminal window.
2. Set the home directory path for the user—enter `useradd user_name -d /home` and press Enter.
3. Open the `/etc/sudoers` file.
4. Insert an exclamation mark [!] on the requiretty line. For example, `!requiretty`
5. Add one of the following based on your preference:
 - `%root ALL=(ALL) NOPASSWD: ALL`—to grant permission to all users in the root group.
 - `user_name ALL=(ALL) NOPASSWD: ALL`—to grant permission to only a specific user.
6. Save the `/etc/sudoers` file.

Credential profiles

A credential profile is a collection of credential accounts for various device types. Credential profiles enable you to assign credentials for multiple device types instead of entering the credentials for each device manually.

The **Credential profiles** page enables you to create, edit, and delete a credential profile. It also displays all the credential profiles that are created for your devices.

When you click a credential profile, the following information is displayed:


- Device type and associated and credential account.
- Hostname, IP address, and type of device to which the credential profile is assigned.

Create a credential profile

About this task

Credential profiles enable you to assign credentials for multiple device types instead of entering the credentials for each device manually.

Steps

1. Go to **Device Management > Manage credentials > Manage credential profiles > Create profile**. The **Create credential profiles** page is displayed.
2. Enter a name for the credential profile.
3. Select the device types and the associated account credential that you want to include in the credential profile.
 **NOTE:** A device type is enabled only if an account credential exists for the device type.
4. To create an account credential, expand the **Add account credentials** section, enter the required details, and then click **Save**. For more information, see [Add account credentials](#).
5. Click **Create profile**.

Assign a credential profile

About this task

After you add devices, you can manually assign a credential profile for one or more devices.

Steps

1. Go to **Device management > Manage devices > Devices > View**.
2. On the **Devices** page, select one or more devices to which you want to assign a credential profile. The **Tasks** pane is displayed.
3. In the **Add devices to an existing profile** section, select the required credential profile, click **Assign**, and click **Yes**.

Credential Vault

A credential vault is a secure system that allows you to store and manage all your certificates and credentials in a single place without storing them locally.

The supported credential vaults for secure connect gateway are:

- CyberArk with Conjur API
- CyberArk Credential Provider
- Azure Key Vault
- HashiCorp Vault

The **Credential vaults** page enables you to add, edit, or delete credential vaults. It also displays the vault name, vault server name, connectivity status, type of credential vault selected and the time of update. Once a vault is added, you can create account credentials for your devices by mapping the credential vault account ID.

Add a credential vault

About this task

A credential vault is a secure system that allows you to store all the certificates and credentials of the devices that you manage in secure connect gateway. Depending on the devices in your environment, you can add one or more credential vaults. Once a vault is added, you can create account credentials for your devices by mapping the credential vault account ID.

Steps

1. Go to **Device management > Manage credentials > Manage credential vaults > Add vault**.

The **Add a credential vault** window is displayed.

2. Enter the following details:
 - a. **Vault name**—a user-defined name.
 - b. **Vault server hostname/IP**—depending on the vault setup, enter the hostname or IP address of the vault server.
 - c. **Port no**—the default port for credential vault is 443. However, if you have configured CyberArk with Conjur API using another port, enter that port number.
 3. If you select the vault type as **CyberArk Conjur**, enter these additional details:
 - a. **Organization account name**—the account name for your organization. For example: myvault, myorg.
 - b. **Client login name**—enter an alphanumeric login name.
 - c. **API key**—an alphanumeric value. This key helps to retrieve the credentials dynamically from the vault. For more information about how to set the API key, see [CyberArk Conjur - Rest API](#).
 - d. **Authentication method**—the method you choose to send the authentication request to CyberArk with Conjur API. The following authenticators are supported in secure connect gateway: Azure, GCP, JWT, OIDC, K8S, and LDAP.
 4. If you select the vault type as **CyberArk CCP**, perform the following steps:
 - a. Enter the **Application ID**—the ID assigned to your device.
 - b. Enter the **Safe Name**—enter an alphanumeric name.
 - c. Upload a certificate, enter the passphrase, and click **Validate**.
For more information, see [CyberArk CCP](#).
 5. If you select the vault type as **Azure Key Vault**, perform the following steps:
 - a. Enter the **Vault name**—the display name you have assigned to the vault.
 - b. Enter the **Key vault name**—the name assigned to the vault in the Microsoft Azure portal.
 - c. Then, enter the **Client ID**, **Client Secret**, and **Tenant ID** that you have created in the Microsoft Azure portal.
 6. If you select the vault type as **HashiCorp Vault**, perform the following steps:
 - a. Enter the **Vault name**—the display name that you have assigned to the vault.
 - b. Enter the **Enter the Namespace**—the namespace configured in the vault.
 - **/root namespace**: Used for global tasks with the highest privileges.
 - **Configured namespace**: Used for team-specific configurations and secret management.
 - c. Enter the **Path**—path specifies the location of secret configurations in the vault.
 - d. **Authentication method**—select the appropriate Authentication method from the dropdown list. Depending on your selection, provide the required authentication details:
 - **LDAP**: Enter **Username** and **Password**.
 - **Token**: Enter **Role ID** and **Secret ID**.
To generate the **Role ID** and **Secret ID**, refer to the [HashiCorp AppRole authentication](#)
 - **Username**: Enter **Username** and **Password**.
For more information, see [HashiCorp Vault](#).
7. Click **Add**.

Results

A success message is displayed if the details are correct. An error message is displayed if the details are incorrect, or if secure connect gateway is unable to connect to the credential vault.

Edit or delete a credential vault

About this task

After you add a credential vault, you can edit or delete the vault.


Steps

1. Go to **Device management > Manage credentials > Manage credential vaults > View**.
The **Credential vaults** page is displayed.
2. Select the vault that you want to edit and click **Edit**.
3. Edit the following based on your preference:

- a. **Vault name**—a user-defined name.
 - b. **Vault server hostname/IP**—depending on the vault setup, enter the hostname or IP address of the vault server.
 - c. **Port no**—the default port for credential vault is 443. However, if you have configured the vault using another port, enter that port number.
 - d. **Authentication method**—the method you choose to send the authentication request to the credential vault. The following authenticators are supported in secure connect gateway: Azure, GCP, JWT, OIDC, K8S, and LDAP.
 - e. **Organization account name**—the account name for your organization. For example: myvault, myorg.
 - f. **Client login name**—enter an alphanumeric login name.
 - g. **API key**—an alphanumeric value. This key helps to retrieve the credentials dynamically from the vault. For more information about how to set the API key, see [CyberArk Conjur - Rest API](#).
4. Click **Save**.
A success message is displayed once the details are updated.
 5. To delete the vault, select the vault on the **Credential vaults** page and click **Delete**.
The vault is deleted and removed from the **Credential vaults** page.

Service requests

The **Service requests** page displays information about only the open service requests that were created for the managed devices. Though secure connect gateway automatically creates service requests when an issue is detected, a service request can also be created over an email, telephone, and chat. For devices with a ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract, the service request status is displayed irrespective of the source from which the service request was created.

 **NOTE:** For devices with a Basic service contract, a temporary service request without a service request ID is created and displayed on the **Service requests** page. However, the service request is automatically deleted from secure connect gateway after a few days.

By default, the service requests are grouped under their respective device name or device IP address. The last refreshed date and time that is displayed in the group header indicates when the service request information was last retrieved from the backend.

You can switch between grid and tabular views to view the following information regarding service requests:

- Service request ID
- Number of days since when the service request was created
- Name or IP address of the device for which the service request was created
- Service request title
- Source from which the service request was created
- Service request status
- Service Tag or serial number of the device

Use the column level filters in the tabular view to customize the information that is displayed. Click **Filter** to view the service requests based on the device type and the service request status.

Telemetry

By default, secure connect gateway collects and sends device telemetry from the devices periodically, irrespective of their service contract. The device telemetry is collected based on the predefined day and time that is specified in the **Automated tasks** page. It also collects telemetry automatically from a device when a service request is created for an issue with the device. You can also initiate a collection from one or more devices. See [Manually initiate a collection](#). The telemetry that is collected includes the following information:

- Hardware and software inventory—installed devices, processors, memory, network devices, usage, and Service Tag
- Software configuration for servers—operating system and installed applications
- Configuration information—interfaces, VLAN, Data Center Bridging (DCB), spanning tree, and stacking
- Identity information—system name, domain name, and IP address
- Event data—Windows event logs, core dump, and debug logs

The following identity information is also collected as part of the telemetry:

- Host name
- IP address
- Subnet mask
- Default gateway
- MAC address
- DHCP server
- DNS server
- Processes
- Environment variables
- Registry
- Logs
- iSCSI data
- Fibre Channel data—host World Wide Name (WWN) and port WWN

If required, you can configure the telemetry settings to exclude the collection of certain attributes from your devices. See [Configure telemetry settings](#).

Dell Technologies does not access or collect personal information, such as your personal files, web-browsing history, or cookies. Any personal attributes that is inadvertently collected or viewed is treated in accordance with the Dell Privacy Policy available for review at [Dell.com/privacy](https://www.dell.com/privacy).

Prerequisites to perform a collection

To perform a collection on a device, ensure the following:

- The local system has sufficient hard drive space to save the collected telemetry.
- The local system and remote devices meet the network port requirements.
- If a server was added using the operating system, IP address, or hostname (agent-based monitoring):
 - Dell OpenManage Server Administrator (OMSA) is installed.
 - If the server is running a Linux operating system:
 - The device credentials must have administrator privileges.
 - No resource (network share, drive, or ISO image) is mounted on the /tmp folder.
 - If OMSA is installed on the device, the latest version of OpenSSL must also be installed on the device.

NOTE: If the server you have added for agent-based monitoring does not have OMSA installed, periodic collection from the device does not include storage and system details.

- If OMSA is not installed on a server that was added by selecting the device type as **Server/Hypervisor**, OS to iDRAC Pass-through is enabled. For steps to enable the enable OS to iDRAC Pass-through, see the *Integrated Dell Remote Access Controller User's Guide* available on the [iDRAC Manuals](#) page

- If a server was added using the iDRAC IP address (agentless monitoring), the iDRAC credentials that you entered must have administrator privileges.
- The local system must have Internet connectivity for uploading the collected telemetry to the backend.
- For collecting telemetry from ESX and ESXi only, ensure that SFCBD and CIMOM are enabled.

Telemetry collections

The **Telemetry collections** page enables you to view and download collections and also manually upload collections to the backend. By default, the name, timestamp, purpose, and status of the collection are displayed. The associated service request number and the status of the collection is also displayed.

NOTE: The **Telemetry collections** page displays information only about the collections that are performed during the last seven days.

Use the column level filters to customize the information displayed, or click **Filter** to view the information for a custom date range, specific collection type, or device type. To manually upload a collection to the backend, select the collection and click **Upload**.

NOTE: The maximum size of the collections that you can upload is 5 GB.

To manually delete a collection, select the collection and click **Delete**.

NOTE: A single device collection is automatically deleted when the device is removed from secure connect gateway. A multi-device collection is automatically deleted only after all the devices associated with the collection are removed from secure connect gateway.

If you click a single device collection, the following details are displayed:

- Hostname or IP address.
- Service Tag.
- Date when the collection was initiated.
- Status of the collection performed.
- Date when the collection was uploaded.
- Upload status.
- Links to view and download the collection.

If you click a multiple device collection, the following details are displayed:

- Date when the collection was initiated.
- Overall status of the collection that is performed and upload status.
- Date when the collection was uploaded.
- IP address or hostname, Service Tag, and collection status of each device on which the collection was performed.
- Link to download the collection.

Analytics telemetry

By default, secure connect gateway collects storage information and SMART logs from iDRAC automatically on a random day every week at 1 a.m. for analytics. For the list of attributes collected, see the *Secure Connect Gateway 5.x — Virtual Edition Reportable Items* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page. An analytic collection is performed on iDRAC9 or later installed with firmware version 4.00.00.00 or later, SMART capable drivers, and an active Datacenter license.

Analytics telemetry page displays the following information about the collections that are performed during the last 30 days, after which, the collections are automatically purged.

- Date when the collection was initiated.
- IP address or hostname of the collection host.
- Status of the collection performed.
- Link to download the collection as a ZIP file to your local system.
- Upload the status of the collection.


View or download collections

About this task

You can view or download collections from the **Devices** and **Telemetry collections** pages.

Steps


1. To view or download collections from the **Devices** page, perform the following steps:
 - a. Go to **Device management > Manage devices > Devices > View**.
 - b. Click a device name or IP address in the **Name / IP Address** column.
The device overview pane is displayed.
 - c. From the **Collections** list, select the required collection.
2. To view or download collections from the **Telemetry collections** page, perform the following steps:
 - a. Go to **Telemetry > Telemetry collections**.
 - b. Click the collection that you want to view or download.
The collection overview pane is displayed.
3. Click **View** or **Download**.

 **NOTE:** The **View** option is displayed only if the collection is performed on a server or iDRAC.

- If you click **View**, the **Configuration Viewer** is displayed in a new web browser window.
- If you click **Download**, the collection is downloaded and saved as a ZIP file. Extract the ZIP file and double-click **index.html**.

Configuration viewer

The **Configuration Viewer** displays the telemetry collected by secure connect gateway from your devices.

 **NOTE:** The **Configuration Viewer** does not display the telemetry that is collected from storage devices with Fluid File System (FluidFS).

The **Configuration Viewer** displays information under various categories and sub categories in a tabbed format. The **Summary** section displays the following information:

- The telemetry settings in secure connect gateway at the time of the collection.
- Summary of errors that were detected in the collected telemetry.
- Brief information about the device.

If you have disabled the collection of identity information from devices, the identity information such as hostname, IP address, and so on, are replaced by tokenized values. The tokenized values are represented as TOKENn—for example, TOKEN0, TOKEN1, or TOKEN2.

For a list of items that may be reported in collections from a server, see [Items reported in periodic collections from servers](#).

Items reported in periodic collections from servers

The items reported in the telemetry that is collected from servers vary depending on the:

- Device type used to add the device in secure connect gateway.
- Type of collection (manual, periodic, or service request).

The telemetry that is collected for a service request or for a manually initiated collection is more detailed in comparison with the telemetry that is collected during a periodic collection. For the complete list of attributes that are collected, see the *Secure Connect Gateway 5.x — Virtual Edition Reportable Items* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page. The telemetry that is collected during periodic collections enables Dell Technologies to provide you an insight into your environment configuration with proactive firmware recommendations and other reports.

The following table provides a summary of the items reported in the collected telemetry during a periodic collection from a server:

Table 6. Items reported in a periodic collection from a server

Items reported	Device added in secure connect gateway with device type as Server / Hypervisor		Device added in secure connect gateway with the device type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
Memory	✓	✗	✓
Memory Array	✓	✗	✓
Memory Operating Mode	✓	✗	✗
Memory Redundancy	✓	✗	✗
Slot	✓	✗	✓
Controller	✓	✗	✓
Connector	✓	✗	✗
PCIe-SSD-Extender	✓	✗	✓
Enclosure	✓	✗	✓
Array Disk	✓	✗	✓
Intrusion Switch	✓	✗	✓
Hardware Log	✓	✗	✓
Main Chassis	✓	✗	✓
Additional Information	✓	✗	✓
Modular Enclosure Information	✓	✗	✓
Firmware	✓	✗	✓
Processor	✓	✗	✓
Fan	✓	✗	✓
Fan Redundancy	✓	✗	✓
Temperature	✓	✗	✓
Voltage	✓	✗	✓
Power Supply	✓	✗	✓
Power Supply Redundancy	✓	✗	✓
Network	✓	✗	✓
IPv4 Address	✓	✗	✗
IPv6 Address	✓	✗	✗
Network Team Interface	✓	✗	✗

Table 6. Items reported in a periodic collection from a server (continued)

Items reported	Device added in secure connect gateway with device type as Server / Hypervisor		Device added in secure connect gateway with the device type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
Interface Member	✓	✗	✗
Remote Access Device	✓	✗	✓
DRAC Information	✓	✗	✗
Serial Over LAN Configuration	✓	✗	✓
IPv6 Detail	✓	✗	✗
User Setting	✓	✗	✓
User Information	✓	✗	✓
iDRAC User Privilege	✓	✗	✓
DRAC User Privilege	✓	✗	✗
Serial Port Configuration	✓	✗	✓
NIC Configuration	✓	✗	✓
Component Detail	✓	✗	✓
Controller TTY Log	✓	✗	✓
Operating System	✓	✓	✗

NOTE: In a collection from an iDRAC, Controller TTY Log is available only if iDRAC firmware version 2.00.00.00 or later is installed on the server.

Manually initiate a collection

Prerequisites

See [Prerequisites to perform a collection](#).

About this task

Secure connect gateway collects telemetry periodically and when a service request is created. You can also manually initiate a collection on one or more devices and allow secure connect gateway to automatically upload the collection.

Steps

1. Go to **Device Management > Manage devices > Devices > View**.
2. To initiate a collection from a single device, perform the following steps:
 - a. Select the device.
The **Tasks** pane is displayed.
 - b. In the **Collect telemetry data** section, click **Start**. Optionally, select the purpose of initiating the collection.

NOTE: To collect Tech-Support logs from Enterprise SONiC operating system, select the device with Enterprise SONiC operating system on the **Devices** page, and select **Technical support** from the **Collection purpose** list. If

you disable collection of identification information on the **Telemetry Settings** page, the Tech support logs are not collected from Enterprise SONiC operating system.

- c. Click **Continue**.
3. To initiate a collection from an MX7000 chassis with the application logs, perform the following steps:
 - a. Ensure that you have configured the Common Internet File System (CIFS) location details in the **Telemetry settings** page. For more information, see [Configure telemetry settings](#).
 - b. Select the device.
The **Tasks** pane is displayed.
 - c. From the **Collection purpose** list, select **Technical support**.
 - d. Ensure that the firmware version running on the chassis is 1.20.10.00 or later. If an earlier firmware version is running on the chassis, ensure that collection of personal identity information is enabled on the **Telemetry settings** page.
 - e. Select the check box to include hardware logs in the telemetry.
 - f. Click **Start** and then click **Continue**.
4. To initiate a collection from multiple devices, perform the following steps:
 - a. Select the devices.
The **Tasks** pane is displayed.
 - b. In the **Collect telemetry data** section, select the purpose of initiating the collection, and then click **Start**.
 - c. Optionally, enter a name for the collection bundle, service request number, email address of the technical support agent, and the associated project ID.
 - d. If you want secure connect gateway to upload the collection bundle to the backend, select the **Upload collections** check box.
 - e. Click **Continue**.

Manually upload collection

About this task

Secure connect gateway collects and upload collections to the backend. You can also upload a collection during the following scenarios:

- Telemetry collection was successful, but upload of the collection was unsuccessful.
- You did not allow secure connect gateway to automatically upload the collection after it was performed.
- You want to upload a collection to the backend again.

Steps

1. Go to **Telemetry > Telemetry collections**.
2. Select the collection that you want to upload and click **Upload**.

Results

The collection is sent to the backend. Dell technical support analyzes the collection to identify and troubleshoot issues, if any.

Extensions

An extension enables you to extend the capabilities of secure connect gateway to devices that are managed by a system management console, such as Dell OpenManage Enterprise.

Adapters

Adapters act as an interface between secure connect gateway and the systems management consoles. They enable secure connect gateway to inventory and retrieve alerts from supported devices that are managed by systems management console such as OpenManage Enterprise, instead of adding each device individually. After inventorying and adding the devices, secure connect gateway can monitor the devices for issues and also collect and upload telemetry to the backend.

From the **Adapter** page, you can set up, edit, or delete an adapter. The **Adapter** page also displays the name or IP address of the server on which the adapter is installed, system management console name and version, number of devices managed by the adapter, and the adapter status.

NOTE: If OpenManage Enterprise Services plug-in is installed and enabled on the OpenManage Enterprise instance, the devices are not retrieved by secure connect gateway and **Inactive** status is displayed for the adapter in the secure connect gateway user interface. When you disable the plug-in and manually sync the adapter, or when secure connect gateway performs a periodic scan, **Connected** status is displayed and the devices are retrieved by secure connect gateway.

When you click the name or IP address of the adapter, the adapter overview pane is displayed with the following details:

- Adapter display name, if any.
- Hostname or IP address of the server on which the systems management console is installed.
- Name and version of the systems management console.
- Operating system type.
- Adapter status.
- Timestamp of when the adapter sync was performed.
- Number of devices added successfully.
- Number of devices in the Staging group.

In the Adapter Overview pane, click **Sync now** to verify and update the devices that are inventoried through the adapter.

Set up an OpenManage Enterprise adapter

Prerequisites

You must have administrator privileges on the server on which OpenManage Enterprise is installed.

About this task


Setting up an OpenManage Enterprise adapter enables you to inventory devices that are managed by OpenManage Enterprise. If OpenManage Enterprise Services plugin is installed and enabled on the OpenManage Enterprise instance, the devices are not retrieved by secure connect gateway and **Inactive** status is displayed for the adapter in secure connect gateway.

Steps

1. Go to **Device management > Manage devices > Adapter > Connect to an adapter**. The **Connect to an adapter** page is displayed.
2. Enter the hostname or IP address of the server on which OpenManage Enterprise is installed.
3. Optionally, enter a name for the adapter.
4. Enter the username and password that is required to access the server on which OpenManage Enterprise is installed.

NOTE: The password must not exceed 50 characters.

5. Optionally, enable the common name check.


 **NOTE:** You must enable the common name check only if you have entered hostname in step 2.

6. Optionally, to enable the certificate authority check, perform the following steps:

 **NOTE:** The certificate authority check enables secure connect gateway to securely access OpenManager Enterprise.


- a. Select the certificate authority check box.
- b. Browse and upload the security certificate in CRT format.

7. If you have already created a credential profile for the devices, select the credential profile.

 **NOTE:** If account credentials for a device type are not available in the credential profile, the device is moved to **Staging** state.

8. If you do not have a credential profile, click **Create a new credential profile** and perform the following steps:

- a. Enter a name for the credential profile.
- b. Select the device types and associated account credentials that you want to include in the credential profile.

 **NOTE:** A device type is enabled only if an account credential exists for the device type.

- c. To create an account credential, expand the **Add account credentials** section, enter the required details, and then click **Save**.
- d. Click **Create**.

9. Select the frequency in which you want secure connect gateway to verify and update the devices inventoried through the adapter.

10. Click **Connect to an adapter**.

Results

If secure connect gateway connects to the adapter successfully, the **Adapter Overview** window is displayed and devices that are managed by OpenManage Enterprise are inventoried in secure connect gateway.

Audits

All the events and activities that are performed in secure connect gateway are saved and classified as **Activity**, **Alert Delivery**, **File Transfer**, and **Logs**.

The following table describes the information that is saved about various activities that were performed in secure connect gateway:

Table 7. Audit categories

Category	Description
Gateway Activity	REST API calls invoked by secure connect gateway, for example, user authentication, file upload, device serial number retrieval, and so on. You can use the column level filters to customize the information displayed, or click Filter to view the information for a custom date range. To save the information displayed on the page in a CSV file, click Export all .
Alert Delivery	Alert payload that is uploaded to the backend when an alert is generated on your device. You can use the column level filters to customize the information displayed, or click Filter to view the information for a custom date range. To save the information displayed on the page in a CSV file, click Export all . To view the current activity, click Active alert delivery .
File Transfer	Files transfers between your device, secure connect gateway, and the backend. To view information about the files that are being transferred, click Active file transfer session .
Remote support	Remote sessions that are currently being performed on your devices.
Remote actions	Remote scripts that are currently running and that were previously run on your devices by a technical support agent. Click Active remote actions to view the scripts that are currently run on your devices.
Logs	Logs that are generated for the gateway, REST, and Migration services. You can download all the logs of a specific type or for a specific date.

Configuring Secure Connect Gateway settings

The **Settings** tab enables you to configure contact information, connectivity to SMTP, proxy, and Policy Manager server, telemetry settings, email notifications, security certificates, and automated tasks. You can also enable API interfaces for secure connect gateway, and allow users to access secure connect gateway through their network credentials.

Configure contact information

About this task

The **Contact** page enables you to configure your primary and secondary support.

Steps

1. Go to **Settings > Preferred contact details**.
2. In the **Support contacts** section, select your country or region, and edit the primary and enter the secondary support contact information.
The contact information that was entered during registration is automatically displayed for the primary support contact.
3. Click **Save**.

NOTE:

If users have configured TechDirect in a previous version, they will notice that TechDirect is removed after they upgrade to version 5.28. As a result, the TechDirect account information is no longer available in the secure connect gateway system. However, PowerEdge servers continue to create cases and send parts for any issues that arise. During the upgrade, a banner appears to inform users about the removal of the TechDirect integration. For more information, click [here](#).

Configuring your environment

The **Environment configuration** page enables you to configure your proxy server settings, SMTP server settings, enable or disable VMware tools, and manage security certificates. You can also ensure connectivity between secure connect gateway and the Policy Manager server.

If the local system connects to the Internet through a proxy server, you must configure the proxy server settings. If your company uses an SMTP server, it is recommended that you configure the SMTP server settings to receive email notifications.

Supported TLS configurations

TLS 1.0 and 1.1 are no longer supported on secure connect gateway. Devices can communicate with secure connect gateway only through TLS 1.2 and 1.3.

If you have devices or services using TLS 1.0 or 1.1 versions, they are automatically disconnected from secure connect gateway. To monitor the disconnected devices, update them to TLS 1.2 or 1.3. You can check the connection status on the **Environment configuration** page and the **Devices** page.

The following devices and services may get disconnected if they are using TLS 1.0 or 1.1:

- SMTP server
- LDAP server
- iDRAC server

- ME4 storage
- Dell Compellent storage
- HitKit or VMware Service Manager (VSM)
- WebScale
- ML3 Tape library
- Chassis MX7000
- Data storage and HCI and CI Products, Data Protection

The supported ciphers for devices and services to communicate with secure connect gateway are:

- Server supported ciphers:
 - TLS 1.2 Ciphers
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
 - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
 - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
 - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
 - TLS 1.3 Ciphers
 - TLS_AES_256_GCM_SHA384
- Client supported ciphers:
 - TLS 1.2 Ciphers
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
 - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
 - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
 - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
 - TLS 1.3 Ciphers
 - TLS_AES_256_GCM_SHA384
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_128_CCM_8_SHA256
 - TLS_AES_128_CCM_SHA256
 - TLS_CHACHA20_POLY1305_SHA256

Configure SMTP server settings

Prerequisites

Ensure that Transport Layer Security (TLS) version 1.2 is enabled on the SMTP server.

About this task


You must configure the SMTP server details of the company to receive email notifications from secure connect gateway. If the SMTP settings are not configured, a banner is displayed on the secure connect gateway user interface asking you to update the same.

NOTE:


- When you go to the **Configure SMTP server settings** page for the first time while you are logged in, an SMTP server connectivity test is performed automatically to check the connectivity status. A success or failure message is displayed after the completion of the test.
- If you close the banner on the secure connect gateway user interface that informs you about withdrawal of support for TLS 1.0 and 1.1, the automatic connectivity test is not performed when you go to the **Configure SMTP server settings** page.

Steps

1. Go to **Settings > Environment configuration > Connectivity details > SMTP server**.
2. Enter the hostname or IP address and port number of the SMTP server.
3. If the SMTP server requires authentication, enable the option to enter the details and enter the username and password to access the proxy server.
4. **STARTTLS** ensures that you receive emails securely. You can select one of the following options:
 - **If available**—Emails are sent from secure connect gateway with encryption. If **STARTTLS** is not supported on the SMTP server, emails are delivered without encryption. Alert delivery emails may not work with this configuration.
 - **Required**—Emails are sent with encryption from secure connect gateway and it is mandatory to have **STARTTLS** on the SMTP server for successful and secure delivery of the emails.
 - **Disable**—Emails are sent without encryption if you disable **STARTTLS**. It is not recommended to disable **STARTTLS**.

 **NOTE:** If you disable **STARTTLS** in secure connect gateway, ensure that it is also disabled on the SMTP server.

5. Click **Test connection** to validate the connection to the SMTP server.
6. Enter up to 10 email recipients and the sender email address that must be used to send the email messages from secure connect gateway.


 **NOTE:** You must add the correct domain to avoid emails being filtered as spam. It is recommended that you use your own domain to send the emails. You can also register the SMTP server with dell.com or emc.com to send your emails.
7. Test the connection and then click **Apply**.

If the connection is successful, a confirmation email is sent to all the email recipients that you provided.

Configure proxy server settings


About this task


If the local system connects to the Internet through a proxy server, you must configure the proxy server settings.


 **NOTE:** Secure connect gateway does not support connectivity through the Windows New Technology LAN Manager (NTLM) protocol.


Steps

1. Go to **Settings > Environment configuration > Connectivity details > Proxy server**.
2. Enable the option to use a proxy network.

 **NOTE:** Secure connect gateway supports the Basic HTTP proxy authentication method. Other authentication methods such as Digest and Negotiate (NTLM) are not supported.
3. Enter the hostname or IP address and port number of the proxy server.

 **NOTE:** The proxy server hostname can only contain . (period) and - (hyphen) special characters. An error message is displayed if the hostname is incorrect.

 **NOTE:** The username must be at least 32 characters, and the password must be at least 64 characters to meet the Linux `useradd` requirements.
4. If the proxy server requires authentication, enable the **Authentication** option to enter credentials.
 - Select **Manually** and enter the username and password that is required to access the proxy server in order to store the proxy credentials locally on the secure connect gateway.
 - To use credentials stored in a credential vault, select **Use a credential vault** and choose the appropriate vault from the **Select Vault** dropdown list to configure proxy credentials. Enter the details as follows:
 - **For Conjurer or Azure Key Vault:** Enter the username identifier and password identifier as configured in the vault.
 - **For CCP Vault:** Enter the account identifier as configured in the vault.
 - **For HashiCorp Vault:** Enter the secret path, username identifier, and password identifier as configured in the vault.
5. If no credential vault is configured, click **Add a vault**, then provide the necessary information to create a new vault entry.

 **NOTE:** An error message is displayed if:

 - You do not enter the username and password, or enter incorrect details.

- The proxy server does not require authentication, and you enter the username and password.

6. Test the connection and then click **Apply**.

Configure Policy Manager settings

Prerequisites

When you install policy manager, the default username and password are set to **admin** and **@\):/GjZmPcuE4xT** respectively. Reset the password before you configure policy manager settings in secure connect gateway.

About this task

Policy manager is a stand-alone application that is installed on a server other than your local system. You can configure policy manager to perform the following tasks:

- Control remote access to your devices.
- Maintain an audit log of remote connections and file transfers.
- Access administration actions performed on the policy manager.

An email notification is sent during the following scenarios:

- Secure connect gateway is unable to connect to the policy manager server.
- Policy Manager is configured to request your approval. For example, if you configure policy manager to prompt you for approval when a technical support agent has initiated a remote session on a device.

For more information about the operations and configuration of policy manager, see the *Policy Manager 5.x for Secure Connect Gateway User's Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

On the **Environment configuration** page, enter the details that are required to ensure connectivity between secure connect gateway and Policy Manager.

Steps

1. Go to **Settings > Environment configuration > Connectivity details > Policy Manager**.
2. Enable the option to enter the policy manager server details.
3. Enter the valid IP address, port number, username, and password of the policy manager server.
4. Select the **Enable SSL** check box if the policy manager is installed on a server that is secured by SSL.
5. If the policy manager server connects to the Internet through a proxy server, perform the following steps in the **Customer proxy server** section.
 - a. Enable the option to enter the proxy server details.
 - b. Enter the hostname or IP address and port number.
 - c. If the proxy server requires authentication, enable the option to enter the details and enter the username and password to access the proxy server.
6. Test the connection and then click **Apply**.

Enable VMware tools

Prerequisites

Secure connect gateway must be deployed on a VMware ESXi hypervisor.

About this task

VMware Tools is a suite of utilities that enhances the performance of the virtual machine guest operating system and improves management of the virtual machine. Without VMware Tools installed in your guest operating system, guest performance lacks important functionality. Installing VMware Tools allows you to remotely manage the local system through a VMware console. It also enables the balloon driver that allows the VMware host kernel to manage the memory available.

Steps

1. Go to **Settings > Environment configuration > Gateway configuration > Enable VMware Tools**.
2. Select the **Enable** check box.

3. Click **Apply**.

Manage Certificates

About this task


A security certificate allows you to:

- Securely access the secure connect gateway user interface or perform any tasks in secure connect gateway through port 5700.
- Securely connect to the backend using RESTful protocol through port 9443.

You can upload certificates in the .pem, .p12, or .pfx formats. If you upload a certificate in the .pem format, you must also upload the key in KEY format as a separate file. The .pem file must have the certificate chain that includes the certificate, intermediate, and root certificate authority. You can upload separate certificates for port 5700 and 9443 or a common certificate for both the ports.

Steps

1. Go to **Settings > Environment configuration > Gateway configuration > Certificate management**.
2. Select the port number for which the certificate is applicable for and then upload the certificate and key file, if applicable.

 **NOTE:** If you upload a certificate in .pem format, you must also upload the key in KEY format as a separate file.

3. If you upload the certificate in .pem format, enter the passphrase.
4. Click **Apply**.
5. Click **Restart now** to restart secure connect gateway.
 - You are logged out of the secure connect gateway user interface.
 - The security certificates are applied to your instance.
 - The certificate name and expiry information are displayed in the **Certificate management** section.

Configure SNMP v3 settings


About this task


Configuring SNMP v3 settings allows devices on your network to send alerts to secure connect gateway for case creation or reporting.

You must configure SNMP v3 settings if you have systems that use SNMP v3.

Steps

1. Go to **Settings > Environment configuration > Gateway configuration > SNMP v3 Settings**.
2. Select **Enable SNMP v3**.

 **NOTE:** SNMP v2 is used by default if you do not select the SNMP v3 option.

 **NOTE:** SNMPv3 must be enabled to support automated case creation for the Connectrix DS-7710B.

3. Enter the SNMP v3 details according to the security level:
 - a. If you select **No authentication, no privacy**, enter the username.
 - b. If you select **Authentication without privacy**, enter the username, select the authentication type, and enter the authentication password.
 - c. If you select **Authentication with privacy**, enter the username, select the authentication type, and enter the authentication password. Select the privacy type and enter the privacy password.

For the Connectrix DS-7710B device, with Fabric OS v9.2.x, it is strongly recommended to use SHA512. MD5 and SHA protocols support are deprecated and will not be supported in a future release of Fabric OS.
4. Click **Apply**.

Enable two-factor authentication

Prerequisites

- RSA must be installed on a system that is accessible by secure connect gateway.
- RSA secure tokens must be assigned to each user.
- RSA SecurID Token application must be installed on your system.

About this task

Two-factor authentication helps reduce security risks and provide secure access to secure connect gateway. When two-factor authentication is enabled, the RSA passcode from the RSA SecurID Token application must be entered when you log into secure connect gateway.

Steps

1. Go to **Settings > Environment configuration > Gateway configuration > Two-factor authentication**.
2. Select **Enable two-factor authentication**.

3. Enter the hostname and port from the RSA SecurID portal. The URL syntax for the RSA SecurID portal is `https://<rsa-am-server-hostname>:<port>/mfa/v1 1`.

The hostname is the fully qualified domain name (FQDN) of the RSA server. The default port is 5555. If the port is changed, to retrieve port information, go to **Setup > System settings > RSA Secur ID > Authentication API** on the RSA Authentication Manager (AM) server.

4. Upload the RSA AM certificate and test the connection.

The acceptable formats for the certificate are .pem or .p7b. The certificates should have the following attributes:

- For core certificates:
 - authorityKeyIdentifier=keyid,issuer
 - basicConstraints=CA:FALSE
 - keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
 - subjectAltName = @alt_names (SAN Names must be provided)
- For intermediate and root certificates:
 - authorityKeyIdentifier = keyid:always,issuer
 - basicConstraints = critical, CA:true
 - keyUsage = critical, digitalSignature, cRLSign, keyCertSign

If you do not have the certificate, contact your RSA server administrator to get the certificate or certificate chain.


5. Enter RSA SecurID client ID, RSA SecurID access key, and click **Apply**.

To retrieve the RSA SecurID from the RSA server, go to **Access > Authentication Agents > Manage Existing**.

To retrieve the RSA access key from the RSA server, go to **Setup > System settings > RSA Secur ID > Authentication API**.

NOTE:

- Secure connect gateway does not validate the RSA SecurID client ID. Ensure that you enter the correct RSA SecurID client ID.
- If you have used the username **admin** for other applications in RSA SecurID, use a different username for secure connect gateway and the RSA SecurID authentication for secure connect gateway. To change the secure connect gateway username using a CLI script, see the *Secure Connect Gateway - Virtual Edition Troubleshooting Guide* on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

 **NOTE:** You can change the secure connect gateway username using CLI script only for appliance systems.

Enable custom Pre-login message

Prerequisites


You must have administrator privileges to enable the Pre-login message.

About this task

This task describes how to enable and configure the Pre-login message, which is displayed to users before authentication. The Pre-login message helps prevent unauthorized access by providing clear notice of system logging and monitoring. A well-defined Pre-login banner reduces the risk of unintentional access by unauthorized users. In the case of legal proceedings that are related to unauthorized access, the presence of this banner can limit a defendant's ability to claim ignorance of access restrictions.

Steps

1. Go to **Settings > Environment configuration > Gateway configuration > Pre-login message**.
2. Enable the **Pre-login message**.
3. Enter a **Title** and compose the content of the pre-login message.
4. Click **Apply**.

 **NOTE:** This is a Pre-authentication message and should be approved by your organization's Legal team.

Results

The Pre-login message is now enabled and displayed to users before authentication.

Configure telemetry settings

About this task

Secure connect gateway collects telemetry at periodic intervals and when a service request is created. The **Telemetry settings** page allows you to enable or disable secure connect gateway to collect telemetry, upload telemetry, and include or exclude identity information in the collected telemetry.


It also enables you to configure a Common Internet File System (CIFS) location in which application logs from MX7000 devices are stored before they are bundled with other collected telemetry.

For more information about the attributes collected, see the *Secure Connect Gateway 5.x — Virtual Edition Reportable Items* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page. To configure periodic and analytic collections, see [Configure automated tasks](#).

Steps

1. Go to **Settings > Telemetry settings**.
2. In the **Data collection settings** section, select or clear the types of telemetry secure connect gateway can collect from your devices.
3. In the **Customer & device data privacy** section, by default, the option to include identification information is selected. But, if you do not want to include the information, clear the check box.

When the checkbox is cleared, the hostname and IP address in your SMTP mails are masked for privacy.

 **NOTE:** If you clear the check box, the collection of logs and diagnostic data are automatically disabled. Also, some of the data about your company network including the system log is not sent to the backend. This may prevent technical support from resolving issues that may occur on your devices.

4. In the **Dell triggered collections** section, by default, the option to allow a technical support agent to remotely initiate a collection on PowerEdge servers and PowerSwitch switches is selected. But, if you do not want to allow such a collection, clear the check box.
5. In the **Upload** section, by default, the option to allow secure connect gateway to automatically send the information that is collected to the Dell backend is selected. But, if you want to manually send the collections to the backend, clear the check box.
6. Click **Apply**.
7. To configure CIFS location, perform the following steps in the **PowerEdge MX7000 Chassis** section:
Secure connect gateway supports IPV4 for PowerEdge MX7000 Chassis.
 - a. Enter the file share path or location.
 - b. Enter the username and password that is required to access the location.
 - c. Click **Apply**.


Configure email notifications

About this task

On the **Email notifications** page, you can configure secure connect gateway to send email notifications for the following in your preferred language:

- Adapter connection status
- Results from recurring gateway health checks
- Maintenance mode
- Device validation status
- Periodic inventory validation
- Staging or Inactive states
- Blocked devices
- Alert delivery notifications
 - Alert delivery failures
 - Alert delivery confirmation
 - Remote support connections

You can receive email notifications in the following languages: Arabic, Bahasa Indonesia, Simplified Chinese, Traditional Chinese, Czech, Danish, Dutch, English, Finnish, French, Canadian French, German, Greek, Hebrew, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Brazilian Portuguese, Russian, Slovak, Spanish, Latin American Spanish, Swedish, Thai, or Turkish.

 **NOTE:** The **Gateway health check results** email notification is received only in English.

To receive email notifications through your company SMTP server, see [Configure SMTP server settings](#).

Steps

1. Go to **Settings > Email notifications**.
2. From the **Preferred email language** list, select the language in which you want to receive your email.
3. Select the email notification purpose.
4. Click **Apply**.



Types of email notifications

The following table provides a summary of the different types of email notifications that are sent by secure connect gateway. The email notifications may include resolution steps or workaround, if applicable.

Table 8. Types of email notifications

Email type	Reason
Administrator account status	Administrator account is locked after five failed attempts and when the account is unlocked.
Alert from devices in Staging and Inactive states	Secure connect gateway has detected that the monitoring and automatic service request creation capabilities are limited for some of your devices.
Automatic maintenance mode	The number of alerts that are generated by a device exceed the predefined threshold and secure connect gateway placed the device automatically in maintenance mode.
Connect Home failover options test status	Secure connect gateway successfully sent a file to the backend while testing the Connect Home failover methods.
Gateway health check results	The gateway health check is performed everyday at 11 p.m, and the heartbeat connection status is performed every 24 hours. For steps to manually request an email with information about the gateway health, see Request gateway health status through an email .


Table 8. Types of email notifications (continued)

Email type	Reason
	 NOTE: An email message is sent even when no issue is detected during the health check.
Device status alert	<p>If fewer than 10 devices have issues, an email is sent at 11 p.m. everyday with the issue details and the possible resolution steps. If more than 10 devices have issues, only the issue summary is displayed.</p>  NOTE: The email is sent only for device setup or configuration issues.
File transfer status	Secure connect gateway is unable to send files to the backend.
File transfer status notification	Secure connect gateway successfully sent files to the backend.
Final message regarding unresolved issue with the adapter	If the issue is not resolved within six hours, after the issue was detected.
Inactive notification	Secure connect gateway is not monitoring any device and no device has been added in the last 30 days.
Inventory validation summary	Secure connect gateway validated your device inventory for connectivity, automated service request creation, and telemetry collections capabilities.
Issue with the adapter	Within five minutes after an adapter connectivity issue is detected.
Policy Manager approval	Policy Manager is configured to request your approval. For example, if you configure policy manager to prompt you for approval when a technical support agent has initiated a remote session on a device, an email is sent.
Policy Manager status	Secure connect gateway is unable to connect to the server on which Policy Manager is installed.
Registration confirmation and welcome email	Registration of secure connect gateway is completed successfully.
Remote session status	Technical support has initiated or ended a remote session on a device.
Resumed normal operations with the adapter	If the issue is resolved within six hours, after the issue was detected.
SMTP configuration saved	Secure connect gateway successfully saved the SMTP server settings.
SMTP configuration test	Secure connect gateway successfully connected to the SMTP server.
Unable to collect telemetry	A service request is created automatically for a device, but secure connect gateway is unable to collect telemetry from the device.
Unable to send the collected telemetry to the backend	A service request is created automatically for a device, but secure connect gateway is unable to send the collected telemetry from the device to the backend.
Update available	Updates are available for docker, operating system, or application configuration files.

Request gateway health status through an email

About this task

By default, secure connect gateway verifies the overall health status of the gateway everyday at 11 p.m. However, you can manually request to receive information about the health status through an email, when necessary.

 **NOTE:** An email message is sent even when no issue is detected during the health check.

Steps

1. Open the terminal window on a system running the Linux operating system.
2. Run the following command to generate an access token:

```
curl -k -X POST -H 'accept: application/json' https://<<IP address of
secure connect gateway virtual appliance>>:5700/SupportAssist/api/v2/auth/token -d
'{"username":"<<username of the administrator account>>", "password":"<<password
of the administrator account>>"}' 2>/dev/null | grep accessToken | sed 's/
^.*accessToken" : "\([^"]*\)",.*$/\1/g'
```

3. Run the following command to view the health status and receive the status through an email:

```
curl -k -H "Authorization: Bearer <<token generated in step 2>>" 'https://<<IP
address of secure connect gateway virtual appliance>>:5700/SupportAssist/api/v2/
service/healthstatus?emailOptin=yes'
```

4. Optionally, you can create and run a shell file with the following commands:

```
TOKEN=`curl -k -X POST -H 'accept: application/json' https://<<IP address of
secure connect gateway virtual appliance>>:5700/SupportAssist/api/v2/auth/token -d
'{"username":"<<username of the administrator account>>", "password":"<<password
of the administrator account>>"}' 2>/dev/null | grep accessToken | sed 's/
^.*accessToken" : "\([^"]*\)",.*$/\1/g`


echo "TOKEN:.$TOKEN"

echo ""
curl -k -H "Authorization: Bearer $TOKEN" 'https://<<IP address of secure
connect gateway virtual appliance>>:5700/SupportAssist/api/v2/service/healthstatus?
emailOptin=yes'
echo ""
```

Configure API settings

About this task

Enabling REST API interfaces allows you to integrate secure connect gateway with your data center tools and applications. For more information, see the *Secure Connect Gateway REST API Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

 **NOTE:** You can perform a maximum of 10 operations such as adding devices and collecting telemetry in parallel. Before you query the operation status and operation ID, ensure that there is a minimum delay of five seconds.

Steps

1. Go to **Settings > API settings**.
2. Select the **Enable API interfaces for this gateway** check box and click **Apply**.

Configure alert delivery settings

About this task

When an alert is generated, secure connect gateway receives the alert data from the device through the listener services. The data is sent to the backend through the Managed File Transfer (MFT) service or FTPS. On the **Alert delivery settings** page, you can configure the failover methods and listener services. You can also configure secure connect gateway to send email notifications with the alert data when the alert data is sent to the backend.

Steps

1. Go to **Settings > Alert delivery settings**.
2. To enable FTPS as a failover method to transfer the alert data, select the **Enable Failover FTPS** check box in the **Failover Options** section, test the connection, and then click **Apply**.

NOTE: By default, the **Enable File Transfer** check box is selected to allow file transfers through MFT.

3. To receive email notifications, perform the following steps:
 - a. Ensure that SMTP settings are configured for the device.
 - b. Select the device model.
NOTE: If you select **DEFAULT**, the settings are applied for all device models.
 - c. Select the required check box to receive the alert data and an email notification when the data is sent to the backend.
 - d. Click **Apply**.
4. In the **Listening services** section, enable or disable the required services, and click **OK**.

By default all the listener services are enabled. The four available listener services are HTTPS, FTP, SNMP, and Redfish services.

- NOTE:**
- Before you disable a service, ensure that none of your devices are using that service. You cannot disable a listening service that is used by a device.
 - If the SNMP and Redfish listening services are disabled, you cannot add servers and networking devices.
 - If you enable the SNMP or Redfish listening service after disabling both of them, the service enables in 30 s.

5. To disable file transfers between the secure connect gateway, and the backend, go to the **Call home** section and ensure that the **Enable primary MFT** channel and **Enable failover FTPS** check boxes are not selected.

Configure automated tasks

About this task

On the **Automated tasks** page, you can schedule when secure connect gateway must initiate a periodic collection, purge the collected telemetry, and validate your device inventory.

- NOTE:** If you want secure connect gateway to collect telemetry on a weekly basis and purge the collected telemetry based on the number of days since the telemetry was collected, it is recommended to allocate 250 GB hard drive space when you deploy or install secure connect gateway. So, if you want secure connect gateway to collect telemetry on a weekly basis, it is recommended to purge the collected telemetry based on the size of the total collected telemetry.

You can also enable or disable analytic collections.

- NOTE:** An analytic collection is performed on iDRAC9 or later installed with firmware version 4.00.00.00 or later, SMART capable drivers, and an active Datacenter license.

Steps

1. Go to **Settings > Automated tasks**.
2. To schedule periodic collections, ensure that the **Collect system state information** check box is selected and perform one of the following steps:

- To schedule weekly collections, select the respective option and then select the day of the week on which the telemetry must be collected.
 - To schedule monthly collections, select the respective option and then select the day of the month on which the telemetry must be collected.
3. To schedule the interval in which the collected telemetry must be purged, perform one of the following steps in the **Purge collected telemetry** section:
 - Select the number of days after which a collection can be purged.
 - Select the size limit of the total telemetry collected. Secure connect gateway automatically purges the oldest collection to ensure that the total size is within the limit.
 4. By default, analytic collections are enabled and performed on a random day every week at 1 a.m.. Clear the **Automatically collect data for analytics** check box to disable analytic collections.
 5. To schedule inventory validation, ensure that the **Automatically check connections between this gateway and your monitored devices** check box is selected, and then select the required day of a month.
 6. To set iSM as the default service for automatic case creation on servers globally, select **Prefer iSM globally**.
Before configuring iSM, ensure the following:
 - iSM is installed, and the iSM services are running.
 - iDRAC access via Host OS is enabled in iSM.
 - SNMP trap configuration for alerts is enabled in iDRAC.
- NOTE:**
- iSM can be used as a default service for 14th generation PowerEdge servers or later. For automatic case creation, the iSM version must be 5.3 or later.
 - To configure iSM on multiple devices, you must enable **Prefer iSM globally** and manually run an inventory validation or wait for a periodic inventory validation.
 - Devices that connect to secure connect gateway through an adapter do not support configuring iSM.
7. To schedule a gateway health check, select the required time and day of the week in the **Check gateway health** section. The default time for the gateway health check is 11:00 PM everyday.
 8. Click **Apply**.

User Management and LDAP configuration

About this task

In the previous versions, the secure connect gateway did not have access control on its features. Any logged-in user can access all features within the gateway. The secure connect gateway 5.28. release introduces role-based access control (RBAC), which implements specific restrictions based on user roles, thereby providing secure access.

The roles and their privileges are as follows:

- **Super Admin** : This role does not have any restrictions. There is only one super admin in the gateway.
- **Administrator** : This role has certain restrictions on user management. Administrators cannot edit or delete other user accounts.
- **Non-Administrator** : This role has read-only access to all features, but does not permit access to the settings option in the secure connect gateway. Non-administrators are restricted to performing collections on devices only.

This section is divided into three tabs: Local users, LDAP users, and LDAP configuration.

- NOTE:** It is best practice to assign individual login credentials to each user instead of sharing a single account. When multiple users share one account and a second login occurs while the first session is still active, the system automatically logs out the previous session without warning. Only the most recent login remains active. This can cause confusion and disrupt ongoing work. Dedicated user accounts help maintain session stability, improve security, and ensure appropriate access control.

Local Users Management

About this task

This section outlines the steps to manage local users within the system, including how to create, edit, and delete local users.

Local users are displayed in a table format with the following columns:

Columns	Description
Email Address	The email associated with the user.
User ID	The unique identifier for the user.
First Name	The user's first name.
Last Name	The user's last name.
Local Admin	Indicates whether the user has local administrator rights.
Last Login	The date and time of the user's most recent login.

Creating a local user

About this task

The task of creating a local user involves setting up a new user account within the system, allowing access to specific functionalities based on the user's assigned role.

Steps

1. Go to the **User management & LDAP configuration** section.
2. Select the **Local users** and, click **Add** .
The user creation form is displayed.
3. Enter the required fields, including User ID, First Name, Last Name, Email, Phone (Optional), and Password.
4. Check or uncheck the **Local Administrator** checkbox to assign the user as either a Local Administrator or Non-Administrator.
5. Click **Save**.

Results

The new user account is created successfully.


Editing a Local user


About this task

The task of editing a local user involves modifying the details of an existing user account within the system.

Steps

1. Go to the **User management & LDAP configuration** section.
2. Select the **Local users** , to view the list of users.
3. Select the user that you want to edit in the table.

 **NOTE:** Only the Super Admin has the authority to edit local users.

 **NOTE:** A logged-in user with Administrator rights can edit their own account, and upon successful modification, the system logs them out of the secure connect gateway.

4. Click **Edit** icon next to the users name and modify the required fields, including User ID, First Name, Last Name, Email, Phone, Password, and Local Administrator Rights.

Results

The user account is edited successfully.


Deleting a local user

About this task

The task of deleting a local user involves removing an existing user account from the system.

Steps

1. Go to the **User management & LDAP configuration** section.
2. Select the **Local users**, to view the list of users.
3. Select the user that you want to delete in the table.

 **NOTE:** Only the Super Admin has the authority to delete local users.

 **NOTE:** A logged-in user with Administrator rights can delete their own account, which logs them out of the secure connect gateway upon deletion.

4. Click **Delete**, and confirm the deletion in the appeared window by clicking **Yes**.

Results

The user account is deleted successfully.

LDAP Users Management

About this task

This section outline how to manage LDAP users and groups, including how to add, edit, and delete them within the system.

LDAP users and groups are listed in separate tables in the LDAP Users tab:

Columns	Description
Email Address	The email associated with the user.
User ID	The unique identifier for the user.
First Name	The user's first name.
Last Name	The user's last name.
Local Admin	Indicates whether the user has local administrator rights.
Last Login	The date and time of the user's most recent login.

Columns	Description
Email Address	The email associated associated with the LDAP group.
Group ID	Shows the unique identifier for each LDAP group.
Group Name	Lists the name of the LDAP group.
Local Admin	Indicates whether the user has local administrator rights.

Adding an LDAP User/Group

About this task


This section outlines the procedure of adding an LDAP User/Group.

Steps

1. Go to **User management & LDAP configuration** section.
2. Select the **LDAP Users** and, click **Add**.

The list of LDAP user/groups is displayed.

3. From the **Select LDAP user/group** list, choose the required option.
4. To add specific users and groups, click **Search** and add the required users and groups.
5. Check or uncheck the **Local Administrator** checkbox to assign the user as either a Local Administrator or Non-Administrator.
6. Click **Save** to add the LDAP user or group.

 **NOTE:** The user rights are looked up in the whitelisted users list instead of whitelisted groups as priority during login to check for Administrator rights.


Editing an LDAP user/group


About this task

The task of editing a local user involves modifying the details of an existing user account within the system.

Steps

1. Go to the **User management & LDAP configuration** section.
2. Select the **LDAP user/group**, to view the list of LDAP user/group.
3. Select the LDAP user/group that you want to edit in the table.

 **NOTE:** Only the Super Admin has the authority to edit LDAP user/group.

 **NOTE:** A logged-in user with Administrator rights can edit their own account, and upon successful modification, the system logs them out of the secure connect gateway.

4. To edit the LDAP user/group **Local Administrator** rights, click **Set as Administrator** or **Set as Non Administrator**.
5. A confirmation window appeared. Select **Yes** to proceed with the changes.


Deleting an LDAP user/group


About this task

The task of deleting an LDAP user/group involves removing an existing user account from the system.

Steps

1. Go to **User management & LDAP configuration** section.
2. Select the **LADP Users /Group**, to view the list of LADP Users /Group.
3. Select the LADP Users /Group that you want to delete in the table.

 **NOTE:** Only the Super Admin has the authority to delete LADP Users /Group.

 **NOTE:** A logged-in user with Administrator rights can delete their own account, which logs them out of the Secure Connect Gateway upon deletion.

4. Click **Delete**, and confirm the deletion in the appeared window by selecting **Yes**.
The LADP Users /Group account is deleted successfully.

Configure update settings

About this task

By default, secure connect gateway installs the latest version. Enable this option to download and install the previous version if the current version is two or more versions older.


Steps

1. Go to **Settings > Update setting**.
2. Select the checkbox **Enable the update to the previous version**.
3. Click **Apply** to save the configuration.

Configure LDAP settings


About this task

By default, you can sign in to secure connect gateway only using the administrator account credentials. Configuring LDAP settings allows users to sign in to secure connect gateway using their network credentials. After you configure the LDAP settings, you can configure access to specific users or user groups in the LDAP server.


 **NOTE:** You can configure only one LDAP server at a time. If you do not configure the access for specific users or user groups, all the users in the LDAP server can access secure connect gateway using their network credentials. Also, If you change the LDAP server details, access to the users in the previously configured LDAP server is automatically disabled.

Steps


1. Go to **Settings > LDAP configuration**.
2. On the **LDAP configuration** page, perform the following steps:
 - a. Select one of the following options.
 - **LDAP**—allows users in an LDAP network to sign in only using their network credentials.
 - **Localhost and LDAP**—allows signing in using the administrator account credentials or the users in an LDAP network to sign in using their network credentials.

 **NOTE:** When the LDAP configuration option is modified, the user is logged out of the gateway. Any other active users are also logged out without notification or warning.

- b. Select the LDAP server type and enter the required credentials.
- c. To allow secure connect gateway to automatically download and install the SSL certificates for your LDAP server, select the **Enable and autoconfigure SSL** check box.

 **NOTE:** It is recommended that you enable and autoconfigure SSL to ensure that LDAP authentication sessions are encrypted end to end.

- d. Click **Test connection**.
 - e. If the connection is successful, click **Apply**.
The domain display name is displayed in the **Domain** list on the sign-in page.
3. To provide access to specific users or user groups in the LDAP server, perform the following steps on the **LDAP user management** page:
 - a. Click **Add**.
 - b. From the **Select LDAP user/group** list, select the required option.
 - c. Search and add users of a group and click **Add**.
 4. To import information about the users or user groups from a CSV file, perform the following steps on the **LDAP user management** page:
 - a. Click **Import**.
 - b. Select the user type and upload the file.

 **NOTE:** UTF-8 encoded CSV file is not supported.
 - c. Click **Import**.
 5. To save the information about the users or user groups in the **LDAP User Management** as a CSV file, select the users or user groups and then click **Export all**.

Configure backup settings

About this task

Secure Connect Gateway allows you to save a backup of secure connect gateway system settings through the **Backup configuration** page. You can use this backup to restore a system after reinstallation of secure connect gateway in case of a critical issue.

You can save the backup on a local system or on the network share. Recurring backup can be scheduled only with the network share option. The backup can be restored if the secure connect gateway version and IP address of the system are the same.

NOTE: The following are not backed up and restored for security reasons:

- Device credentials
- SNMP v3 settings
- Certificate details
- Proxy Server details
- Backup and restore configurations
- Preferred contact details
- SMTP and adapter credentials
- LDAP, and Policy Manager
- Credential vault API key
- RSA SecurID certificate and access key that is required for two-factor authentication

Steps

1. Go to **Settings > Backup configuration**.
2. To save the backup on the local system, select **Local system** and click **Start backup**. You can download the .zip file to the local system after the backup is complete.
3. To manually save the backup on the network share, select **Network share**, click **Manually**, and perform the following steps:
 - a. Enter the network location where you want to save the backup.
 - b. Enter the username, password, share type, and click **Check location**.

NOTE: The supported share types are—CIFS, HTTPS, and SCP.

NOTE: If you selected **HTTPS** as the share type and if you are an anonymous user, enter any username and password to configure the network share and backup your data.

The **Schedule recurring backup** section is displayed if the entered location is valid.

4. To use a credential vault to backup your credentials, select **Network share**, click **Use a credential vault**, and perform the following steps:
 - a. Enter the network location where you want to save the backup.
 - b. Select the vault to backup your credentials.
 - c. Enter the details as follows:
 - **For Conjur or Azure Key Vault:** Enter the username identifier and password identifier as configured in the vault.
 - **For CCP Vault:** Enter the account identifier as configured in the vault.
 - **For HashiCorp Vault:** Enter the secret path, username identifier, and password identifier as configured in the vault.
 - d. Select the share type and click **Check location**.

NOTE: The supported share types are—CIFS, HTTPS, and SCP.

NOTE: If you selected **HTTPS** as the share type and if you are an anonymous user, enter any username and password to configure the network share and backup your data.

The **Schedule recurring backup** section is displayed if the entered location is valid.

5. To schedule recurring backups, select the frequency, days, time, and click **Schedule**. If you do not want to schedule recurring backups, click **Skip and backup now**.

Results




The backup location and recurring backup information is displayed on the **Backup configuration** page. You can also edit or delete the scheduled backup frequency.

Configuring Syslog Server for Secure Connect Gateway

About this task

The secure connect gateway system enables users to send audit events to a syslog or Splunk server, providing a centralized logging solution for improved monitoring and analysis.

Steps

1. Go to the **Settings** and expand it.
2. Scroll down to the **Syslog Configuration** section and click the switch to enable syslog.
 **NOTE:** Ensure the correct syslog server information is entered, including the host, port, and authentication details.
3. Select the log types that you want to send to the syslog server.
 **NOTE:** Choose the categories of audit events to send to the syslog server based on your specific needs.
 **NOTE:** Set the minimum syslog log level type for each category to filter the events sent to the syslog server.
4. To configure **Application** mode, select one or more of the following options under the **Application** mode section:
 - GATEWAY_ACTIVITY
 - FILE_TRANSFER
 - ALERT_DELIVERY
5. To configure **Virtual edition** mode, select one or more of the following options under the **Virtual edition** mode section:
 - GATEWAY_ACTIVITY
 - FILE_TRANSFER
 - REMOTE_SUPPORT
 - REMOTE_ACTIONS
6. For **Facility Codes**, you can enter input like LOCAL0, which is commonly used. For more information about facility codes, see the following table:


Facility Code	Facility Name	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authorization messages (legacy)
5	syslog	Messages generated internally by syslog
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon (cron and at)

Facility Code	Facility Name	Description
10	authpriv	Security/authorization messages (private)
11	ftp	FTP daemon
12	ntp	Network Time Protocol
13	audit	Log audit records
14	alert	Log alert messages
15	clock	Clock daemon (note: different from cron)
16	local0	Local use 0 (customizable)
17	local1	Local use 1 (customizable)
18	local2	Local use 2 (customizable)
19	local3	Local use 3 (customizable)
20	local4	Local use 4 (customizable)
21	local5	Local use 5 (customizable)
22	local6	Local use 6 (customizable)
23	local7	Local use 7 (customizable)

 **NOTE:** These facility codes are standardized in the syslog protocol (RFC 5424).


7. To choose the **Log Level Type**, select one of the following options from the dropdown:

- ERROR
- WARN
- INFO
- DEBUG
- TRACE

 **NOTE:** When syslog is enabled, secure connect gateway continues to write events to the local Virtual machine (visible under the Audit tab of the SCG UI) while also sending selected audit events to the syslog server. Events are mapped to syslog severity levels based on the chosen **Log Level Type**. If an secure connect gateway event has a severity level, it is preserved. Otherwise, it maps to **Info** for success, **Warning** or **Error** for failure, and **Info** for events with no obvious category.


8. To exclude Stack Trace Data, set to **True**, this option ensures that only the class name and associated message are in the log entries. You can select **Yes** or **No** from the dropdown.

9. The default server port is set to 514. If you are using TLS, the default port changes to 6514. Also, you have the option to configure the syslog server with a custom port of your choice when using TLS.

 **NOTE:** If using TLS encryption, ensure that the certificate is valid and trusted by the syslog server.

10. The default suffix pattern is configured as follows: `scg-syslog %thread: %-5level %logger{36} - %msg%n`. Users have the option to modify the **scg-syslog** portion of this pattern.

11. To configure and enter the syslog server information, provide the server details in the format mentioned below:

 **NOTE:** The below format is for reference only. Ensure the information entered matches your specific server configurations.

- **Server Display Name:** MySyslogServer
- **Server Host Name:** syslog.example.com
- **Exclude Stack Trace Data:** true
- **Suffix Pattern:** `scg-syslog %thread: %-5level %logger {36} - %msg%n`
- **Syslog Server Port:** 514 (or 6514 for TLS)

- **Log Level Type:** INFO
- **Syslog Facility:** local0
- **TLS Encryption:** true (requires importing the syslog client certificate file)
- **Recommendation:** For enhanced security, use the TLS option.

 **NOTE:** Set the minimum syslog level type ERROR, WARN, INFO, DEBUG, TRACE according to your requirements.

Configuring alert and event settings

Configuring the alert and event destination of a device ensures that secure connect gateway receives alerts or events from the device. Secure connect gateway can automatically configure the alert and event destination of a server. If it fails, you can configure the alert destination using a script file or by accessing the alert trap service.

NOTE:


- For iDRAC9 running firmware version 5.x or later, secure connect gateway uses the Redfish protocol to receive alert and event information. If Redfish protocol is disabled, SNMP protocol is used to receive alert and event information from the device.
- Alerts and events are supported only on devices that are configured with SNMP v2 and SNMP v3.

For information about configuring the alert destination for a PowerEdge VRTX, PowerEdge FX2, or PowerEdge M1000E chassis, go to the [Chassis Management Controller](#) documentation page. For information about configuring the alert destination for PowerEdge MX7000 chassis, go to the [Chassis Management Controller](#) documentation page, click **Dell OpenManage Enterprise**, and then click **Dell OpenManage Enterprise-Modular**.

For information about configuring the alert destination for an iDRAC, see the *Integrated Dell Remote Access Controller User's Guide* available on the [iDRAC Manuals](#) page.

Manually configure alert destination of a networking device

About this task

 **NOTE:** The steps to configure the alert destination of networking devices may vary based on the model. For information about configuring the alert destination of a specific model, see the device-specific documentation.

Steps

- Log in to the device using a terminal emulator such as PuTTY.
- Run `configure`.
- Run `snmp-server host <IP address of the local system> traps version 2`.
- To verify if the alert destination is configured successfully, run `show running-config snmp`.
The list of alert destinations that are configured on the device is displayed.

Manually configure alert destination using the script file for a server running Linux operating system

Prerequisites

- Ensure that Net-SNMP is installed on the system. See [Install Net-SNMP on a server running Linux operating system](#).
- Ensure that you have root privileges on the device.

Steps

- In the install directory on the local system, go to the `/opt/dell/secureconnectgateway/scripts` folder.
- Copy and paste `LinuxSNMPConfig.sh` in the desired location.
- Log in to the terminal window using root privileges.

4. Run the script file on the device using the following syntax: `sh LinuxSNMPConfig.sh -d <IP address of the local system>`. For example, `sh LinuxSNMPConfig.sh -d 10.10.10.10`.

Install Net-SNMP on a server running Linux operating system

Prerequisites

Log in to the server with a user account that has root privileges.

About this task

Secure connect gateway receives alerts that are forwarded from remote devices through an SNMP agent. Net-SNMP consists of a suite of SNMP tools, including an SNMP agent. On devices running Linux operating system, Net-SNMP must be installed to allow secure connect gateway to receive alerts.

Steps

1. Open the terminal window on the device running the Linux operating system.
2. Enter the following commands based on the operating system:
 - Red Hat Enterprise Linux, CentOS, and VMware ESX: `yum install net-snmp`
 - Oracle Linux: `rpm -ivh net-snmp-x.x-xx.x.x.xxx.x86_64.rpm`, where `x.x-xx.x.x.xxx.x` represents the version number in the rpm file name.
 - SUSE Linux Enterprise Server:
 - a. `zypper addrepo http://download.opensuse.org/repositories/net-snmp:factory/SLE_12/net-snmp:factory.repo`
 - b. `zypper refresh`
 - c. `zypper install net-snmp`


Manually configure alert destination by accessing the SNMP trap service for a server running Linux operating system

Steps

1. Log in to the terminal window using root privileges.
2. Run `rpm -qa | grep snmp`, and ensure that the **net-snmp** package is installed.
3. Run `cd /etc/snmp` to go to the SNMP directory.
4. Open **snmpd.conf** in the VI editor (**vi snmpd.conf**).
5. Search **snmpd.conf** for **# group context sec.model sec.level prefix read write notif** and ensure that the values for **read**, **write**, and **notif** are set to **all**.
6. At the end of the **snmpd.conf** file, before **Further Information**, add an entry in the following format: `Trapsink <IP address of the local system> <community string>`, for example, `trapsink 10.94.174.190 public`.
7. Run `service snmpd restart` to restart the SNMP service.

Updating Secure Connect Gateway

Secure connect gateway displays banner notifications when an update is available. You also receive a mail informing you of a new available update. You can download and install the updates immediately or schedule the updates to be installed later. You can also manually check for updates from the **About** page. Apart from updates to secure connect gateway, the **About** page also displays patch updates to the operating system which are independent of the secure connect gateway updates.


 **NOTE:** It is recommended that you capture snapshots of the virtual appliance before you install the updates. You can use the snapshot to restore secure connect gateway to a previous state, if necessary.

Install hotfix updates

About this task

A hotfix is a quickfix update to resolve certain system issues. The **About** page lists the hotfixes available, severity, and the description of the hotfixes.

Steps


1. Go to **About > Hotfix updates**.
2. Select the hotfixes that you want to install on your system and click **Apply**.
 **NOTE:** All hotfixes are available for appliance systems. Host-based hotfixes are not available for Docker and Podman systems.
3. If you have already installed certain hotfix updates, they are listed under **Applied hotfix updates**. To uninstall any installed hotfix, select the hotfix, and click **Remove**. You cannot select and uninstall crucial hotfix updates.

Update Host OS Patch update- when available

About this task

This is applicable to gateways running SUSE Linux Enterprise Server 15 SP6 as the host OS.

Steps

1. In the notification bar, click **Learn more** or go to the **About** page to view the list of available **Host OS Patch** updates.
2. Click **Apply** to update the **Host OS Patch**.
3. When you receive the prompt to update patches, click **Continue**.
The update process begins, and you are automatically logged out to install the updates. When you log in again, a success message appears at the top of the header.
 **NOTE:** If the Host OS patch update fails, follow the above steps to retry the update. If the issue persists, contact Dell Support for further assistance.

Upgrade to SUSE Linux Enterprise Server 15


About this task

If you upgrade from a previous release of secure connect gateway virtual edition to version 5.28 (or above), the virtual machine OS is upgraded online to SUSE Linux Enterprise Server 15 SP6.


Steps

If the gateway feature update is successful but the SUSE Linux Enterprise Server 15 SP6 Host OS update fails, perform the following steps:

- a. To initiate the SUSE Linux Enterprise Server 15 SP6 Host OS update, click **Retry SUSE Linux Enterprise Server 15 SP6 Host OS update** at the top of the header.

 **NOTE:** Logs for the upgrade are located in `/var/log/esrs/slesupgrade/`.

- b. You are prompted to download the package. Click **Download** to start the download process.
- c. To view the progress of the download, click the **Check progress** link on the banner at the top of the screen. The progress bar and percentage are displayed.
- d. Once updates are successfully downloaded, click **Install** on the banner. A screen appears with the spinner which shows the OS upgrade progress. You are then automatically logged out to install the updates. A success message is displayed at the top of the screen when you log in again.

 **NOTE:** If the update fails, follow the above steps to retry the SUSE Linux Enterprise Server 15 SP6 Host OS update. If the issue persists, contact Dell Support for further assistance.

Update Secure connect gateway for appliance


Steps


1. In the notification banner or the **About** page, click **Update now**.
2. In the **Update this secure connect gateway** window, click **Download now**.
3. After the updates are downloaded, perform one of the following steps:
 - Click **Install now** to install the updates immediately.
 - Click **Schedule for later** to install the updates later.

If you clicked **Install now**, the upgrade process is initiated and you are automatically logged out to install the updates. A success message is displayed on top of the header when you log in again. If you clicked **Schedule for later**, you are prompted to select the date and time when the updates must be installed.

4. If you clicked, **Schedule for later**, perform the following steps:
 - a. Select the date and time when the updates must be installed.
 - b. Click **Confirm schedule**.

A message with the scheduled date and time is displayed. A link to reschedule the updates is also displayed.

 **NOTE:** The option to schedule an update displays the time as per the time zone from which you access the secure connect gateway user interface. However, the updates are installed according to the time zone in which the secure connect gateway virtual appliance is deployed. For example, if the appliance is in EST time zone and you scheduled an update for March 10 at 2:00 PM from the CST time zone, the update is installed on March 10 at 4:00 PM EST.

 **NOTE:** When you select **Enable upgrade to previous version** in the **Update settings**, you can view and download only the version just before the current one—if your current version is at least two versions behind. This setting resets automatically after a successful upgrade.

Update Secure connect gateway for Docker and Podman

Steps

1. Download the latest bin file for Docker and Podman on the [Secure Connect Gateway - Drivers and Downloads](#) page.
2. Run the `./SCG-5.xx.xx.xx.bin --upgrade` command.
3. After the update, verify that the container is running with the latest images.

Results

The secure connect gateway user interface is available with the updated version. You can check the updated version on the **About** page.

Update Secure connect gateway for Kubernetes

About this task

Perform the following steps to update secure connect gateway on the RKE2 server node:

Steps

1. Download the latest bin file for Kubernetes on the [Secure Connect Gateway - Drivers and Downloads](#) page.
2. Run the `./SCG-5.xx.xx.xx-RKE2.bin --extract` command to extract the files.
3. To import the .tar images on the server node, run the `ctr -n= k8s.io image import SCG/images.tar` command.
 - a. If you have multiple nodes, to copy images on the agent nodes, run the `scp images.tar root@<worker_node_ip>:/root` command.
 - b. To import images on the agent nodes, run the `ctr -n= k8s.io image import images.tar` command.
4. Run the `./SCG-5.xx.xx.xx.bin --upgrade` command.
5. To verify that the container is running with the latest images, run the `kubectl get pods -n scg` command.

Results

The secure connect gateway user interface is available with the updated version. You can check the updated version on the **About** page.

Secure Connect Gateway resources


This section provides information about the documentation resources and other useful links that provide more information about secure connect gateway.

Table 9. Secure Connect Gateway resources

For more information about	See	Available at
Minimum system and network requirements, and deployment instructions	Deployment Guide	Secure Connect Gateway - Virtual Edition documentation page
Features available in secure connect gateway and how to use the features	User's Guide	
List of supported devices, protocols, firmware versions, and operating systems	Support Matrix	
List of attributes that are reported in the telemetry that is collected by secure connect gateway from different device types	Reportable Items	
New features, enhancements, known issues, and limitations in the release	Release Notes	
Secure connect gateway infrastructure, alert processing, and automatic service request creation policies	Infrastructure and Alert Policy Guide	
Integrating data center tools and applications with secure connect gateway using Representational State Transfer (REST) APIs	REST API Guide	
Troubleshooting issues that may occur while using secure connect gateway	Troubleshooting Guide	
Procedural or reference information to help with using the application	Online Help	Secure connect gateway user interface
Peer-to-peer questions about secure connect gateway	Community forum	Secure Connect Gateway community
Video tutorials to learn about the features of secure connect gateway — virtual edition	Secure Connect Gateway Virtual Edition playlist	YouTube


Contacting Dell Technologies

About this task

 **NOTE:** If you do not have an active Internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell Technologies product catalog.

Dell Technologies provides several online and telephone-based support and service options. Availability varies by country or region and product, and some services may not be available in your area.

Steps

1. To contact Dell Technologies for sales, technical support, or customer service issues, perform the following steps:
 - a. Go to [Dell Support](#).
 - b. Select your country or region in the selection list at the bottom of the page.
 - c. Click **Contact Support** and select the appropriate support link.
 2. To find manuals and documents, perform the following steps:
 - a. Go to [Dell Support](#).
 - b. Click **Browse all products**.
 - c. Select the appropriate product category and then select the desired product.
 - d. To view or download the manuals and documents, click the **Documentation** tab.
-  **NOTE:** You can also directly access the manuals and documents for Serviceability Tools from the [Serviceability Tools](#) page.