


Secure Connect Gateway 5.x — Virtual Edition

Support Matrix

Notes, cautions, and warnings

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

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

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

Contents

Chapter 1: Introduction.....	5
Version.....	5
Release history.....	5
Document purpose.....	6
Secure Connect Gateway capabilities available with Dell Technologies service contracts.....	6
Methods of adding devices.....	6
 Chapter 2: New and enhanced features.....	 9
v5.22.00.18.....	9
v5.20.00.10.....	9
v5.18.00.20.....	9
v5.16.00.14.....	10
v5.14.00.16.....	10
v5.14.00.10.....	10
v5.12.00.10.....	10
v5.10.00.10.....	11
 Chapter 3: Minimum requirements to deploy and use Secure Connect Gateway.....	 12
System requirements.....	12
Network requirements.....	13
Supported browsers.....	16
Supported hypervisors.....	16
 Chapter 4: Supported servers.....	 17
16th generation PowerEdge servers.....	17
15th generation PowerEdge servers.....	18
14th generation PowerEdge servers.....	19
13th generation PowerEdge servers.....	19
12th generation PowerEdge servers.....	20
11th generation PowerEdge servers.....	21
10th generation PowerEdge servers.....	21
9th generation PowerEdge servers.....	22
C series PowerEdge servers.....	22
XE series PowerEdge servers.....	23
XR series PowerEdge servers.....	23
Datacenter Scalable Solutions.....	24
AX nodes.....	24
PowerVault devices.....	25
 Chapter 5: Supported Integrated Remote Access Controllers (iDRAC).....	 26
 Chapter 6: Supported chassis.....	 27
 Chapter 7: Supported data storage devices.....	 28


Enterprise storage devices.....	29
Entry level and midrange storage devices.....	31
PS Series or EqualLogic devices.....	32
PowerVault MD3 and ME4 devices.....	33
SC series or Dell Compellent devices.....	34
Network Attached Storage devices.....	35
PowerVault tape libraries.....	35
Networking storage devices.....	36
Legacy storage devices.....	37
Storage software.....	37
Analytic software.....	38
Support software.....	39
Chapter 8: Supported networking switches.....	41
PowerSwitch switches.....	41
PowerSwitch switches with Enterprise SONiC operating system.....	43
PowerConnect switches.....	43
Dell Force10 switches.....	45
Brocade switches.....	46
Cisco Catalyst switches.....	46
Cisco Nexus switches.....	47
Cisco MDS switches.....	47
Chapter 9: Supported hypervisors.....	49
Chapter 10: Supported virtual machines.....	50
Chapter 11: Supported data protection devices.....	51
Chapter 12: Supported direct liquid cooling devices.....	54
Chapter 13: Supported converged and hyperconverged infrastructure appliances.....	55
XC series Web-Scale converged appliances.....	56
Chapter 14: Supported systems management consoles.....	58
Chapter 15: Supported management and monitoring software.....	59
Chapter 16: Supported server operating systems and recommended OMSA version.....	60
Linux and ESXi operating systems.....	60
Chapter 17: Support for OEM devices.....	63
Chapter 18: Secure Connect Gateway resources.....	64
Chapter 19: Contacting Dell Technologies.....	65

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. 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.

Secure connect gateway is verified in Windows Defender Application Control (WDAC) enabled mode to receive alerts and automatically create service requests for iDRAC devices.

 **NOTE:** SupportAssist Enterprise and Secure Remote Services capabilities are now part of secure connect gateway.

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
5.22.00.18	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
5.10.00.10	March 9, 2022

Document purpose

This document provides information about the devices, protocols, firmware versions, and operating systems supported 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.

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 assets 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.	✓	✓
Telemetry collections	System state telemetry that is required to troubleshoot issues is collected from managed devices and securely sent to Dell Technologies.	✓	✓
Proactive response from technical support	A technical support agent proactively contacts you about the service request and helps resolve the issue.	✓	✓
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.	✗	✓
Predictive detection of hardware failures	Dell Technologies provides predictive detection of hardware failures for certain products. 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.	✗	✓

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.
- Inventory and add devices that are managed by system management consoles.
- 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.

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 3. Devices types or models and method of adding devices

Configure the device to connect to secure connect gateway	Add device from secure connect gateway user interface	Configure the device to connect to secure connect gateway or add device from secure connect gateway user interface
AppSync	9th generation of PowerEdge servers and later	Avamar
Cloud Array	Atmos	Connectrix
CloudBoost Virtual Appliance	Centera	Data Domain
CloudIQ Collector	Chassis	Disk Library Mainframe (DLm) series 4 and 5
Converged Management Software	Customer Management Station	Elastic Cloud Storage (ECS)
Data Protection Advisor	Data Computing Appliance	Isilon or PowerScale
Data Protection Appliance	Dell Compellent	MetroNode or VPLEX
DatalQ	Dell Technologies Disk Library (EDL)	Switch Brocade
Dell Storage Resource Manager (SRM)	Disk Library (DL3D)	ViPR
Dell InterConnect Fabric	Disk Library Mainframe (DLm) series 3	ViPR Storage Resource Manager
Dell ML3	EqualLogic	VMAX (VMAX, VMAX v3, and VMAX AFA)
DellSvcs-Auth	Fluid File System	XtremeIO
DellSvcs-Automate	HIT Kit/VSM for VMware	-
DellSvcs-Connector	iDRAC	-
DellSvcs-CPMS	Linux virtual machines	-
DellSvcs-Monitor	Networking	-
Enterprise Copy Data Management	PowerVault MD3 and ME4	-
Networker	RecoverPoint	-
ObjectScale	Switch Cisco	-
PowerFlex Appliance	Symmetrix	-
PowerFlex	vCenter	-
PowerFlex Rack	VNX	-
PowerMaxV4	VNXe	-
PowerPath	Web Scale	-
PowerPath Management Appliance	-	-
PowerProtect Appliance	-	-
PowerProtect Data Manager	-	-
PowerScale SD	-	-
PowerStore*	-	-
PowerVault ME5	-	-
S5000 series servers	-	-

Table 3. Devices types or models and method of adding devices (continued)

Configure the device to connect to secure connect gateway	Add device from secure connect gateway user interface	Configure the device to connect to secure connect gateway or add device from secure connect gateway user interface
PowerFlex	-	-
Streaming Data Platform	-	-
UCC	-	-
Unisphere	-	-
Unity	-	-
Unity VSA	-	-
VxRack SDDC	-	-
VxRail	-	-

*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 5.x for Secure Connect Gateway User's Guide* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.

New and enhanced features

The section provides information about the devices, protocols, firmware versions, and operating systems supported in the current and earlier versions of secure connect gateway — virtual edition.

v5.22.00.18

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.

v5.20.00.10

- 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 version 8.7 operating system on the managed devices.
 - Dell Data Analytics Engine.
- Discontinued support for NFS share type for MX7000 export and application logs.

v5.18.00.20

- 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.

- o Port 8080 for APEX Navigator for Multicloud Storage.
- Removed support for Skyline.

v5.16.00.14

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 Win 2022 operating systems on the managed devices.
- Azure 22H2 OS node.

v5.14.00.16

- Added support for:
 - o iDRAC9 firmware versions 6.10.00.00 and 6.00.30.00 on 15th generation and 14th generation PowerEdge servers.
 - o Firmware version GT280R010-01 for ME4.
 - o Firmware version 3.40 for VRTX.
 - o Firmware version 2.00.00 for MX7000.
 - o OpenManage Enterprise version 3.10.
 - o SLES 15 SP4 operating system on the managed devices and the server or virtual machine on which secure connect gateway is installed.

v5.14.00.10


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.

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 in this release.

- 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

v5.10.00.10

Added support for:

- OpenManage Enterprise version 3.8.2 and 3.8.3
- XC450 and XC7525 appliances
- Firmware versions 5.10.00.00 and 5.00.10.20
- PowerEdge servers R450, R550, R650xs, R750xa, R750xs, XR11, and XR12
- PowerVault ME5 and Dell InterConnect Fabric

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

Minimum requirements to deploy and use Secure Connect Gateway

The following sections provide information about:

- Minimum system and network requirements for the local system to deploy secure connect gateway.
- Minimum system requirements for the local system to enable secure connect gateway to monitor your devices and collect telemetry.
- Browsers that can be used to access the secure connect gateway user interface.
- Hypervisors that can be used to deploy secure connect gateway.

System requirements

The system requirements to deploy and use secure connect gateway vary depending on:

- The number of devices to be monitored.
- The secure connect gateway functionality that you want to use—only collect telemetry or monitor devices and collect telemetry.

The following table provides the number of devices you can monitor using secure connect gateway based on the device type or model:

Table 4. Number of devices based on device type or model

Device type or model	Number of devices you can monitor using secure connect gateway
<ul style="list-style-type: none"> • Server or hypervisor • Chassis • Networking • iDRAC • Fluid File System (FluidFS) • PeerStorage (PS) or EqualLogic • Storage Center (SC) or Dell Compellent • PowerVault • Web-Scale • Software • Virtual Machines 	8000
<ul style="list-style-type: none"> • Data protection • Data storage devices other than Fluid File System (FluidFS), EqualLogic, Dell Compellent, and PowerVault. • Converged or hyperconverged infrastructure appliances other than Web-Scale. 	250

The following table provides the minimum system requirements to deploy and use secure connect gateway:

Table 5. Recommended minimum system requirements to deploy and use secure connect gateway

Number of devices	Monitor and collect telemetry	Number of processor cores	Installed memory (RAM)	Hard drive space
1-50	Yes	4	16 GB	140 GB
51-4250	Yes	8	16 GB	140 GB

Table 5. Recommended minimum system requirements to deploy and use secure connect gateway (continued)

Number of devices	Monitor and collect telemetry	Number of processor cores	Installed memory (RAM)	Hard drive space
4251–8250	Yes	8	16 GB	140 GB ¹

NOTE: While installing secure connect gateway using containers, the system must have a free disk space of 140 GB, of which a minimum of 10 GB must be allocated for the following directories depending on the container:

- Docker—/var/lib/docker directory.
- Podman — defined directory in <volumePath> from the podman info command.
- Kubernetes—defined directory in <PV.yaml file>.

¹—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 manually initiate single and multiple device collections. However, you can only select up to 100 devices for a multiple device collection. A multiple device collection performed for deployment, system maintenance, or consulting purposes may result in high system resource utilization at irregular intervals.

The following table provides the minimum system requirements to collect telemetry:

NOTE: Ensure that the hard drive space required to collect telemetry is available in the total hard drive space that is assigned for the appliance.

Table 6. Minimum system requirements to collect telemetry

Number of devices	Number of processor cores	Installed memory (RAM)	Hard drive space
1	4	16 GB	10 GB
2-30	4	16 GB	10 GB
31-50	4	16 GB	40 GB
51-100	8	16 GB	60 GB

Network requirements

This section lists the minimum network requirements, port requirements, and the IP address translation details for the local system.

NOTE: For information about device-specific ports, see the *Secure Connect Gateway 5.x — Virtual Edition Support Matrix* available on the [Secure Connect Gateway - Virtual Edition documentation](#) page.


- Network Address Translation (NAT) is supported only between secure connect gateway and Dell Technologies. NAT **is not supported** between secure connect gateway and the managed devices.
- Port Address Translation (PAT) is not supported for the IP addresses of any of the devices that are managed by secure connect gateway.
- Dynamic IP addresses (DHCP) should not be used for any components of the secure connect gateway servers, policy manager servers, or any managed devices.
- Internet connectivity—Standard 1 GbE network or faster through HTTP with basic authentication
- The local system must be able to connect to the following **Enterprise** servers through ports 443 and 8443:
 - For IPV6
 - srs-1-v6.dell.com
 - For IPV4
 - esrs3-core.emc.com
 - esrs3-coredr.emc.com
- The local system must be able to connect to the following **Global access** servers through ports 443 and 8443:
 - For IPV6
 - SRSgduprd01-v6.dell.com

- SRSgduprd02-v6.dell.com
- SRSgduprd03-v6.dell.com
- SRSgduprd04-v6.dell.com
- SRSgduprd05-v6.dell.com
- SRSgduprd06-v6.dell.com
- SRSghopr01-v6.dell.com
- SRSghopr02-v6.dell.com
- SRSghopr03-v6.dell.com
- SRSghopr04-v6.dell.com
- SRSghopr05-v6.dell.com
- SRSghopr06-v6.dell.com

o For IPV4

- esr3gduprd01.emc.com
- esr3gduprd02.emc.com
- esr3gduprd03.emc.com
- esr3gduprd04.emc.com
- esr3gduprd05.emc.com
- esr3gduprd06.emc.com
- esr3ghopr01.emc.com
- esr3ghopr02.emc.com
- esr3ghopr03.emc.com
- esr3ghopr04.emc.com
- esr3ghopr05.emc.com
- esr3ghopr06.emc.com
- esr3gscprd01.emc.com
- esr3gscprd02.emc.com
- esr3gscprd03.emc.com
- esr3gscprd04.emc.com
- esr3gscprd05.emc.com
- esr3gscprd06.emc.com
- esr3gckprd01.emc.com
- esr3gckprd02.emc.com
- esr3gckprd03.emc.com
- esr3gckprd04.emc.com
- esr3gckprd05.emc.com
- esr3gckprd06.emc.com
- esr3gckprd07.emc.com
- esr3gckprd08.emc.com
- esr3gckprd09.emc.com
- esr3gckprd10.emc.com
- esr3gckprd11.emc.com
- esr3gckprd12.emc.com
- esr3gspprd01.emc.com
- esr3gspprd02.emc.com
- esr3gspprd03.emc.com
- esr3gspprd04.emc.com
- esr3gspprd05.emc.com
- esr3gspprd06.emc.com

- Configure at least one DNS server.
- Use only a static IP address for the local system. Dynamic IP addresses are not supported.
- To ensure communication security and integrity, networking devices must not perform any method of SSL decryption on traffic for the backend. Attempting to do so causes a loss of connectivity to the backend.

 **NOTE:** If SSL decryption is enabled on the proxy servers and other devices, ensure the **Global access** and **Enterprise** servers are added to the SSL decryption exclusion list on the proxy servers and devices.

The following table lists the ports that must be open on the local system:

Table 7. Network ports for local system


Port	Protocol	Direction	Usage
25	TCP and SMTP	Inbound	Receive call-home email messages from data storage devices other than the following models: <ul style="list-style-type: none"> • Fluid File System (FluidFS) • PeerStorage (PS) or EqualLogic • Storage Center (SC) or Dell Compellent • PowerVault • PowerVault tape libraries
25	TCP and SMTP	Outbound	Send email messages through your SMTP server.
80	TCP and HTTP	Outbound	Communicate using HTTP.
161	UDP and SNMP	Outbound	Query device status through SNMP
162	UDP and SNMP	Inbound	Receive alerts (SNMP traps) from remote devices.
443	TCP and HTTPS	Inbound	<ul style="list-style-type: none"> • Communicate with OpenManage Enterprise. • Receive alert data from data storage devices other than the following models: <ul style="list-style-type: none"> ◦ Fluid File System (FluidFS) ◦ PeerStorage (PS) or EqualLogic ◦ Storage Center (SC) or Dell Compellent ◦ PowerVault ◦ PowerVault tape libraries • Receive heartbeat data and alert information from the following device types and models: <ul style="list-style-type: none"> ◦ Data protection ◦ Data storage devices other than the following models: <ul style="list-style-type: none"> ▪ Fluid File System (FluidFS) ▪ PeerStorage (PS) or EqualLogic ▪ Storage Center (SC) or Dell Compellent ▪ PowerVault ▪ PowerVault tape libraries ◦ Converged or hyperconverged infrastructure appliances other than Web-Scale.
990	FTPS	Outbound	Used for alert failover if 443 file transfer channel is unavailable.
443 and 8443	TCP and HTTPS	Outbound	<ul style="list-style-type: none"> • Connect to the Global access and Enterprise servers. • Communicate using HTTPS secured with TLSv1.2. • Communicate using Secure Socket Layer (SSL) and WS-MAN. • Receive secure connect gateway updates. • Upload collected telemetry to the backend
1311	TCP	Outbound	Communicate with Dell OpenManage Server Administrator.
5700	TCP and HTTPS	Inbound	Open secure connect gateway user interface using HTTPS with TLS v1.2.
5701, 5702, 5703, and 5704	TCP and HTTPS	Inbound	Collect telemetry from devices.
5705	TCP and HTTPS	Inbound	Receive Redfish alerts from remote devices through secure connect gateway alert services.*
9001	N/A	Internal	Establish connection with the Dell Technologies secure connect gateway DB service.  NOTE: This port is for internal use only. You must ensure that this port is open and is not used by other applications.
8443	TCP and HTTPS	Outbound	Communicate with policy manager using SSL encryption.

Table 7. Network ports for local system (continued)

Port	Protocol	Direction	Usage
8888	TCP	Outbound	Communicate with policy manager without SSL encryption.
9443	TCP and HTTPS	Inbound	Register and receive alert and heartbeat data from data storage devices other than the following models using REST APIs: <ul style="list-style-type: none">• Fluid File System (FluidFS)• PeerStorage (PS) or EqualLogic• Storage Center (SC) or Dell Compellent• PowerVault• PowerVault tape libraries

* For iDRAC9 running firmware version 5.x or later, the Redfish protocol must be enabled on the device. For instructions on how to enable Redfish notifications, see the *Integrated Dell Remote Access Controller User's Guide* available on the [iDRAC Manuals](#) page.

Supported browsers

You can access the secure connect gateway user interface using the following web browsers:

- Mozilla Firefox 122
- Google Chrome 121
- Microsoft Edge 121


Supported hypervisors

You can deploy secure connect gateway on the following hypervisors:

- VMware vSphere ESXi 8.0.x
- VMware vSphere ESXi 7.0.x
- Microsoft Hyper-V Server 2022
- Microsoft Hyper-V Server 2019
- Microsoft Hyper-V Server 2016

Supported servers

This section provides information about the supported Dell servers, and the protocols and ports that are required to discover servers and collect telemetry.

 **NOTE:** If you add non-Dell servers in secure connect gateway, only collection of host information is supported.

Collection protocols

The following protocol services are required to collect telemetry from the devices:

- On a server running Windows operating system—WMI
- On a server running Linux operating system—SSH
- On a server running VMware ESXi, ESX, Oracle Virtual Machine, Citrix XenServer, or Microsoft Hyper-V—SSH and VMware SDK

Ports used

The following ports must be open on the server to enable discovery and telemetry collections:

- On a server running Windows operating system—135
- On a server running Linux operating system—22
- On a server running VMware ESXi, ESX, Oracle Virtual Machine, Citrix XenServer, or Microsoft Hyper-V—22 and 443
- If the device connects to the Internet through a proxy server, ports 161, 22, and 1311 must be open on the proxy server firewall.
- 1311 to communicate with Dell OpenManage Server Administrator

16th generation PowerEdge servers

The following table lists the supported 16th generation PowerEdge servers:

Table 8. Supported 16th generation PowerEdge servers

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
HS5610	7.10.30.00	See Supported servers .	See Supported servers .	—
HS5620	7.10.30.00			—
MX760C	7.10.30.00			—
R360	7.10.30.00			—
R660	7.10.30.00			—
R660xs	7.10.30.00			—
R6615	7.10.30.00			—
R6625	7.10.30.00			—
R760	7.10.30.00			—
R760xa	7.10.30.00			—

Table 8. Supported 16th generation PowerEdge servers (continued)

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
R760xd2	7.10.30.00			—
R760xs	7.10.30.00			—
R7615	7.10.30.00			—
R7625	7.10.30.00			—
R860	7.10.30.00			—
R960	7.10.30.00			—
T360	7.10.30.00			—
T560	7.10.30.00			—

15th generation PowerEdge servers

Installation or deployment of secure connect gateway is supported on Red Hat Enterprise Linux 8.0 Z-stream and Red Hat Enterprise Linux 7.6 Z-stream operating systems. If Ubuntu 18.04.x operating system is installed on the server, only telemetry collections is supported.

The following table lists the supported 15th generation PowerEdge servers:

Table 9. Supported 15th generation PowerEdge servers

Model	Latest iDRAC firmware versions	Collection protocol	Ports used	Support notes
MX750c	7.10.30.00	See Supported servers .	See Supported servers .	—
R250				—
R350				—
R450				—
R550				—
R650				—
R650xs				—
R6515				—
R6525				—
R750				—
R750xa				—
R750xs				—
R7515				—
R7525				—
T150				—
T350				—
T550				—

14th generation PowerEdge servers

The following table lists the supported 14th generation PowerEdge servers:


 **NOTE:** Installation of secure connect gateway is supported on Red Hat Enterprise Linux 8.0 operating system.

Table 10. Supported 14th generation PowerEdge servers

Model	Latest iDRAC firmware version	Collection protocol	Ports used	Support notes
FC640	7.00.00.00	See Supported servers	See Supported servers .	—
M640				—
MX740C				—
MX840C				—
R240				—
R340				—
R440				—
R540				—
R640				—
R740				—
R740xd				—
R840				—
R940				—
R940XA				—
R6415				Support for these models has been assessed based on secure connect gateway compatibility with similar models.
R7415				
R7425				
T140				
T340				—
T440				—
T640				—

13th generation PowerEdge servers

The following table lists the supported 13th generation PowerEdge servers:

 **NOTE:** Installation of secure connect gateway is supported on Red Hat Enterprise Linux 8.0 operating system.

Table 11. Supported 13th generation PowerEdge servers

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
FC430	2.85.85.85	See Supported servers .	See Supported servers .
FC630	2.85.85.85		
FC830	2.85.85.85		
FM120	2.85.85.85		

Table 11. Supported 13th generation PowerEdge servers (continued)

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
M630	2.85.85.85		
M830	2.85.85.85		
R230	2.85.85.85		
R330	2.85.85.85		
R430	2.85.85.85		
R530	2.85.85.85		
R530xd	2.85.85.85		
R630	2.85.85.85		
R730	2.85.85.85		
R730xd	2.85.85.85		
R830	2.85.85.85		
R930	2.85.85.85		
T130	2.85.85.85		
T330	2.85.85.85		
T430	2.85.85.85		
T630	2.85.85.85		

12th generation PowerEdge servers

The following table lists the supported 12th generation PowerEdge servers:

Table 12. Supported 12th generation PowerEdge servers

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
M420	2.60.60.60	See Supported servers .	See Supported servers .
M520	2.60.60.60		
M620	2.60.60.60		
M820	2.60.60.60		
R220	2.60.60.60		
R320	2.60.60.60		
R420	2.60.60.60		
R520	2.60.60.60		
R620	2.60.60.60		
R720	2.60.60.60		
R720xd	2.60.60.60		
R820	2.60.60.60		
R920	2.60.60.60		
T320	2.60.60.60		

Table 12. Supported 12th generation PowerEdge servers (continued)

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
T420	2.60.60.60		
T620	2.60.60.60		

11th generation PowerEdge servers

The following table lists the supported 11th generation PowerEdge servers:

Table 13. Supported 11th generation PowerEdge servers

Model	Collection protocol	Ports used	Support notes
M610	See Supported servers .	See Supported servers .	Remote monitoring and case creation are supported only if OpenManage Server Administrator (OMSA) is installed and running on the server.
M610x			
M710			
M710HD			
M910			
M915			
R210			
R210II			
R310			
R410			
R415			
R510			
R515			
R610			
R710			
R715			
R810			
R815			
R910			
T110			
T110II			
T310			
T410			
T610			
T710			

10th generation PowerEdge servers

The following table lists the supported 10th generation PowerEdge servers:

Table 14. Supported 10th generation PowerEdge servers

Model	Collection protocol	Ports used	Support notes
M600	See Supported servers .	See Supported servers .	Remote monitoring and case creation are supported only if OpenManage Server Administrator (OMSA) is installed and running on the server.
M605			
M805			
M905			
R200			
R300			
R805			
R900			
R905			
T100			
T105			
T300			
T605			

9th generation PowerEdge servers

The following table lists the supported 9th generation PowerEdge servers:

Table 15. Supported 9th generation PowerEdge servers

Model	Collection protocol	Ports used	Support notes
R1900	See Supported servers .	See Supported servers .	Remote monitoring and case creation are supported only if OpenManage Server Administrator (OMSA) is installed and running on the server.
R1950			
R1955			
R2900			
R2950			
R2970			
R6950			

C series PowerEdge servers

The following table lists the supported C Series PowerEdge servers:

Table 16. Supported C Series PowerEdge servers

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
C1100	—	See Supported servers .	See Supported servers .	—
C2100	—			—
C4130	2.83.83.83			—
C4140II	5.00.00.00			Support for this model has been assessed


Table 16. Supported C Series PowerEdge servers (continued)

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
				based on secure connect gateway compatibility with other similar PowerEdge servers.
C6100	—			—
C6105	—			—
C6145	—			—
C6320	2.83.83.83			—
C6320p	2.83.83.83			—
C6420	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.
C6520	6.00.00.00			
C6525	6.00.00.00			
C6615	7.00.55.00			—
C6620	6.10.39.00			—

XE series PowerEdge servers

You must select the device type as **iDRAC** to monitor these devices in secure connect gateway. The following table lists the supported XE series PowerEdge servers:

Table 17. Supported XE series PowerEdge servers

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
XE2420	5.00.00.00	WSMan, REST, and Redfish  NOTE: Redfish is supported only if 4.x version of iDRAC firmware is installed.	443 and 161
XE7420	5.00.00.00		
XE7440	5.00.00.00		
XE8545	4.22.00.100		
XE8640	7.00.30.00		
XE9640	7.00.39.00		
XE9680	7.00.30.00		


XR series PowerEdge servers


You must select the device type as **iDRAC** to monitor these devices in secure connect gateway. The following table lists the supported XR series PowerEdge servers:

Table 18. Supported XR series PowerEdge servers

Model	Latest iDRAC firmware versions	Collection protocol	Ports used
XR11	6.10.00.00	REST and Redfish	443 and 161

Table 18. Supported XR series PowerEdge servers (continued)


Model	Latest iDRAC firmware versions	Collection protocol	Ports used
XR12	6.10.00.00	 NOTE: Redfish is supported only if 4.x version of iDRAC firmware is installed.	
XR4510c	6.10.85.00		
XR4520c	6.10.85.00		
XR5610	7.00.30.00		
XR7620	7.10.30.00		
XR8000r	7.10.30.00		
XR8610t	7.10.30.00		
XR8620t	7.10.30.00		

 **NOTE:** Data from XR4000w gets automatically collected with XR4510c and XR4520c collections.

Datacenter Scalable Solutions

You must select the device type as **iDRAC** to monitor these devices in secure connect gateway. The following table lists the supported Datacenter Scalable Solutions (DSS):


Table 19. Supported Datacenter Scalable Solutions

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
DSS 1500	2.83.83.83	WSMAN, REST, and Redfish  NOTE: Redfish is supported only if 4.x version of iDRAC firmware is installed.	443 and 161	—
DSS 1510	2.83.83.83			—
DSS 2500	2.83.83.83			—
DSS 8440	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.
DSS 9600	6.00.00.00			Support for these models and firmware version 6.00.00.00 has been assessed based on secure connect gateway compatibility with similar models and other firmware versions.
DSS 9620	6.00.00.00			
DSS 9630	6.00.00.00			

AX nodes

You must select the device type as **iDRAC** to monitor these devices in secure connect gateway. The following table lists the supported AX nodes:

Table 20. Supported AX nodes

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used
AX-640	7.00.00.00	WSMan, REST, and Redfish  NOTE: Redfish is supported only if 4.x version of iDRAC firmware is installed.	443 and 161
AX-650	7.00.30.00		
AX-6515	7.00.30.00		
AX-740XD	7.00.00.00		
AX-750	7.00.30.00		
AX-7525	7.00.30.00		

PowerVault devices

You must select the device type as **Server / Hypervisor** to add these devices in secure connect gateway. If a critical hardware issue is detected on these devices, a support case is created for the server on which it is attached. The following PowerVault devices are supported in secure connect gateway:

Table 21. Supported PowerVault devices

Model	Latest supported iDRAC firmware version	Collection protocol	Ports used	Support notes
MD1000	—	See Supported servers .	See Supported servers .	Secure connect gateway can also detect hardware issues with these devices if the server to which the storage device is attached is added in secure connect gateway
MD1120	—			
MD1200	—			
MD1220	—			
MD1400	—			
MD1420	—			
NX200	—			—
NX300	—			—
NX430	—			—
NX440	—			—
NX1950	—			—
NX3000	—			—
NX3230	—			—
NX3240	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.
NX3330	—			—
NX3340	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.

Supported Integrated Remote Access Controllers (iDRAC)

The following table lists the supported Dell Integrated Remote Access Controllers:



 **NOTE:** Secure connect gateway capabilities are not available for an iDRAC on an SC series or Dell Compellent device.

Table 22. Supported Dell Integrated Remote Access Controllers

Model	Collection protocol	Ports used	Support notes
iDRAC7	WSMan and REST	443 and 161	—
iDRAC8	WSMan and REST	443 and 161	—
iDRAC9	WSMan, REST, and Redfish  NOTE: Redfish supports collection only if 4.x version of iDRAC9 firmware is installed.	443 and 161	Monitoring is not supported for iDRAC9 with basic license.

Supported chassis

The following table lists the supported chassis:

Table 23. Supported chassis

Model	Supported firmware version	Collection protocol	Ports used	Support notes
PowerEdge M1000e	6.21	SSH2	22	-
PowerEdge VRTX	<ul style="list-style-type: none"> 3.40 3.30 	SSH2	22	Support for these firmware has been assessed based on secure connect gateway compatibility for this device with similar firmware.
PowerEdge FX2/FX2s	2.30	SSH2	22	-
PowerEdge MX7000	2.00.00	SSH2	22	-
	<ul style="list-style-type: none"> 1.30.00 1.20.10 1.20.00 1.10.00 	REST	443	Support for these firmware has been assessed based on secure connect gateway compatibility for this device with similar firmware.

Storage modules

The following table lists the supported storage modules:

Table 24. Supported storage modules

Model	Latest supported firmware version	Support notes
PowerEdge FD332	3.31	The telemetry that is collected from the storage module is included in the telemetry that is collected from the chassis.
PowerEdge MX5016s	2.20	<ul style="list-style-type: none"> Remote monitoring and case creation are not supported. The telemetry that is collected from the storage module is available in the telemetry that is collected from the chassis.

Supported data storage devices

This section provides information about the supported PS Series or EqualLogic, MD series, ME3 and ME4 series, SC series or Dell Compellent, Network Attached Storage, and other data storage devices. The following table displays how the data storage devices are grouped:

Table 25. Supported data storage devices

Enterprise storage	Entry level and midrange storage	Networking storage	Legacy storage	Storage software	Analytic software	Support software
Atmos	Network Attached Storage	Dell InterConnect Fabric	Centera	RecoverPoint	Streaming Data Platform	CloudIQ Collector
Cloud Array	PowerStore	Connectrix	—	Dell Storage Resource Manager (SRM)	—	Customer Management Station
Elastic Cloud Storage (ECS)	PowerVault MD3 and ME4	Switch Brocade	—	ViPR	—	DataIQ
Isilon or PowerScale	PowerVault tape libraries	Switch Cisco	—	ViPR Storage Resource Manager	—	Data Computing Appliance
PowerScale SD	PowerVault ME5	—	—	—	—	DellSvcs-Monitor
ObjectScale	PS Series or EqualLogic	—	—	—	—	DellSvcs-Auth
PowerMax	SC series or Dell Compellent	—	—	—	—	DellSvcs-Automate
S5000 series	Unity or Unity VSA	—	—	—	—	DellSvcs-Connector
PowerFlex	VNX	—	—	—	—	DellSvcs-CPMS
Symmetrix	VNXe	—	—	—	—	Disk Library (DL3D)
Unisphere	—	—	—	—	—	Disk Library Mainframe (series 3) and Disk Library Mainframe (series 4 + 5)
VMAX (VMAX, VMAX v3, and VMAX AFA)	—	—	—	—	—	Dell Disk Library (EDL)
MetroNode or VPLEX	—	—	—	—	—	—
XtremIO	—	—	—	—	—	—

Enterprise storage devices

The following table lists the enterprise storage devices:

Table 26. Enterprise storage devices

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
APEX Navigator for Multicloud Storage	HTTPS 443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS_ALT 8080	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote Support
Atmos	Passive FTP	Outbound	To secure connect gateway	ConnectEMC	Service notification
	SMTP		To secure connect gateway or to your SMTP server		
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote Support
	443		Secure Web UI		
Bare Metal Orchestrator (BMO)	HTTPS 443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
Cloud Array	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC or DialEMC	
	Passive FTP ¹				
	SMTP				
	41022	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	443			BMCUI CLOUDARRAYUI	
Dell Data Analytics Engine	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
Dell NativeEdge	HTTPS 443	Outbound	To secure connect gateway	From secure connect gateway	Service notification
	HTTPS	Inbound	From secure connect gateway	HTTPS	Remote support
Elastic Cloud Storage (ECS)	HTTPS ¹	Outbound	To secure connect gateway	ConnectEMC	Service notification
	Passive FTP ¹				
	SMTP				
	HTTPS 9443			REST	
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443, 4443			ECS UI	
Isilon or PowerScale	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	

Table 26. Enterprise storage devices (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
	Passive FTP	Inbound	From secure connect gateway		Configuration information
	SMTP				
	Managed File Transfer (MFT) 8118			ISI-Gather Log Process	
	22			CLI (using SSH)	Remote support
	8080			Secure Web UI	
PowerScale SD	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
ObjectScale	9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	443, 4443, 80			ObjectScale UI	
PowerMaxV4	9443	Outbound	To secure connect gateway	REST	Service notification
	22, 9519	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
S5000 series	9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote Support
PowerFlex	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	6611	Inbound	From secure connect gateway	ScaleIOClient	Remote support
	22			CLI (using SSH)	
	3389			Remote desktop	
	443			PFMPHTTPS	
SCALEIO	443	Inbound	From secure connect gateway	PFMPHTTPS	Remote support
Symmetrix	HTTPS ¹	Outbound	To secure connect gateway	ConnectEMC or DialEMC	Service notification
	Passive FTP ¹				
	SMTP				
	HTTPS 9443			MFT	
	9519	Inbound	From secure connect gateway	RemotelyAnywhere	Remote support
	5414			EMCRemote	
	4444, 5555, 7000, 23003, and 23004			SGBD/Swuch/ChatServer/RemoteBrowser/InlineCS	
Unisphere	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification

Table 26. Enterprise storage devices (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
VMAX (VMAX, VMAX v3, and VMAX AFA) <i>i</i> NOTE: If TLS v1.2 is not enabled on the device, see here .	HTTPS ¹	Outbound	To secure connect gateway	ConnectEMC	Service notification
	Passive FTP ¹				
	SMTP				
	HTTPS 9443			REST/MFT-VMAX	
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	5414			EMCRemote	
	4444, 5555, 7000			InlineCS	
	7000			RemoteBrowser	
	9519			RemotelyAnywhere	
	5555, 23004, 23003, 1300			SGDB	
	5555, 23004			SWUCH	
MetroNode or VPLEX	SMTP	Outbound	To secure connect gateway	ConnectEMC	Service notification
				CLI (using SSH)	
	443	Inbound	From secure connect gateway	Unisphere	Remote support
	22			CLI (using SSH)	
	5020			iDRACManager	
XtremIO	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	
	Passive FTP ¹				
	SMTP				
	22, 80, 443	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443, 42502			XtremIO UI	

1—The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

Entry level and midrange storage devices

The following table lists the network port requirements of the following entry-level and midrange storage devices—PowerStore, PowerVault ME5, Unity or Unity VSA, VNX, VNXe.

For the network port requirements of EqualLogic, PowerVault MD3 and ME4 series, Dell Compellent, and Network Attached Storage devices, see:

- [PS Series or EqualLogic devices](#)
- [PowerVault MD3 and ME4 devices](#)
- [SC series or Dell Compellent devices](#)
- [Network Attached Storage devices](#)

Table 27. Entry level and midrange storage devices

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
PowerStore	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	443			PowerStore Manager	
PowerVault ME5	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
Unity or Unity VSA	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443			Unisphere	
VNX	HTTPS ²	Outbound	To secure connect gateway	ConnectEMC	Service notification
	Passive FTP ¹				
	SMTP				
	HTTPS 9443			MFT	
	13456	Inbound	From secure connect gateway	KTCONS	Remote support
	13456,13457			RemoteKTrace	
	9519			Remotely-Anywhere	
	22, 2022			CLI (using SSH)	
	80, 443, 2162, 2163, 8000			Unisphere/USM/Navisphere SecureCLI	
	6391, 6392, 60020			Remote Diagnostic Agent	
VNXe	HTTPS ³	Outbound	To your SMTP server To secure connect gateway	ConnectEMC	Service notification
	Passive FTP				
	SMTP				
	HTTPS 9443			MFT	
	22, 2022	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443			Unisphere	

1—The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

2—HTTPS is supported only on devices running Block-Operating-Environment version 05.33.009.5.231 or later and file Operating Environment version 8.1.9.231 or later.

3—HTTPS is supported only on devices running Operating Environment version 3.1.10 or later.

PS Series or EqualLogic devices

The following table lists the supported PS Series or EqualLogic devices.

Table 28. Supported PS Series or EqualLogic devices

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
PS-M4110	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	—
PS4000	9.1.9	SNMPv2, SSH2, and FTP	161, 22, and 21	—
PS4100	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
PS4110	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	
PS4210	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	—
PS6000	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
PS6010	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	
PS6100	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	
PS6110	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	
PS6210	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	—
PS6500	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
PS6510	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	
PS6610	10.0.3	SNMPv2, SSH2, and FTP	161, 22, and 21	—

PowerVault MD3 and ME4 devices

The following table lists the supported MD3 Series devices:


 **NOTE:** Telemetry collections are also supported from PowerVault MD3060e that is attached to a server.

Table 29. Supported MD3 Series devices

Model	Latest supported firmware version	Collection protocol	Ports used
MD3000i	7.35.39.64	SYMboISDK	2463
MD3200i	7.84.56	SYMboISDK	2463
MD3220i	7.84.56	SYMboISDK	2463
MD3260	8.20.24.60	SYMboISDK	2463
MD3260i	8.20.24.60	SYMboISDK	2463
MD3400	8.25.9.61	SYMboISDK	2463
MD3420	8.25.9.61	SYMboISDK	2463

Table 29. Supported MD3 Series devices (continued)

Model	Latest supported firmware version	Collection protocol	Ports used
MD3460	8.25.13.60	SYMbolSDK	2463
MD3600	7.84.56	SYMbolSDK	2463
MD3600f	7.84.56	SYMbolSDK	2463
MD3600i	7.84.56	SYMbolSDK	2463
MD3620f	8.20.21.61	SYMbolSDK	2463
MD3620i	8.20.21.61	SYMbolSDK	2463
MD3660f	8.20.21.61	SYMbolSDK	2463
MD3660i	8.20.21.61	SYMbolSDK	2463
MD3800f	8.25.09.61	SYMbolSDK	2463
MD3800i	8.25.09.61	SYMbolSDK	2463
MD3820f	8.25.09.61	SYMbolSDK	2463
MD3820i	8.25.9.61	SYMbolSDK	2463
MD3860f	8.25.9.61	SYMbolSDK	2463
MD3860i	8.25.9.61	SYMbolSDK	2463

The following table lists the supported ME4 Series devices.

Table 30. Supported ME4 Series devices

Model	Latest Supported firmware versions	Collection protocol	Ports used	Support notes
ME4012	GT280R010-01	REST	443	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
ME4012 with ME412	GT280R008	REST	443	
ME4024	GT280R010-01	REST	443	-
ME4024 with ME424	GT280R008	REST	443	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
ME4084	GT280R010-01	REST	443	
ME484	GT280R008	REST	443	

SC series or Dell Compellent devices

Secure connect gateway only supports multiple-device collections for deployment purpose. Remote monitoring, case creation, and periodic collections are supported through the secure connect gateway solution that is available on the device when using Dell Storage Manager secure connect gateway feature.

NOTE: Remote monitoring and case creation are supported on SC200, SC220, SC280, SC100, SC120, SC180, SC400, SC420, SC360, SC460, and SC480 expansion enclosures by using Dell Storage Manager.

The following table lists the supported SC series or Dell Compellent devices:

Table 31. Supported SC series or Dell Compellent devices

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
SC4000	7.5	REST	443	—
SC4020	7.5	REST	443	—
SC5020	7.5	REST	443	—
SC7020	7.5	REST	443	—
SC8000	7.5	REST	443	—
SC9000	7.5	REST	443	—
SCv2000	7.5	REST	443	—
SCv2020	7.5	REST	443	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
SCv2080	7.5	REST	443	
SCv3000	7.5	REST	443	—
SCv3020	7.5	REST	443	—

Network Attached Storage devices

The following table lists the supported Network Attached Storage (NAS) devices:

Table 32. Supported NAS devices

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
FS8610i	6.0	SSH2, FTP, and SSH2	22 and 44421	—
FS8600	6.0	SSH2, FTP, and SSH2	22 and 44421	To enable secure connect gateway capabilities for the device, add the device manually in secure connect gateway.
FS7500	4.0	SSH2 and FTP	22 and 44421	
FS7600	4.0	SSH2 and FTP	22 and 44421	
FS7610	4.0	SSH2 and FTP	22 and 44421	
NX3500	3.0	SSH2 and FTP	22 and 44421	
NX3600	3.0	SSH2 and FTP	22 and 44421	
NX3610	3.0	SSH2 and FTP	22 and 44421	

PowerVault tape libraries

The following table lists the supported PowerVault tape libraries:


Table 33. Supported PowerVault tape libraries

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
Dell ML3	1.4.0.0	HTTPS	3031	Remote monitoring and service request creation capabilities are not available.

Networking storage devices

The following table lists the supported networking storage devices:

Table 34. Supported networking storage devices

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
Connectrix ⁶	HTTPS ¹	Outbound	To secure connect gateway	ConnectEMC or DialEMC	Service notification
	Passive FTP ¹				
	SMTP				
	HTTPS 9443			REST	
	5414	Inbound	From secure connect gateway	EMCRemote	Remote support
	3389			Remote desktop	
	22			CLI (using SSH)	
Dell InterConnect Fabric	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
Switch Brocade ⁵	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	SMTP ²				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	23 ³  NOTE: If this device is managed by Connectrix Manager, then use port 5414.			Telnet	
Switch Cisco	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	SMTP ²		To your SMTP server		
	22 ⁴	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	23 ³			Telnet	

1—the use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

2—requires separate Windows monitoring workstation running Fabric Manager Server 5.x or higher.

3—Telnet port should be enabled only if SSH (port 22) cannot be used.

4—SSH must be enabled and configured on the device.

5—the following Brocade switches can be configured to connect to secure connect gateway directly or you can add them from the secure connect gateway user interface. When you add the device from the secure connect gateway user interface, select the **Device Type** as **Data Storage** and the **Storage type** as **Switch Brocade**.

- Connectrix DS 6620B
- Connectrix DS 6630B

- Connectrix DS-7720B
- Connectrix DS-6610B
- Connectrix DS-6620B
- Connectrix DS-6630B
- Connectrix ED-DCX7-4B
- Connectrix ED-DCX7-8B
- Connectrix ED-DCX6-4B
- Connectrix ED-DCX6-8B
- Connectrix MP 7810B

i **NOTE:** For information about Brocade 6505, see [Brocade switches](#).

6-the following Cisco MDS switches must be added from the secure connect gateway user interface. When you add the device from the secure connect gateway user interface, select the **Device Type** as **Data Storage** and the **Storage type** as **Connectrix**.

- Connectrix MDS-9132T
- Connectrix MDS-9148S
- Connectrix MDS-9148T
- Connectrix MDS-9250i
- Connectrix MDS-9396S
- Connectrix MDS-9396T
- Connectrix MDS-9706
- Connectrix MDS-9706-V2
- Connectrix MDS-9710
- Connectrix MDS-9710-V2
- Connectrix MDS-9718
- Connectrix MDS-9718-V3

For information about the other supported Cisco MDS switches that must be added in secure connect gateway by selecting the **Device type** as **Networking**, see [Cisco MDS switches](#).

Legacy storage devices

The following table lists the legacy storage devices:

Table 35. Supported legacy storage devices

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
Centera	SMTP	Outbound	To your SMTP server	ConnectEMC	Service notification
	3218 and 3682	Inbound	From secure connect gateway	Dell Centera Viewer	Remote Support
	22			CLI (using SSH)	

Storage software

The following table lists the supported storage software:

Table 36. Supported storage software

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
RecoverPoint	REST	Outbound	To secure connect gateway	REST	Service notification

Table 36. Supported storage software (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443, and 7225			RecoverPoint Management UI	
Dell Storage Resource Manager (SRM)	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	Passive FTP ¹			ConnectEMC	
	SMTP				
	HTTPS ¹				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	3389			Remote desktop	
	58443, 58080			ViPRSRM UI	
ViPR	Passive FTP ¹	Outbound	To secure connect gateway	ConnectEMC	Service notification
	SMTP				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	443, 4443, 80	ViPR Management UI			
ViPR Storage Resource Manager	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	
	Passive FTP ¹				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	3389			Remote desktop	
	58443, 58080			ViPRSRM UI	

1—The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

Analytic software

The following table lists the supported analytic software:

Table 37. Supported analytic software

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
Streaming Data Platform	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	1080	Inbound	From secure connect gateway	SOCKS5	Remote support
	22			CLI (using SSH)	

Support software

The following table lists the supported support software:

Table 38. Supported support software

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
CloudIQ Collector	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
Customer Management Station	5414	Inbound	From secure connect gateway	EMCRemote	Remote support
	9519			RemotelyAnywhere	
	3389			Remote desktop	
	80, 443, 8443			WebHTTP/HTTPS	
	22			CLI (using SSH)	
DataIQ	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹				
	Passive FTP				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	80, 443, 30003			DataIQ UI	
Data Computing Appliance	Passive FTP	Outbound	To your SMTP server	ConnectEMC	Service notification
	SMTP				
	22	Inbound	From secure connect gateway	CLI (using SSH)	N/A
DellSvcs-Auth, DellSvcs-Automate, DellSvcs-Connector, DellSvcs-CPMS, and DellSvcs-Monitor.	22, 443	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
				SSLWebBrowser	
	3389			RDP	
	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹				
	Passive FTP ¹				
	SMTP				
Disk Library (DL3)	SMTP	Outbound	To your SMTP server	CentOS	Service notification
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	443			Secure Web UI	
	11576			EDL Mgt Console	
Disk Library Mainframe series 5	HTTPS 9443	Outbound	To secure connect gateway	ConnectEMC	Service notification
	FTP 20, 21				
	SSH/SFTP 22				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support

Table 38. Supported support software (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
	80, 443			DLmConsole / DLm System Manager	
Dell Disk Library (EDL)	HTTPS ^{2, 1}	Outbound	To secure connect gateway	ConnectEMC	Service notification
	Passive FTP ^{2, 1}				
	SMTP ²				
	22	Inbound	From secure connect gateway	CLI (using SSH)	Remote support
	11576			EDL Mgt Console	
	443			Secure Web UI	

1—The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

2—The service notification for EDL is supported only on the centrally managed devices through a management server. For the service notifications, the distributed EDL devices use secure connect gateway or the SMTP email server.

Supported networking switches

This section provides information about the supported PowerSwitch, PowerConnect, Dell Force10, Brocade, and Cisco switches.

PowerSwitch switches

The following table lists the supported PowerSwitch switches:

NOTE: In secure connect gateway, case creation is supported only on networking switches running operating system version 10.4.3.2 and later if the switches are added through secure connect gateway.

Table 39. Supported PowerSwitch switches

Model	Latest supported OS version	Collection protocol	Ports used	Supporting secure connect gateway versions for PowerSwitch models	Support notes
FN410T	9.10	SSH2	22	5.22, 5.20, 5.18	Secure connect gateway does not automatically create service requests.
FN410S	9.10	SSH2	22	5.22, 5.20, 5.18	
FN2210S	9.10	SSH2	22	5.22, 5.20, 5.18	
N1108EP-ON	6.4.3	SSH2	22	5.22, 5.20, 5.18	—
N1148P-ON	6.6	SSH2	22	5.22, 5.20, 5.18	—
N1524	6.5.1	SSH2	22	5.22, 5.20, 5.18	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
N1524P	6.5.1	SSH2	22	5.22, 5.20, 5.18	
N1548	6.5.1	SSH2	22	5.22, 5.20, 5.18	
N2024	6.5.2	SSH2	22	5.22, 5.20, 5.18	—
N2128PX-ON	6.6	SSH2	22	5.22, 5.20, 5.18	—
N3024, N3024P, N3048, and N3048P	6.3	SSH2	22	5.22, 5.20, 5.18	—
N3024EF-ON	6.6	SSH2	22	5.22, 5.20, 5.18	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
N3024EP-ON	6.6	SSH2	22	5.22, 5.20, 5.18	
N3024ET-ON	6.5.2	SSH2	22	5.22, 5.20, 5.18	
N3024F	6.3.9	SSH2	22	5.22, 5.20, 5.18	—
N3048EP-ON	6.6	SSH2	22	5.22, 5.20, 5.18	Support for these models has been assessed based on secure connect gateway
N3048ET-ON	6.5.1	SSH2	22	5.22, 5.20, 5.18	

Table 39. Supported PowerSwitch switches (continued)

Model	Latest supported OS version	Collection protocol	Ports used	Supporting secure connect gateway versions for PowerSwitch models	Support notes
					compatibility with similar models.
N3248TE	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
N4032F-ON	6.5.2	SSH2	22	5.22, 5.20, 5.18	Support for this model has been assessed based on secure connect gateway compatibility with similar models.
S3048-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4048-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4048T-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4112F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4112T-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4128F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4128T-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4148F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4148FE-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4148T-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4148U-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S4248FB-ON	10.5.5.3	SSH2	22	5.22, 5.20, 5.18	—
S4248FBL-ON	10.5.5.3	SSH2	22	5.22, 5.20, 5.18	—
S5148F-ON	10.5.5	SSH2	22	5.22, 5.20, 5.18	—
S5212F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S5224F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S5232F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S5248F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S5296F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
S5448F-ON	10.5.6.0	SSH2	22	5.22, 5.20	—
S6010-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
Z9100-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
Z9264F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
Z9332F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—
Z9432F-ON	10.5.6.0	SSH2	22	5.22, 5.20	—
Z9664F-ON	10.5.6.0	SSH2	22	5.22, 5.20, 5.18	—

NOTE: The supporting secure connect gateway versions refers only to the PowerSwitch models and not the operating system.

PowerSwitch switches with Enterprise SONiC operating system

The following table lists the supported PowerSwitch switches with Enterprise SONiC operating system:

Table 40. Supported PowerSwitch switches with Enterprise SONiC operating system

Model	Latest supported Enterprise SONiC OS version	Collection protocol	Ports used	Supporting secure connect gateway versions for PowerSwitch models
S5212F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
S5224F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
S5232F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
S5248F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
S5296F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
S5448F-ON	4.2.0	gNMI	22	5.22, 5.20
Z9264F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
Z9332F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18
Z9432F-ON	4.2.0	gNMI	22	5.22, 5.20
Z9664F-ON	4.2.0	gNMI	22	5.22, 5.20, 5.18

NOTE: The supporting secure connect gateway versions refers only to the PowerSwitch models and not the operating system.

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.

PowerConnect switches

The following table lists the supported PowerConnect switches:

Table 41. Supported PowerConnect switches

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
2808, 2816, 2824, and 2842	1.x	SNMPv2	161	—
3524, 3524P, 3548P and 3548	2.x	SSH2	22	—
5424 and 5448	2.x	SSH2	22	—
6224 and 6248	3.3	SSH2	22	—
6224F, 6224P, and 6248P	3.3.14.2	SSH2	22 and 161	—
7024, 7048, 7024F, 7024P, 7048P, and 7048R	5.1	SSH2	22	—
8024 and 8024F	5.1	SSH2	22	—

Table 41. Supported PowerConnect switches (continued)

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
8132 and 8164F	5.1	SSH2	22	—
B8000	7.0.1	SSH2	22	—
B8000E	7.2.1	SSH2	22 and 161	—
M6220	5.1	SSH2	22	—
M6348	5.1	SSH2	22 and 161	—
M8024	5.1	SSH2	22	—
M8024-K	5.1	SSH2	22	—
M8428-K	6.3.1	SSH2	22	—
N1100	6.4.2	SSH2	22	Support for this model has been assessed based on secure connect gateway compatibility with similar models.
N1108EP-ON	6.4.3	SSH2	22	—
N1148P-ON	6.6	SSH2	22	—
N1500	6.5	SSH2	22	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
N1524	6.5.1	SSH2	22	
N1524P	6.5.1	SSH2	22	
N1548	6.5.1	SSH2	22	
N2000	6.3.2.3	SSH2	22	—
N2024	6.5.2	SSH2	22	—
N2100	6.3	SSH2	22	—
N2128PX-ON	6.6	SSH2	22	—
N3000	6.2	SSH2	22	—
N3024, N3024P, N3048, and N3048P	6.3	SSH2	22	—
N3024EF-ON	6.6	SSH2	22	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
N3024EP-ON	6.6	SSH2	22	
N3024ET-ON	6.5.2	SSH2	22	
N3024F	6.3.9	SSH2	22	—
N3048EP-ON	6.6	SSH2	22	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
N3048ET-ON	6.5.1	SSH2	22	
N3100	6.3	SSH2	22	—
N4032F-ON	6.5.2	SSH2	22	Support for this model has been assessed based on secure

Table 41. Supported PowerConnect switches (continued)

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
				connect gateway compatibility with similar models.
W-3200	6.3	SSH2 and SNMPv2	22 and 161	—
W-3400	6.3	SSH2 and SNMPv2	22 and 161	—
W-3600	6.3	SSH2 and SNMPv2	22 and 161	—
W-6000	6.3	SSH2 and SNMPv2	22 and 161	—
W-620	6.3	SSH2 and SNMPv2	22 and 161	—
W-650	6.3	SSH2 and SNMPv2	22 and 161	—
W-651	6.3	SSH2 and SNMPv2	22 and 161	—
W-7210, W-7220, and W-7240	6.3	SSH2 and SNMPv2	22 and 161	—
X1008 and X1018P	3.0.0.94	SNMPv2	161	—
X1026P and X4012	3.0.0.94	SNMPv2	161	—

Dell Force10 switches

The following table lists the supported Dell Force10 switches:

Table 42. Supported Dell Force10 switches

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
C7004/C150 and C7008/C300	8.4.7	SSH2	22	—
C9010 (with C1048p)	9.14	SSH2	22	Support for this model has been assessed based on secure connect gateway compatibility with similar models.
C9010 (with N3PeX)	9.14	SSH2	22	—
MX5108n	10.5.0.5	SSH2	22	—
MX9116n	10.5.0.5	SSH2	22	—
MXG610s	8.1.0_Inx2	SSH2	22	Remote monitoring and automatic case creation is not supported.
MXL 10/40 GbE	9.3	SSH2	22	—
S3124-ON	9.14	SSH2	22	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
S3124F-ON	9.14	SSH2	22	
S3124P-ON	9.14	SSH2	22	—

Table 42. Supported Dell Force10 switches (continued)

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
S3148-ON	9.14	SSH2	22	Support for these models has been assessed based on secure connect gateway compatibility with similar models.
S3148P-ON	9.14	SSH2	22	
S4810 and S4820T	9.14	SSH2	22	—
Z9000	9.7	SSH2	22	—
Z9500	9.9	SSH2	22	—

Brocade switches

The following table lists the supported Brocade switches that you can add only from the secure connect gateway user interface as a networking device.

Table 43. Supported Brocade switches

Model	Latest supported OS version	Collection protocol	Ports used
6505	9.2.0	SNMPv2 and SSH2	22
6510	9.2.0	SNMPv2 and SSH2	22
6520	9.2.0	SNMPv2 and SSH2	22

The following Brocade switches can be configured to connect to secure connect gateway directly or you can add them from the secure connect gateway user interface. When you add the device from the secure connect gateway user interface, select the **Device Type** as **Data Storage** and the **Storage type** as **Switch Brocade**.

- Connectrix DS 6620B
- Connectrix DS 6630B
- Connectrix DS-7720B
- Connectrix DS-6610B
- Connectrix DS-6620B
- Connectrix DS-6630B
- Connectrix ED-DCX7-4B
- Connectrix ED-DCX7-8B
- Connectrix ED-DCX6-4B
- Connectrix ED-DCX6-8B
- Connectrix ED-DCX8510-4B
- Connectrix ED-DCX8510-8B
- Connectrix MP 7810B
- Connectrix MP-7840

For information about the TCP ports and protocols that are required to perform remote sessions or collect telemetry, see [Networking storage devices](#).

Cisco Catalyst switches

The following table lists the supported Cisco Catalyst switches:

Table 44. Supported Cisco Catalyst switches

Model	Latest supported OS version	Collection protocol	Ports used
2960	15.0	SNMPv2 and SSH2	22
3750G	12.2(55)SE3	SNMPv2 and SSH2	22
3750E	12.2(46)SE	SNMPv2 and SSH2	22
3750X	15.2(4)E6	SNMPv2 and SSH2	22
4948	15.0	SNMPv2 and SSH2	22

Cisco Nexus switches

The following table lists the supported Cisco Nexus switches:

Table 45. Supported Cisco Nexus switches

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
5010	5.2(1)N1(9a)	SNMPv2 and SSH2	22	To enable secure connect gateway capabilities, add the device manually in secure connect gateway.
5020	5.2(1)N1(9a)	SNMPv2 and SSH2	22	
5548	7.3(3)N1(1)	SNMPv2 and SSH2	22	

Cisco MDS switches

The following table lists the supported Cisco MDS switches that you must add in secure connect gateway by selecting the **Device type** as **Networking**.

Table 46. Supported Cisco MDS switches

Model	Latest supported OS version	Collection protocol	Ports used	Support notes
9124	3.2(2c)	SNMPv2 and SSH2	22	To enable secure connect gateway capabilities, add the device manually in secure connect gateway.

The following Cisco MDS switches can be configured to connect to secure connect gateway directly or you can add them from the secure connect gateway user interface. When you add the device from the secure connect gateway user interface, select the **Device Type** as **Data Storage** and the **Storage type** as **Connectrix**.

- Connectrix MDS-9132T
- Connectrix MDS-9148S
- Connectrix MDS-9148T
- Connectrix MDS-9250i
- Connectrix MDS-9396S
- Connectrix MDS-9396T
- Connectrix MDS-9706
- Connectrix MDS-9706-V2
- Connectrix MDS-9710
- Connectrix MDS-9710-V2
- Connectrix MDS-9718

- Connectrix MDS-9718-V3


For information about the TCP ports and protocols that are required to perform remote sessions or collect telemetry, see [Networking storage devices](#).

Supported hypervisors

The following table lists the supported hypervisors:

Table 47. Supported hypervisors

Model	Collection protocol	Ports used	Support notes
ESXi 6.5	SSH and VMware SDK	22 and 443	Remote monitoring and automatic case creation are supported only if OMSA is installed and the SNMP settings are configured on the hypervisor. Secure connect gateway does not support the automatic installation of OMSA and configuration of SNMP settings on the hypervisor. For more information about OMSA support, see the product documentation.
ESXi 6.5 U1	SSH and VMware SDK	22 and 443	
ESXi 6.5 U3	SSH and VMware SDK	22 and 443	
ESXi 6.7	SSH and VMware SDK	22 and 443	
ESXi 6.7 U3	SSH and VMware SDK	22 and 443	
ESXi 7.0	SSH and VMware SDK	22 and 443	
ESXi 7.0 U1	SSH and VMware SDK	22 and 443	
ESXi 8.0	SSH and VMware SDK	22 and 443	
ESXi 8.0 U2	SSH and VMware SDK	22 and 443	
ESXi 8.0 U3	SSH and VMware SDK	22 and 443	

 **NOTE:** ESXi 6.7 U2 is supported only on R540, R640, R740, and R740xd servers.

Supported virtual machines

The following table lists the supported virtual machines:

Table 48. Supported virtual machines

Operating system	Collection protocol	Ports used
Linux	SSH	22

Supported data protection devices

The following table lists the supported data protection devices:

Table 49. Supported data protection devices

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
AppSync	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹				
Avamar	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	
	Passive FTP				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	443			AVInstaller	
	80, 443, 8778, 8779, 8780, 8781, 8580, 8543, 9443, 7778, 7779, 7780, and 7781			Enterprise Manager	
	7778, 7779, 7780, 7781, and 9443			MCGUI	
CloudBoost Virtual Appliance	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC or DialEMC	
	Passive FTP ¹				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
Data Domain	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	443, 25, 21			ConnectEMC	
	80, 443	Inbound	From secure connect gateway	Enterprise Manager	Remote support
	22			CLI (via SSH)	
	23 ²			Telnet	
Data Protection Advisor	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	
	Passive FTP ¹				
	SMTP				

Table 49. Supported data protection devices (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	9002, 9003, and 9004			DPA GUI	
	3389			Remote desktop	
Data Protection Appliance	HTTPS ¹	Outbound	To secure connect gateway	ConnectEMC	Service notification
	Passive FTP ¹				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	8543			DPAppliance ACM	
	443			Data Protection Search UI, vSphere Web Client, IDRAC Web	
Enterprise Copy Data Management	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS ¹			ConnectEMC	
	Passive FTP				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	9000			Skyline UI	
	14443			SkylineUpgradeUI	
	8443			SkylineRESTAPIUI	
Networker	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	7938	Inbound	From secure connect gateway		N/A
PowerPath	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
PowerPath Management Appliance	9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLIViaSSH	Remote Support
PowerProtect Appliance	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
PowerProtect Data Manager	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
UCC	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support

1—The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set

to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

2—Telnet port should be enabled only if SSH (port 22) cannot be used.

Supported direct liquid cooling devices

The following table lists the supported direct liquid cooling devices:


 **NOTE:** Direct liquid cooling only supports discovery and collection of data.

Table 50. Supported direct liquid cooling devices

Model	Collection protocol	Ports used
CHx80	SNMP	161

Supported converged and hyperconverged infrastructure appliances

The following table lists the supported converged and hyperconverged infrastructure appliances:

Table 51. Supported converged and hyperconverged infrastructure appliances

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
APEX Cloud Platform	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
Converged Management Software	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	443			Secure Web UI	
PowerFlex Appliance	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	3389 and 3390			Remote desktop	
	8080			Web UI	
PowerFlex	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	443			PFMPHTTPS	
PowerFlex Rack	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
	3389			Remote desktop	
	8080			Secure Web UI	
	443			PFMPHTTPS	
VxRail	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	HTTPS			ConnectEMC	
	Passive FTP				
	SMTP				
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support
VxRack SDDC	HTTPS 9443	Outbound	To secure connect gateway	REST	Service notification
	22	Inbound	From secure connect gateway	CLI (via SSH)	Remote support

Table 51. Supported converged and hyperconverged infrastructure appliances (continued)

Model	TCP port or collection protocol	Direction	Source or Destination	Application name	Communication
Web-Scale	9440 and 22	—	—	—	—
	REST and SSH				

NOTE: The use of HTTPS for service notifications depends on the version of ConnectEMC used by the managed device. For more information, see the product documentation. The default port for HTTPS is 443. The value for Passive Port Range in FTP is set to 21 and 5400 through 5413. This range indicates the data channel ports available for the response to the PASV commands. These ports are used for the Passive FTP mode of the Connect Home messages and for the GWExt loading and output.

XC series Web-Scale converged appliances

You must select the device type as **iDRAC** to monitor these devices in secure connect gateway. Support for XC core systems of the following XC series appliances is inferred based on secure connect gateway compatibility with the XC series appliances. The following table lists the supported XC series Web-Scale converged appliances:

Table 52. Supported XC series Web-Scale converged appliances

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
XC430	5.0	REST and SSH2	9440 and 22	—
XC450	6.10.30.20			—
XC630	5.0			—
XC6320	5.0			—
XC640	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.
XC6420	6.00.00.00			Support for this model and firmware version has been assessed based on secure connect gateway compatibility with similar appliance models and firmware versions.
XC650	5.00.10.20			Support for firmware version 5.00.10.20 has been assessed based on secure connect gateway compatibility with 5.00.10.00.
XC720xd	5.0			—
XC730	5.0			—
XC730xd	5.0			—
XC740	5.0			—
XC740xd	6.00.00.00			Support for firmware version 6.00.00.00 is

Table 52. Supported XC series Web-Scale converged appliances (continued)

Model	Latest supported firmware version	Collection protocol	Ports used	Support notes
				based on secure connect gateway compatibility with other firmware versions.
XC750	6.10.30.20			—
XC750xa	5.00.10.00			—
XC940	5.0			—
XC740xd2	6.00.00.00			Support for firmware version 6.00.00.00 is based on secure connect gateway compatibility with other firmware versions.
XCXR2	6.00.00.00			Support for this model and firmware version 6.00.00.00 has been assessed based on secure connect gateway compatibility with similar appliance models and firmware versions.
XC6520	5.00.10.20			Support for firmware version 5.00.10.20 has been assessed based on secure connect gateway compatibility with 5.00.10.00.
XC7525	5.00.10.20			

Supported systems management consoles

The following table lists the supported systems management consoles:

Table 53. Supported systems management consoles

Systems management console	Adapter version	Console versions
OpenManage Enterprise	5.00.00.00	<ul style="list-style-type: none">• 4.0• 3.10• 3.9• 3.8.3• 3.8.2• 3.8• 3.7• 3.6.1• 3.6• 3.5• 3.4.1• 3.4• 3.3.1• 3.2.1• 3.2• 3.1• 3.0

Supported management and monitoring software

The following table lists the supported management and monitoring software:

Table 54. Supported management and monitoring software

Model	Collection protocol	Ports used
VMware HIT KIT v3.1	SSH	22
VMware VSM v5.0	SSH	22
VMware vCenter v6.5	HTTPS	443

Supported server operating systems and recommended OMSA version

To monitor a server that you have added in secure connect gateway, the Dell OpenManage Server Administrator (OMSA) agent must be installed and running on the server. The recommended version of OMSA may vary depending on the generation of the server and the operating system running on the server. To download the applicable OMSA version, go to [Enterprise Systems Management](#), and click **OpenManage Server Administrator**.

NOTE: Secure connect gateway depends on the OMSA agent to monitor a server only if you have added the server by selecting the device type as **Server / Hypervisor**. PowerEdge servers running iDRAC7 and later can be monitored without OMSA.

Linux and ESXi operating systems

The following table lists the Linux and ESXi operating systems that are supported on managed devices and the recommended OMSA version:

Table 55. Linux and ESXi operating systems and recommended OMSA version

Operating system	Generation of PowerEdge server						
	16th	15th	14th	13th	12th	11th	10th
ESXi 8.0 U1	11.0.1	11.0.1	11.0.1	—	—	—	—
ESXi 7.0 U1	11.0.1	11.0.1	11.0.1	9.5	9.5	—	—
ESXi 6.7 U1	—	—	9.3	9.3	—	—	—
ESXi 6.5 U1	—	—	—	—	—	9.1	9.1
ESXi 6.5 U3	—	9.4	9.4	9.4	9.4	—	—
Red Hat Enterprise Linux 9.2	11.0.1	11.0.1	11.0.1	—	—	—	—
Red Hat Enterprise Linux 9.0	—	10.3	10.3	—	—	—	—
Red Hat Enterprise Linux 8.8	11.0.1	11.0.1	11.0.1	—	—	—	—
Red Hat Enterprise Linux 8.6	—	10.3	10.3	—	—	—	—
Red Hat Enterprise Linux 8.5	—	10.2	10.2	—	—	—	—
Red Hat Enterprise Linux 8.4	—	—	9.5	9.5	9.5	—	—

Table 55. Linux and ESXi operating systems and recommended OMSA version (continued)

Operating system	Generation of PowerEdge server						
	16th	15th	14th	13th	12th	11th	10th
Red Hat Enterprise Linux 8.3	—	10.0.1	9.5	9.5	—	—	—
Red Hat Enterprise Linux 8.2	—	10.0.1	9.5	9.5	9.5	—	—
Red Hat Enterprise Linux 8.1	—	9.4	9.4	9.4	—	—	—
Red Hat Enterprise Linux 8.0 (64-bit) Z-stream	—	9.3.1	—	—	—	—	—
Red Hat Enterprise Linux 8.0 (64-bit)	—	—	9.3.1	9.3.1	—	—	—
Red Hat Enterprise Linux 7.9	—	10.0.1	9.5	9.5	—	—	—
Red Hat Enterprise Linux 7.8	—	10.0.1	9.5	9.5	9.5	—	—
Red Hat Enterprise Linux 7.7	—	9.4	9.4	9.4	9.4	—	—
Red Hat Enterprise Linux 7.6 (64-bit) Z-stream	—	9.3.1	—	—	—	—	—
Red Hat Enterprise Linux 7.5 (64-bit)	—	—	9.3	9.3	—	—	—
Red Hat Enterprise Linux 7.4 (64-bit)	—	—	9.1	9.1	—	—	—
Red Hat Enterprise Linux 7.2 (64-bit)	—	—	—	—	8.5	8.5	8.5
SUSE Linux Enterprise Server 15 SP5	11.0.1	11.0.1	11.0.1	—	—	—	—
SUSE Linux Enterprise Server 15 SP3	—	10.2.0.0	10.2.0.0	10.2.0.0	10.2.0.0	—	—

Table 55. Linux and ESXi operating systems and recommended OMSA version (continued)

Operating system	Generation of PowerEdge server						
	16th	15th	14th	13th	12th	11th	10th
SUSE Linux Enterprise Server 15 SP2	—	10.0.1	9.5	9.5	9.5	—	—
SUSE Linux Enterprise Server 15 (64-bit)	—	—	9.3	9.3	—	—	—
SUSE Linux Enterprise Server 12 SP3 (64 bit)	—	—	9.1	9.1	—	—	—
Ubuntu 22.04	11.0.1	11.0.1	11.0.1	—	—	—	—
Ubuntu 20.04	—	9.5	9.5	9.5	9.5	—	—
Ubuntu 20.04.4	—	10.3	10.3	—	—	—	—
Ubuntu 18.04.x	—	—	9.3	9.3	—	—	—

Support for OEM devices

Dell OEM-ready devices (either rebranded or debranded Dell hardware), when added, are classified under the rebranded name and not the original Dell hardware name. All the functionality available for Dell standard devices, such as alerts handling and automatic case creation (when the support level has been validated at the time of the support incident as ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service) are available for OEM-ready devices. For some OEM devices, the model name may be blank in the secure connect gateway user interface.

Automatic case creation is supported through Dell Technologies technical support and not available through other case management systems.

As with any system that is modified for custom solutions, validate all the secure connect gateway features to ensure proper operation with those modifications.


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 56. 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

 **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.

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.