SupportAssist Enterprise Version 4.0

User's Guide

November 2021
Rev. A10

Notes, cautions, and warnings

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

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

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

Contents

1

Overview

SupportAssist Enterprise is an application that automates technical support for your Dell EMC server, storage, and networking devices. SupportAssist monitors your devices and proactively detects hardware issues that may occur. Depending on your service contract, SupportAssist also automates support request creation for issues that are detected on the monitored devices.

ⓘ **NOTE:** In this document, the term local system refers to the server where SupportAssist Enterprise is deployed; remote device refers to any other device in your environment.

When a hardware issue is detected, SupportAssist automatically collects the system state information required for troubleshooting the issue or the collection is automatically sent to the backend by the device itself. The collected system information helps technical support to provide you an enhanced, personalized, and efficient support experience. SupportAssist capability also includes a proactive response from technical support to help you resolve the issue.

Additionally, SupportAssist can monitor hardware issues that may occur on devices that you are managing by using OpenManage Enterprise.

Topics:

How SupportAssist Enterprise works

When SupportAssist Enterprise is set up and the devices are configured correctly, SupportAssist receives an alert whenever a hardware event occurs on a device. The alert is filtered using various policies to determine if the alert qualifies for creating a support case or for updating an existing support case. All qualifying alerts are sent securely to the backend, for creating a support case or for updating an existing support case. After the support case is created or updated, SupportAssist collects system information from the device and sends it to the backend. Also, some of the devices send the information directly to the backend when an alert is generated. Dell EMC technical support uses the system information to troubleshoot the issue and provide an appropriate solution.

ⓘ **NOTE:** To experience the automatic case creation and system information collection capabilities of SupportAssist, you must complete the registration.

ⓘ **NOTE:** SupportAssist does not create a support case for every alert received from a monitored device. A support case is created only for a device that has an active service contract, and if the alert type and number of alerts received from the device match the predefined criteria for support case creation.

ⓘ **NOTE:** SupportAssist sends you automatic email notifications about support cases, device status, network connectivity status, and so on. For information about the various email notifications, see Types of email notifications on page 97.

System information collected by SupportAssist Enterprise

SupportAssist Enterprise continually monitors the configuration information and usage information of the managed hardware and software devices. While Dell EMC does not anticipate accessing or collecting personal information, such as your personal files, web-browsing history, or cookies in connection with this program, any personal system information inadvertently collected or viewed will be treated in accordance with the Dell Privacy Policy available for review at Dell.com/privacy.

The information encrypted in the collected system information log contains the following categories of data:

- **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

You can also access and view the system information collected by SupportAssist. For information about viewing the collected system information, see View collection from the Devices page on page 75.

By default, SupportAssist collects system information from all devices, irrespective of the service contract of the devices, and sends the system information securely to the backend. System information is collected from one device at a time based on the predefined collection start day and time specified in the **Preferences** page.

NOTE: If the security policy of your company restricts sending some of the collected system information outside of your company network, you can configure SupportAssist to exclude the collection of certain system information from your devices. For information about excluding the collection of certain system information, see Enable or disable collection of identity information on page 81 and Enable or disable collection of system information on page 82.

SupportAssist Enterprise capabilities available with Dell EMC service contracts

The following table provides a comparison of the SupportAssist Enterprise capabilities available with the ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contracts.

NOTE: Completing the registration is a prerequisite to receive the full benefits of SupportAssist Enterprise for your Dell EMC devices. For information about registering SupportAssist Enterprise, see Register SupportAssist Enterprise on page 22.

Table 1. SupportAssist Enterprise capabilities and Dell service contracts

SupportAssist Enterprise capability	Description	Basic Hardware	ProSupport	ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center
Proactive detection of hardware failures	SupportAssist Enterprise receives alerts for hardware events that occur in monitored devices and proactively determines if the alerts indicate a hardware failure.	✓	✓	✓
Predictive detection of hardware failures*	Intelligent analysis of system information collected from a monitored device is used to predict hardware failures that may occur in future.	✗	✗	✓
Automated collection of system information	The system information required for troubleshooting an issue is automatically collected from the monitored device and sent securely to the Dell EMC backend.	✓	✓	✓
Automated support case creation	When a hardware failure is detected either proactively or predictively, a support case is automatically created with Technical Support.	✗	✓	✓
Automated email notification	An email notification about the support case or issue is automatically sent to your company's primary and secondary contacts.	✗	✓	✓
Proactive response from Technical Support	A Technical Support agent contacts you proactively about the support case and helps you resolve the issue.	✗	✓	✓
Proactive parts dispatch	After analyzing the collected system information, if the Technical Support agent	✗	✓	✓

Table 1. SupportAssist Enterprise capabilities and Dell service contracts (continued)

SupportAssist Enterprise capability	Description	Basic Hardware	ProSupport	ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center
	determines that a part must be replaced to resolve the issue, a replacement part is dispatched to you based on the dispatch preferences provided in SupportAssist Enterprise.			

ⓘ **NOTE:** SupportAssist Enterprise also detects hardware issues in devices with a Dell EMC Basic Hardware service contract. However, a support case is not created automatically for devices with a Basic Hardware service contract.

* Predictive detection of hardware failures is applicable only for the batteries, hard drives, backplanes, and expanders of 12th and later generation of PowerEdge servers that have PowerEdge RAID Controller (PERC) Series 5 to 10. Predictive detection of hardware failures is available only when the automated periodic collection and upload of system information is enabled in SupportAssist Enterprise.

Downloading SupportAssist Enterprise

SupportAssist Enterprise is available in OVF and VHD formats. Depending on your hypervisor, you can download and deploy the required format. To download SupportAssist Enterprise, you must have a business enterprise account. The business enterprise account also enables you to access other related software download and support pages available for SupportAssist Enterprise.

If you do not have a business enterprise account, you can create an account while downloading SupportAssist Enterprise. You can also upgrade an existing account to a business enterprise account.

ⓘ **NOTE:** Dell EMC recommends that you use the *SupportAssist Enterprise Version 4.0 Pre-site Checklist* to understand the best sequence to download and deploy SupportAssist Enterprise Version 4.0.

Topics:

Download SupportAssist Enterprise

Prerequisites

You must have a business enterprise account. If you do not have a business enterprise account, see Create business enterprise account and download SupportAssist Enterprise on page 12. To upgrade your existing account to a business enterprise account and download SupportAssist Enterprise, see Upgrade to business enterprise account and download SupportAssist Enterprise on page 12.

Steps

1. Go to https://www.dell.com/SAE-v4.
2. Click **Log in**.
   The **Sign In** page is displayed.
3. Enter the email address and password, and click **Sign In**.
   The **Dell EMC SupportAssist Enterprise Version 4.0 - Virtual Edition** page is displayed with links to download SupportAssist Enterprise and generate an access key.
4. Click **Generate key**.
   The **Generate key** page is displayed with site details of your devices.
5. Select the required site.
6. Enter a four-digit PIN, and click **Generate key**.
   An access key is generated and sent to your email address.
7. Click **Done**.

   ⓘ **NOTE:** The access key and PIN are valid for seven days. Use the access key and PIN to complete SupportAssist Enterprise registration.
8. Click **Download File**.

Results

The SupportAssist Enterprise package is downloaded.

Create business enterprise account and download SupportAssist Enterprise

Steps

1. Go to https://www.dell.com/SAE-v4.
2. Click **Log in**.
   The **Sign In** page is displayed.
3. In the **Create an Account** section, enter the required details, and click **Create Account**.
4. A verification mail is sent to your email address. Click the **Verify Email** link in the email.
   An OTP is sent to your email address and you are prompted to complete the OTP verification process.
5. Enter the OTP and click **Validate Account**.
   The account is validated, and the process to create a business enterprise account is initiated.
6. If your organization profile does not exist in the backend, you are prompted to create a business enterprise account. Perform the following:
   a. Select **I own Dell EMC products or services** and click **Next**.
   b. Enter the details of your organization and click **Next**.
      A business enterprise account is created.
   c. Click **Log in**, enter the email address and password of the business enterprise account and click **Sign In**.
      The links to download SupportAssist Enterprise and generate an access key are displayed.
7. If your organization profile exists in the backend, you are prompted to select your organization. Perform the following:
   a. Enter the country and contact details of your organization.
   b. Select your preferred language.
   c. Click **Submit**.
   d. Select your organization from the displayed results and click **Submit**.
      A business enterprise account is created.
8. Click **Generate key**.
   The **Generate key** page is displayed with site details of your devices.
9. Select the required site.
10. Enter a four-digit PIN, and click **Generate key**.
    An access key is generated and sent to your email address.
11. Click **Done**.

    ⓘ **NOTE:** The access key and PIN are valid for seven days. Use the access key and PIN to complete SupportAssist Enterprise registration.

12. Click **Download File**.

Results

The SupportAssist Enterprise package is downloaded.

Upgrade to business enterprise account and download SupportAssist Enterprise

Steps

1. Go to https://www.dell.com/SAE-v4.
2. Click **Log in**.
   The **Sign In** page is displayed.
3. Enter the email address and password, and click **Sign In**.
   The **Dell EMC SupportAssist Enterprise Version 4.0 - Virtual Edition** page is displayed with links to download SupportAssist Enterprise and generate an access key.
4. Click **Business account registration**.

5. If your organization profile does not exist in the backend, you are prompted to create a business enterprise account. Perform the following:
   a. Select **I own Dell EMC products or services** and click **Next**.
   b. Enter the details of your organization and click **Next**.
      A business enterprise account is created.
   c. Click **Log in**, enter the email address and password of the business enterprise account and click **Sign In**.
      The links to download SupportAssist Enterprise and generate an access key are displayed.
6. If your organization profile exists in the backend, you are prompted to select your organization. Perform the following:
   a. Enter the country and contact details of your organization.
   b. Select your preferred language.
   c. Click **Submit**.
   d. Select your organization from the displayed results and click **Submit**.
      A business enterprise account is created.
7. Click **Generate key**.
   The **Generate key** page is displayed with site details of your devices.
8. Select the required site.
9. Enter a four-digit PIN, and click **Generate key**.
   An access key is generated and sent to your email address.
10. Click **Done**.

    NOTE: The access key and PIN are valid for seven days. Use the access key and PIN to complete SupportAssist Enterprise registration.

11. Click **Download File**.

Results

The SupportAssist Enterprise package is downloaded.

Deploying SupportAssist Enterprise

Dell EMC SupportAssist Enterprise is available as a virtual appliance that can be deployed on a hypervisor to monitor your devices and minimize the downtime. The virtual appliance is available in OVF and VHD formats. This section provides the minimum requirements and the steps to deploy the OVF and VHD files using the VMware vSphere Web Client and Microsoft Hyper-V Manager respectively.

ⓘ **NOTE:** You can deploy the OVF file only on a vCenter Server.

Topics:

Minimum requirements for deploying and using SupportAssist Enterprise

The following sections describe the minimum hardware, software, and networking requirements for deploying and using SupportAssist Enterprise.

Hardware requirements

The hardware requirements for deploying and using SupportAssist Enterprise vary depending on:

- The number of devices you want to monitor
- The SupportAssist Enterprise functionality you want to use by either collection of system information only or both monitoring and collection of system information

The following table provides a summary of the minimum hardware requirements on the server where you want to deploy SupportAssist Enterprise.

Table 2. Hardware requirements for deploying and using SupportAssist Enterprise

Devices	Monitoring	Collecting System Information	Processor	Installed memory (RAM)	Hard drive (free space)
Up to 50	Yes	Yes	4 cores	16 GB	140 GB—Thin provisioning
50 to 4250	Yes	Yes	8 cores	16 GB	140 GB—Thin provisioning

ⓘ **NOTE:** For monitoring more than 100 devices in your environment, it is recommended that you deploy SupportAssist Enterprise on a server that meets the specified hardware requirements. Periodic collections from more than 100 devices may result in a high processor or memory utilization on the monitoring server. This high resource utilization may affect other applications that are running on the monitoring server, if the resources are shared with other applications.

ⓘ **NOTE:** If SupportAssist Enterprise is deployed in a virtual environment, hardware resources of the system such as processor, memory, and I/O are shared among the virtual machines. Therefore, more hardware resources may be used by the virtual machine where SupportAssist Enterprise is deployed. For optimal performance, ensure that you allocate dedicated processor and memory to the VM as specified in the hardware requirements for SupportAssist Enterprise.

> To change the amount of processor resources allocated to a VM by using the shares, reservations, and limits settings, see the following:
>
> - - For ESX, see the "Allocate CPU Resources" section in the VMware vSphere documentation at **docs.vmware.com**.
>   - For Hyper-V, see the "Hyper-V CPU Scheduling" blog post at **msdn.microsoft.com**.
>   - For other virtual environments, see the respective documentation.

The following table provides a summary of the minimum hardware requirements on the server running SupportAssist Enterprise for performing multiple device collections.

Table 3. Hardware requirements for performing multiple device collections

Devices	Processor	Installed memory (RAM)	Hard drive (free space)
Up to 30 devices	4 cores	16 GB	10 GB
Up to 50 devices	4 cores	16 GB	40 GB
Up to 100 devices	8 cores	16 GB	60 GB
Up to 300 devices	8 cores	16 GB	100 GB

> **NOTE:** Performing a multiple device collection for Deployment, System Maintenance, or Consulting purposes may result in high system resource utilization at irregular intervals.

Software requirements

The following sections provide information about the web browser and hypervisor requirements for deploying and using SupportAssist Enterprise.

Web browser requirements

To view the SupportAssist Enterprise user interface, one of the following web browsers is required:

- Internet Explorer 10 or later
- Mozilla Firefox 31 or later
- Google Chrome 59 or later
- Microsoft Edge 38 or later

> **NOTE:** Transport Layer Security (TLS) version 1.1 or later must be enabled on the web browser.

> **NOTE:** To open SupportAssist Enterprise by using Internet Explorer:
>
> - In the **Security** tab, enable **Active Scripting**.
> - In the **Advanced** tab, enable **Play animations in web pages**.

Hypervisor requirements

- VMware vSphere versions:
  - vSphere ESXi 6.7
  - vSphere ESXi 6.5
  - vSphere ESXi 6.0
- Microsoft Hyper-V supported on:
  - Windows Server 2012
  - Windows Server 2016

Network requirements

The following are the networking requirements for the server on which you deploy SupportAssist Enterprise.

- Internet connection—Standard 1 GbE network or faster.

- The server must connect to the following destinations to ensure connectivity to the **Global and enterprise servers**:
    - **https://esrs3.emc.com**
    - **https://esrs3-core.emc.com**
    - **https://esrs3-dr.emc.com**
    - **https://esrs3-coredr.emc.com**
    - **https://esr3gduprd01.emc.com**
    - **https://esr3gduprd02.emc.com**
    - **https://esr3gduprd03.emc.com**
    - **https://esr3gduprd04.emc.com**
    - **https://esr3gduprd05.emc.com**
    - **https://esr3gduprd06.emc.com**
    - **https://esr3ghoprd01.emc.com**
    - **https://esr3ghoprd02.emc.com**
    - **https://esr3ghoprd03.emc.com**
    - **https://esr3ghoprd04.emc.com**
    - **https://esr3ghoprd05.emc.com**
    - **https://esr3ghoprd06.emc.com**
    - **https://esr3gscprd01.emc.com**
    - **https://esr3gscprd02.emc.com**
    - **https://esr3gscprd03.emc.com**
    - **https://esr3gscprd04.emc.com**
    - **https://esr3gscprd05.emc.com**
    - **https://esr3gscprd06.emc.com**
    - **https://esr3gckprd01.emc.com**
    - **https://esr3gckprd02.emc.com**
    - **https://esr3gckprd03.emc.com**
    - **https://esr3gckprd04.emc.com**
    - **https://esr3gckprd05.emc.com**
    - **https://esr3gckprd06.emc.com**
    - **https://esr3gckprd07.emc.com**
    - **https://esr3gckprd08.emc.com**
    - **https://esr3gckprd09.emc.com**
    - **https://esr3gckprd10.emc.com**
    - **https://esr3gckprd11.emc.com**
    - **https://esr3gckprd12.emc.com**
    - **https://esr3gspprd01.emc.com**
    - **https://esr3gspprd02.emc.com**
    - **https://esr3gspprd03.emc.com**
    - **https://esr3gspprd04.emc.com**
    - **https://esr3gspprd05.emc.com**
    - **https://esr3gspprd06.emc.com**
- The local system must be able to connect to the following destinations:
    - **https://downloads.dell.com/***—for downloading Dell OpenManage Server Administrator (OMSA) and receiving new SupportAssist Enterprise release information, policy files, and product support files.

      ⓘ **NOTE:** The downloads.dell.com page uses the Akamai third-party vendor for improved download experience.
    - **https://sa-is.us.dell.com/***—for TechDirect integration.

      ⓘ **NOTE:** During registration, SupportAssist Enterprise verifies connectivity to the Internet by trying to connect to **http://www.dell.com**, and then gets redirected to **https://www.dell.com**.
- SSL checking, certificate verification, and certificate proxy are not allowed on the Dell EMC SupportAssist Enterprise connection to the backend. It causes disruption to the connectivity.
- At least one DNS server must be configured.
- Do not use dynamic IP addresses.

The following table lists the network bandwidth requirements for monitoring and collecting system information from devices.

Table 4. Network bandwidth requirements

Devices	Monitoring	Collecting System Information	LAN bandwidth*	WAN bandwidth**
1	No	Yes	10 Mbps	5 Mbps
20	Yes	Yes	0.5 Gbps	10 Mbps
Up to 100	Yes	Yes	0.5 Gbps	10 Mbps
Up to 300	Yes	Yes	0.5 Gbps	10 Mbps
Up to 1000	Yes	Yes	1 Gbps	20 Mbps
Up to 4000	Yes	Yes	1 Gbps	20 Mbps

* Network bandwidth that is required for monitoring and collecting system information from devices within a single site.

** Network bandwidth that is required for monitoring and collecting system information from devices that are distributed across multiple sites.

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

Table 5. Network port requirements on the local system

Port	Direction	Usage
443	Outbound	Ensures connectivity between the local system and Dell EMC backend.
8443	Outbound	Enables remote access and remote scripting capability.

Internet Control Message Protocol (ICMP) must be enabled on the device to perform the following tasks:

- Run a device discovery rule
- Perform manual or periodic inventory validation
- Edit an account credential
- Assign a credential profile
- Edit a credential profile
- Perform periodic validation of device credentials

Deploy SupportAssist Enterprise using Hyper-V Manager

Prerequisites

You must have the VHD file in a location where you want to host the virtual disk for the virtual machine.

Steps

1. Start the Hyper-V Manager.
2. Click **Actions** > **New** > **Virtual Machine**.
   The **New Virtual Machine Wizard** window is displayed.
3. On the **Before You Begin** page, click **Next**.
4. On the **Specify Name and Location** page, perform the following and click **Next**.
   a. Enter a name for the virtual machine.
   b. By default, the virtual machine is stored at `C:\ProgramData\Microsoft\Windows\Hyper-V`. To store the virtual machine in a different location, select **Store the virtual machine in a different location**, click **Browse**, and then select a folder.
5. On the **Specify Generation** page, select **Generation 1** and click **Next**.

   NOTE: SupportAssist Enterprise does not support Generation 2.
6. On the **Assign Memory** page, enter the startup memory and click **Next**.

ⓘ **NOTE:** The minimum startup memory that you must provide is 16,384 MB.

7. On the **Configure Networking** page, from the **Connection** list, select the network adapter and click **Next**.
8. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual hard disk**, click **Browse** to select the VHD file, and then click **Next**.
9. Verify the details that are displayed on the **Summary** page and click **Finish**.
   The virtual machine is created and is displayed in the **Virtual Machines** list.
10. Right-click the virtual machine and click **Start** to power on the virtual machine.
11. Right-click the virtual machine and click **Connect**.
    The first boot process is initiated, and the **YaST2** window is displayed.
12. In the **YaST2** window, perform the following:
    a. On the **License Agreement** page, accept the terms and conditions and press F10.
    b. Select the region and time zone and press F10.
    c. Enter a root password and press F10.

    ⓘ **NOTE:** It is recommended to have a complex root password. The password may have a minimum eight characters with at least one uppercase and one lowercase letter, one number, one special character.

    ⓘ **NOTE:** Use this root password to log in to SupportAssist Enterprise for the first time after the deployment.

    d. Enter an administrator username and press F10.

    ⓘ **NOTE:** Use this username to log in to SupportAssist Enterprise after you log in with the root credentials.

    The first boot process is completed. However, you must configure the network settings to complete the deployment process.
13. To configure the network settings, perform the following:
    a. Log in to the virtual machine using the root credentials and run `yast`.
    b. On the **YaST Control Center** page, go to **System** > **Network Settings** and press F10.
    c. Press F4 to edit the network configuration settings.
    d. Enter a static IP address, subnet mask, and hostname, and then press F10.

    ⓘ **NOTE:** SupportAssist Enterprise does not support Dynamic Host Configuration Protocol (DHCP).

    e. Enter the hostname, domain name, servers and domain search information, and press F10.
    f. Enter the default IPv4 and IPv6 gateway information and press F10.
    g. Press F9 to close the **YaST2** window.

    ⓘ **NOTE:** Wait for 10-15 minutes before you log in to the SupportAssist Enterprise user interface.

Deploy SupportAssist Enterprise using VMware vSphere Web Client

About this task

ⓘ **NOTE:** You can deploy the OVF file only on a vCenter Server.

Steps

1. Download the OVF file from the support site and extract the file to a location accessible by the VMware vSphere Client.
2. On the right pane, click **Create/Register VM**.
   The **New virtual machine** window is displayed.
3. On the **Select creation type** page, select **Deploy a virtual machine from an OVF or an OVA file** and click **Next**.
4. On the **Select OVF and VMDK files** page, enter a name for the virtual machine, select the OVF and VMDK files, and click **Next**.
   The **Select storage** page is displayed.

5. If there is more than one datastore available on the host, the **Select storage** page displays such datastores. Select the location to store the virtual machine (VM) files and click **Next**.
6. On the **License agreements** page, read the license agreement, click **I agree**, and then click **Next**.
7. On the **Deployment options** page, perform the following:
    a. From the **Network mappings** list, select the network the deployment template must use.
    b. For **Disk provisioning**, select **Thin**.
    c. Click **Next**.
8. On the **Additional settings** page, enter the following details and click **Next**.
    - Domain name server
    - Hostname
    - Default gateway
    - Network IPV4 and IPV6
    - Time zone
    - Root password

        ⓘ **NOTE:** It is recommended to have a complex root password. The password may have a minimum eight characters with at least one uppercase and one lowercase letter, one number, one special character.

        ⓘ **NOTE:** Use this root password to log in to SupportAssist Enterprise for the first time after the deployment.
    - ESRS web administrator user name
9. On the **Ready to complete** page, verify the details that are displayed and click **Finish**.
    A message is displayed after the deployment is complete and the virtual machine is powered on.

    ⓘ **NOTE:** Wait for 10-15 minutes before you log in to SupportAssist Enterprise user interface.

4

Upgrading to Secure Connect Gateway

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

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

To upgrade to secure connect gateway 5.00.00.xy — virtual edition, first upgrade to SupportAssist Enterprise 4.00.05 or later. When you upgrade to secure connect gateway, the device information and settings are securely migrated.

For more information about upgrading from SupportAssist Enterprise 4.00.05 or later, see https://www.dell.com/support/kbdoc/000190637.

5

Getting started with SupportAssist Enterprise

SupportAssist Enterprise automates technical support from Dell EMC for your devices. Depending on your requirement, you can deploy and set up SupportAssist Enterprise to automate technical support for one or more of your devices.

Topics:

Open the SupportAssist Enterprise user interface

Steps

To access SupportAssist Enterprise from a remote system, open a web browser and enter the following: **`https://<IP address or host name of the server on which SupportAssist Enterprise is deployed>:5700/SupportAssist`**

For example, https://10.25.35.1:5700/SupportAssist

ⓘ **NOTE:** When typing the address, ensure that you type `SupportAssist` with the `S` and `A` in uppercase.

- If you use Internet Explorer, the following message may be displayed: **There is a problem with this website's security certificate**. To open SupportAssist Enterprise, click **Continue to this website (not recommended)**.
- If you use Mozilla Firefox, the following message may be displayed: **This Connection is Untrusted**. To open SupportAssist Enterprise, click **I Understand the Risks**, and then click **Add Exception**. In the **Add Security Exception** window, click **Confirm Security Exception**.

Log in to SupportAssist Enterprise

About this task

After you deploy SupportAssist Enterprise and complete the first boot configuration, you can log in to SupportAssist from any system in your network. When you log in for the first time, enter your root credentials, create an administrator account, and then register SupportAssist Enterprise. After you register SupportAssist Enterprise, you can login using the administrator account credentials.

Steps

1. Go to **https://<SAE IP>:5700/SupportAssist**, where <SAE IP> is the IP address of the virtual machine on which you have deployed SupportAssist Enterprise.
2. Enter **`root`** in the **Username** box.
3. Enter the password.

ⓘ **NOTE:** You must enter the same password that you entered for the root account while deploying SupportAssist Enterprise.

4. Click **Sign In**.
   The **License Agreement** page is displayed.
5. Read the terms and conditions and click **Accept**.
   The **Create an admin account** page is displayed.
6. Perform the following steps:
   a. Enter the username and password for the administrator account.

      ⓘ **NOTE:** The administrator account username is case-sensitive and must be the same as configured during the deployment.

   b. Click **Login as admin**.

   The **Welcome** page in **Set Up and Configure SupportAssist Enteprise** wizard is displayed.

Next steps

Register SupportAssist Enterprise. You cannot use SupportAssist Enterprise without registration. See Register SupportAssist Enterprise on page 22.

Register SupportAssist Enterprise

About this task

After you log in to SupportAssist Enterprise as an administrator, you must register SupportAssist Enterprise to experience the full benefits. If you do not register SupportAssist, you cannot monitor your devices for hardware issues or automatically collect system information.

Steps

1. On the **Welcome** page, click **Next**.
   The **Proxy Settings** page is displayed.
2. If your system connects to the Internet through a proxy server, perform the following steps:
   a. Select **Use proxy server**.
   b. Enter the hostname or IP address and port number.
   c. If the proxy server requires authentication, select **Requires authentication**.
   d. Enter the username and password for the proxy server.
   e. Click **Test Connection** to verify the proxy settings.
3. Click **Next**.
   The **Authentication** page is displayed.
4. Enter the access key and PIN generated while downloading the SupportAssist Enterprise package.

   If you do not have the access key and PIN, go to https://www.dell.com/SAE-v4 to create a new access key and PIN.
5. Click **Next**.
   The **Contact** page is displayed.
6. Enter the primary contact information.

   ⓘ **NOTE:** After registering SupportAssist Enterprise, you can update the primary contact information and also provide a secondary contact from **Settings** > **Contact Information** page. If the primary contact is unavailable, Dell EMC contacts your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, an email is sent to both the contacts.

7. Click **Next**.
   The **Parts Replacement Preferences for Dell EMC Servers (Optional)** page is displayed.
8. If you want Dell EMC to automatically ship the replacement parts for your servers, select **I want to have replacement part shipped automatically** and enter the primary and secondary shipping contact information.

   ⓘ **NOTE:** If you want to copy the primary contact information entered on the **Contact** page, click the link that is displayed above the **Primary Shipping Contact** section.

9. Click **Next**.
   The **Summary** page is displayed with details of the primary contact and parts dispatch information.
10. Click **Finish**.
    The **Site Health** page is displayed.

Next steps

Configure the SMTP settings to receive email notifications from SupportAssist Enterprise. See Configure SMTP server settings on page 101.

Reset administrator password

Prerequisites

You must have root access to the server on which SupportAssist Enterprise is deployed.

Steps

1. Log in to the appliance through Secure Shell (SSH) using the root credentials.
2. Run **`docker exec -it esrsde-app bash`**.
3. Go to `cd /opt/esrs/webuimgmt-util`.
4. Run **`.passwordAdmin.sh`**.
   You are prompted to reset the password.
5. Enter the new password.
6. Renter the new password.

Results

The new administrator account password is saved.

SupportAssist Enterprise product information

The **About** page displays SupportAssist Enterprise product information, host details, and setup details. You can enable or disable global-level maintenance mode or set the SupportAssist application to offline mode from the **About** page. For more information about maintenance mode, see Maintenance mode overview on page 109. For information about offline mode, see Offline mode overview on page 111.

On the SupportAssist header area, click **About** to see the SupportAssist Enterprise product information.

Network Connectivity Test

On the page you can verify and test connectivity status to servers that affect the functionality of SupportAssist Enterprise. The network connectivity test does not verify the ports used by SupportAssist Enterprise.

By default, SupportAssist Enterprise automatically tests connectivity to the dependent resources every day at 11 p.m. (time as on the server on which SupportAssist Enterprise is deployed) and displays the result in the **Status** column. If there is an issue with connectivity to a dependent resource, an email is sent to your primary and secondary contacts. You can also test SupportAssist Enterprise connectivity to the dependent servers at any time.

To view the Network Connectivity Test page, in the SupportAssist Enterprise header area, click ***user name*** and then click **Network Connectivity Test**.

The following table describes the information displayed on the **Network Connectivity Test** page.

Table 6. Network Connectivity Test

Column	Description
Test	Displays the type of dependent network servers that you can test. The available options are:

Table 6. Network Connectivity Test (continued)

Column	Description
	● **Internet Connectivity** ● **SMTP Server** ● **Global and enterprise servers**
Description	Describes the purpose of each test.
Status	Displays an icon and a message that indicates the connectivity status. The possible statuses are: ● ⚙ **Not Configured** (applicable only for the SMTP Server test)—The SMTP server settings are not configured in SupportAssist Enterprise. If your company uses an SMTP server, it is recommended that you configure **SMTP Settings** in SupportAssist Enterprise. See Configure SMTP server settings on page 101. ● 🕓 **In Progress**—The connectivity test is in progress. ● ✓ **Connected**—The connectivity test is successful. ● ⛔ **Error**—The connectivity test is unsuccessful. ⓘ **NOTE:** The **Error** status is displayed as a link that you can click to view a description of the issue and possible resolution steps.
Last Verified	The date and time the connectivity status was last verified. The date and time are displayed as on the server on which SupportAssist Enterprise is deployed.

SupportAssist Enterprise test

The **SupportAssist Enterprise Test** page enables you to verify the ability of SupportAssist Enterprise to run specific tasks.

The following table describes the information that is displayed on the **SupportAssist Enterprise Test** page:

Table 7. SupportAssist Enterprise test

Column	Description
Test	SupportAssist feature that you can test
Description	Purpose of the test
Status	An icon and a message that indicates the test status
Last Verified	Date and time when the status was last verified

Test the case creation capability

About this task

Test the **Case Creation** functionality to ensure that support case creation is working before an actual alert that would automatically create a support case.

Steps

1. In the SupportAssist Enterprise header area, click ***user name*** and then click **SupportAssist Enterprise Test**.
   The **SupportAssist Enterprise Test** page is displayed.
2. Select **Case Creation**.
3. Click **Test Connectivity**.
   One of the following statuses is displayed:
   - **Not validated**—The support case creation task has not been tested.

- 🕒 **In Progress**—The support case creation test is in progress.
- ✓ **Ready to Create Cases**—SupportAssist Enterprise can create support cases.
- ⛔ **Unable to Create Case**—SupportAssist Enterprise cannot create support cases.

SupportAssist service status

There are multiple RESTful and Core services running as part of SupportAssist Enterprise. The **Service Status** page lists these services, and their status.

In the SupportAssist Enterprise header area, click ***user name*** link and then click **Service Status** to view the **Service Status** page.

The following table describes the information that is displayed on the **Service Status** page:

Table 8. Service Status

Column	Description
Service	Name of the RESTful or core service
Status	Icon indicating the status of the service. One of the following is displayed: ● ⚙—When the service is running ● ⚙—When the service has stopped ● ⚙—When the service is disabled
Description	Purpose of the service

Evaluating SupportAssist Enterprise

SupportAssist Enterprise has several configuration settings that you can enable or disable to evaluate the monitoring and system information collection capabilities.

Evaluating the monitoring capability

You can disable SupportAssist Enterprise from monitoring some specific devices or all devices.

When you disable monitoring of a specific device, SupportAssist Enterprise does not process alerts that are received from that device. Therefore, even if a hardware issue may occur on the device, SupportAssist Enterprise does not open a support case automatically. For instructions to disable monitoring of a specific device, see Enable or disable device monitoring on page 115.

You can also temporarily disable monitoring of a specific device by placing the device in maintenance mode. Placing a device in maintenance mode ensures that SupportAssist Enterprise does not process alerts received from the device during a planned maintenance activity. For instructions to place a device in maintenance mode, see Enable or disable device-level maintenance mode on page 110.

If necessary, you can disable SupportAssist Enterprise from monitoring all your devices by placing all your devices in maintenance mode. For instructions to place all your devices in maintenance mode, see Enable or disable global-level maintenance mode on page 110.

Evaluating the system information collection capability

By default, SupportAssist Enterprise automatically collects system information from all devices at periodic intervals, and also when a support case is created. The collected system information is then sent securely to Dell. For information about the system information collected by SupportAssist Enterprise from devices, see System information collected by SupportAssist Enterprise on page 8.

You can also view the system information that is collected by SupportAssist Enterprise. For information about viewing the collected data, see Viewing collections on page 74.

If the security policy of your company restricts sending some of the collected system information outside of your company network, you can use the following configuration options available in SupportAssist Enterprise:

- You can disable the collection of identity information from all devices. See Enable or disable collection of identity information on page 81.
- You can disable the collection of software information and the system log from certain devices. See Enable or disable collection of system information on page 82.
- You can disable the periodic collection of system information from all devices. See Enable or disable periodic collection of system information on page 81.
- You can disable the automatic collection of system information when a support case is created. See Enable or disable automatic collection of system information on support case creation on page 81.
- You can also prevent the upload of collections. See Enable or disable automatic upload of collections on page 82.

NOTE: In most cases, part or all of the system information collected by SupportAssist Enterprise is required by Technical Support to properly diagnose issues and provide an appropriate resolution. To receive the full benefits of SupportAssist Enterprise, you must enable all the system information collection options.

6

Site health

SupportAssist Enterprise enables you to view the overall site health connectivity and status of your devices. Site health contains key connectivity result information that enables you to identify and prioritize the most important issue on your site.

The following table describes the information that is displayed on the **Site Health** page.

Table 9. Site Health

Field	Description
⇆	Number of active remote sessions in-progress
🔌	Number of active connect home sessions in-progress
📈	Number of REST API calls invoked by SupportAssist Enterprise.
🖥	Status of the SRS virtual engine. The following statuses are displayed: ● ✓—Connected ● ✗—Disconnected
Overview ⓘ **NOTE:** The **Overview** section is displayed only after you add devices in SupportAssist Enterprise. If you do not have any devices added in SupportAssist Enterprise, links to add a device, discover multiple devices, and set up an adapter are displayed.	Graphical representation of the number of devices in the following statuses. You can click the status to view additional details in the **Status Details** section. ● **Managed**—Click to view the number of monitored devices according to device type. ● **Staging**—Click to view the issue and resolution for devices in the group. ● **Not Managed**—Click to view the number of non-supported, disabled and offline devices. ● **Inactive**—Click to view the number of inactive devices.
Current SupportAssist Overview	Number of devices monitored by SupportAssist Enterprise and the number of support cases that are open. Click **Managed Devices** to view the **Devices** page. Click **Cases** to view the **Cases** page.
Device Validations	Total number of devices that are discovered or added in SupportAssist Enterprise and their site-wide inventory validation status is displayed. The following statuses are displayed: ● ✓ **Success**—Number of devices for which tests for connectivity, collection capability, and monitoring capability were successful. ● ⛔ **Failed**—Number of devices for which tests for connectivity, collection capability, or monitoring capability were not successful. The total count of devices in Site Inventory Validation may not match the total number of devices that you have added or discovered in SupportAssist Enterprise. This variance is because inventory validation does not support validating: ● Devices added in SupportAssist Enterprise through the adapter

Table 9. Site Health (continued)

Field	Description
	- Devices that require manual configuration of SNMP settings, for example, networking devices
Network Resources	Status of SupportAssist Enterprise connectivity to the following network resources: - **Dell EMC Enterprise Servers** - **Dell EMC Global Access Servers** - **SMTP Server**

7

Adding devices

Adding devices prepares SupportAssist Enterprise to automate support from Dell EMC Technical Support for your devices. To use SupportAssist Enterprise to either monitor hardware issues or collect system information from your devices, you must add your devices in SupportAssist Enterprise.

For the complete list of devices types and device models that you can add in SupportAssist Enterprise, see the *SupportAssist Enterprise Version 4.0 Support Matrix* at https://www.dell.com/serviceabilitytools.

ⓘ **NOTE:** By default, a SupportAssist component is available on 14th generation of PowerEdge servers. You can register the SupportAssist component on the server to receive the automated support capabilities of SupportAssist. When an iDRAC is added in SupportAssist Enterprise, the SupportAssist component is automatically disabled, but the automatic support capabilities are available through SupportAssist Enterprise.

ⓘ **NOTE:** IPv4 and IPv6 addresses are supported for adding devices and collecting system information.

If the device is part of a domain, you must configure its Domain Name System (DNS) correctly to view the host name in the **Devices** page.

Topics:

Methods of adding devices

You can add devices in SupportAssist Enterprise by using one of the following methods:

- Add a single device—Add each device individually by entering the details of the device
- Create a device discovery rule—Add devices based on a specific IP address range. For more information about discovery rules, see Create device discovery rule on page 58.
- Set up an adapter—Inventory and add devices that are managed by OpenManage Enterprise. For more information about setting up an adapter, see Adapters on page 90.
- Add device to SupportAssist through REST protocol using the user interface available on the device.

For information about the device types and models that can be monitored using SupportAssist, see Device types and applicable devices on page 29.

Device types and applicable devices

The following table lists the devices that you can add by selecting a specific device type.

NOTE: SupportAssist Enterprise may not be compatible with all models of a supported device type. For the list of supported device types and corresponding models, see the *SupportAssist Enterprise version 4.0 Support Matrix* available at https://www.dell.com/serviceabilitytools.

Table 10. Device types

Device Type	Devices that you can add
Chassis	● PowerEdge M1000e ● PowerEdge VRTX ● PowerEdge FX2/FX2s ● PowerEdge MX7000
Data Protection	● AppSync[1] ● Avamar[3] ● CloudBoostAppliance[1] ● DPA[1] ● DataDomain[3] ● iDPA ● DPAppliance[1] ● EMCeCDM[1] ● Networker[1] ● PowerPath[1] ● RecoverPoint[2] ● UCC[1]
iDRAC	12th and later generations of PowerEdge servers **NOTE:** To add an iDRAC, you must provide the iDRAC IP address of the server.
Networking	● PowerConnect ● Force10 ● Dell Networking ● Networking Wireless Controllers Mobility Series ● Other supported Networking devices (Brocade and Cisco)
Server/Hypervisor	9th and later generations of PowerEdge servers running: ● Linux ● VMware ESX or ESXi ● Citrix XenServer ● Oracle Virtual Machine **NOTE:** To add a server or hypervisor, you must provide the operating system IP address of the server.
Software	● HIT Kit/VSM for VMware ● vCenter
Virtual Machine	● Linux
Converged infrastructure appliance	● VxBlock ● PowerOne ● VCE Vision[1] ● VxBlock Central ● WebScale
Hyperconverged infrastructure appliance	● VxFlex ● VxFlex OS ● VxFlex appliance ● VSPEXBLUE/VXRail[1] ● VxRackFlex[1] ● VXRack SDDC[1]

Table 10. Device types (continued)

Device Type	Devices that you can add
Data Storage	● Fluid File System (FluidFS) ○ Storage PS Series with FluidFS ○ Storage MD Series with FluidFS ○ Storage SC Series with FluidFS ● Peer Storage (PS)/EqualLogic ○ Storage PS Series arrays ● PowerVault ○ Storage MD Series arrays ○ Storage ME4 Series arrays ● Storage Center (SC)/Compellent ○ Storage SC Series solutions ● Atmos[2] ● Celerra[2] ● Centera[2] ● Clariion[2] ● CloudArray[1] ● CloudIQ-CLTR[1] ● CustManageSta[2] ● DL3D[2] ● DLm3[2] ● DLm4[3] ● DLm[2] ● DSSD[1] ● EDL-Engine[2] ● ElasticCloudStorage[3] ● Isilon or PowerScale[3] ● Isilon-SD[1] ● ScaleIO[1] ● Symmetrix[2] ● Unity[1] ● VMAX3[3] ● VNXe[2] ● VNX[2] ● ViPR[3] ● ViPRSRM[1] ● XtremIO[3] ● Connectrix[3] ● Switch-Brocade-B[3] ● Switch-Cisco[2]

- 1—Device must be added to SupportAssist Enterprise directly from the device using the RESTful protocol.
- 2—Device can be added from the SupportAssist Enterprise user interface.
- 3—Device can be added from the SupportAssist Enterprise user interface and also using RESTful protocol. If you add this device from the SupportAssist user interface, only limited SupportAssist capabilities are enabled for the device. See the product configuration documentation for the model and version for connectivity configuration.

Add chassis

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Ports 22, 161, and 443 must be open on the device.
- SSH service must be running on the device.

About this task

You can monitor your chassis for hardware issues and collect system information. For the list of chassis models that you can add, see Device types and applicable devices on page 29.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ➕.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Chassis**.
4. Enter the hostname or IP address of the device in the appropriate field.

   ⓘ **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
7. Perform one of the following steps:
   - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.
   - If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
8. If you do not want SupportAssist Enterprise to monitor hardware issues that may occur on the device, clear the **Enable Monitoring** check box.
9. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
10. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

    If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
11. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.
12. Click **OK**.
    The **Devices** page is displayed.

Next steps

⚠ **CAUTION: If the device is not configured to forward alerts, SupportAssist Enterprise cannot detect hardware issues that may occur on the device.**

For monitoring hardware issues that may occur on the device only, ensure that the device is configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is deployed. For instructions how to configure alert forwarding, see Manually configuring SNMP settings on page 112.

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add data protection device

Prerequisites

The device must be reachable from the server where SupportAssist Enterprise is deployed.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Protection**.
4. From the **Model type** list, select the required model.
5. Enter the IP address and serial number of the device in appropriate fields.
6. From the **Extension** list, select the device extension.
7. Click **Next**.
   The summary page is displayed with the device details.

   > **NOTE:** Certain device types are added to the device inventory and displayed on the **Devices** page only after they are validated. This process may take up to 24 hours.
8. Click **OK**.
   The **Devices** page is displayed.

Add iDRAC

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- The device must be a 12th or later generation Dell PowerEdge server (iDRAC7 or later). For information about identifying the generation of a PowerEdge server, see Identify series of PowerEdge server on page 123.
- If the device connects to the Internet through a proxy server, ports 161 and 443 must be open on the proxy server firewall.
- To add an iDRAC7 or iDRAC8, Enterprise or Express license must be installed on the iDRAC. To add an iDRAC9, Basic, Enterprise, or Express license must be installed on the iDRAC. For information about purchasing and installing an Enterprise or Express license, see the “Managing Licenses" section in the *iDRAC User’s Guide* at www.dell.com/idracmanuals.

About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from Dell servers. You can perform the following steps to add Dell's 12th or later generation of PowerEdge servers. While adding the device, you can enable SupportAssist Enterprise to automatically configure the SNMP settings of the device. Configuration of SNMP settings is required to forward alerts from the device to SupportAssist Enterprise.

> **NOTE:** By default, a SupportAssist component is available on 14th generation PowerEdge servers. You can register the SupportAssist component on the server to receive the automated support capabilities of SupportAssist. When an **iDRAC** is added in SupportAssist Enterprise, the SupportAssist component is automatically disabled, but the automatic support capabilities are available through SupportAssist Enterprise.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **iDRAC**.
4. Enter the hostname or IP address of the device in the appropriate field.

NOTE: It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
6. From the **Account Credentials** list, select an account credential that you want to assign to the device. To create a new account credential, select **Create New Account** and then click **Create**. See Add account credentials on page 61.
7. If you do not want SupportAssist Enterprise to monitor hardware issues that may occur on the device, clear the **Enable monitoring** and **Configure SNMP settings** check boxes.

   For SupportAssist Enterprise to monitor hardware issues that may occur on the device, the device must be configured to forward SNMP traps (alerts) to the server where SupportAssist Enterprise is deployed. To help you meet this requirement, SupportAssist Enterprise can configure SNMP trap (alert) forwarding automatically. To enable SupportAssist Enterprise to automatically configure the device to forward alerts, the **Configure SNMP settings** option must be selected. A task to configure alert forwarding is initiated after the device is added successfully to the device inventory.

   NOTE: If you prefer to configure alert forwarding manually, clear the **Configure SNMP settings** check box.

8. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
9. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
10. Click **Finish**.

    NOTE: If you have selected the **Configure SNMP Settings** option, device addition may take some time.

    The device is added to the device inventory, and the **Summary** page is displayed.
11. Click **OK**.

    CAUTION: If the SNMP settings of the device are not configured to forward alerts to the server where SupportAssist Enterprise is deployed, SupportAssist Enterprise cannot monitor hardware issues that may occur on the device.

    The device is added to the device inventory with an appropriate status. When SupportAssist Enterprise is configuring the SNMP settings, the device displays a 🕒 **Configuring SNMP** status. After the configuration of SNMP settings is completed, the device status changes to ✓ **Success**. If an issue occurs during the configuration of SNMP, the device displays an appropriate status in the **Devices** page.

    NOTE: If the device displays an ⛔ error status, click the error link to view the description of the issue and possible resolution steps. To retry the SNMP configuration, you can use the **Tasks** list available on the device overview pane.

Next steps

Optionally, add the server in SupportAssist Enterprise by using the operating system details. In this case, SupportAssist Enterprise automatically correlates the alerts and collection of system information from both the operating system and the iDRAC. For instructions to add the server, see Add server or hypervisor on page 36. For more information about how SupportAssist Enterprise correlates device information, see Device correlation on page 121.

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add networking device

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Ports 22 and 161 must be open on the device.
- SSH and SNMP services must be running on the device.

About this task

You can monitor your networking devices for hardware issues and collect system information. For the list of networking devices that you can add, see Device types and applicable devices on page 29.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Networking**.
4. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
7. Perform one of the following steps:
   - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.
   - If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
8. If you do not want SupportAssist Enterprise to monitor hardware issues that may occur on the device, clear the **Enable monitoring** check box.

   SupportAssist Enterprise can monitor the device only if the SNMP settings of the device are configured to the forward SNMP traps (alerts) to SupportAssist Enterprise. For instructions to configure alert forwarding, see Manually configure alert destination of networking device on page 114.
9. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
10. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

    If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
11. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.
12. Click **OK**.
    The **Devices** page is displayed.

Next steps

> **CAUTION: If the device is not configured to forward alerts, SupportAssist Enterprise cannot detect hardware issues that may occur on the device.**

For monitoring hardware issues that may occur on the device only, ensure that the device is configured to forward SNMP traps (alerts) to SupportAssist Enterprise. For instructions to configure alert forwarding, see Manually configure alert destination of networking device on page 114.

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add server or hypervisor

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- If the device is running a Linux operating system:
  - SSH service must be running on the device.
  - SSH password authentication must be enabled (enabled by default).
  - Unzip package must be installed on the server where SupportAssist Enterprise is deployed.
- If the device is running VMware ESXi, ESX, Oracle Virtual Machine, or Citrix XenServer:
  - SSH service must be running on the device.
  - Ports 22 and 443 must be open on the device.
  - For collecting system information from ESX and ESXi only, ensure that SFCBD and CIMOM are enabled.
- Port 1311 must be open on the device for OMSA communication.
- If the device connects to the Internet through a proxy server, the following ports must be open on the proxy server firewall: 161, 22 (for adding devices running Linux) and 1311.
- Review the requirements for installing OMSA on the device. For more information, see the “Installation Requirements” section in the *Dell OpenManage Server Administrator Installation Guide* at www.dell.com/openmanagemanuals.

About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from Dell EMC servers. You can perform the following steps to add a Linux server or a hypervisor. While adding the device, you can enable SupportAssist Enterprise to automatically perform the following tasks that are required for monitoring hardware issues that may occur on the device:

- Install or upgrade OMSA — OMSA is required to generate alerts for hardware events that occur on the device and also to collect system information from the device.
- Configure SNMP — Configuration of SNMP settings is required to forward alerts from the device to SupportAssist Enterprise.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ⊞.
   The **Add single device** window is displayed.
3. From the **Device Type** list, select **Server/Hypervisor**.
4. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
6. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
7. Perform one of the following steps:
   - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.

- If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.

8. If you do not want SupportAssist Enterprise to monitor hardware issues that may occur on the device, clear the **Enable monitoring**, **Configure SNMP settings**, and **Install or upgrade OMSA** check boxes.

   For SupportAssist Enterprise to monitor hardware issues that may occur on the device, the following dependencies must be met:

   - The SNMP settings of the device must be configured to forward SNMP traps (alerts) to SupportAssist Enterprise.
   - The recommended version of Dell OpenManage Server Administrator (OMSA) must be installed on the device.

   To help you meet these dependencies, SupportAssist Enterprise can configure SNMP trap (alert) forwarding and also install or upgrade OMSA automatically on the device. To enable SupportAssist Enterprise to automatically:

   - Configure the device to forward alerts, ensure that the **Configure SNMP Settings** option is selected.
   - Install or upgrade OMSA on the device, ensure that the **Install / Upgrade OMSA** option is selected.

   Tasks to configure alert forwarding and to install OMSA are initiated after the device is added successfully to the device inventory.

   NOTE: If you prefer to perform both tasks (configure alert forwarding and install or upgrade OMSA) manually, clear the **Configure SNMP settings** and **Install or upgrade OMSA** check boxes.

9. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.

10. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

    If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.

11. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.

12. Click **OK**.

    CAUTION: If the SNMP settings of the device are not configured and OMSA is not installed on the device, SupportAssist Enterprise cannot monitor hardware issues that may occur on the device.

    NOTE: Installation of OMSA is not supported on devices running CentOS, Oracle Virtual Machine, and Oracle Enterprise Linux. When you add these devices with the **Device Type** as **Server / Hypervisor**, SupportAssist Enterprise can only collect and upload system information. To enable SupportAssist Enterprise to monitor these devices for hardware issues, add these devices by selecting the **Device Type** as **iDRAC**. See Add iDRAC on page 33.

    The device is added to the device inventory with an appropriate status:

    - When SupportAssist Enterprise is configuring the SNMP settings, the device displays a 🕓 **Configuring SNMP** status.
    - When SupportAssist Enterprise is installing or upgrading OMSA, the device displays an 🕓 **Installing OMSA** status.

    After the installation of OMSA and configuration of SNMP settings are completed, the device status changes to ✓ **Success**. If an issue occurs during the configuration of SNMP or OMSA installation, the device displays an appropriate status in the **Devices** page.

    NOTE: If the device displays an ⛔ error status, click the error link to see a description of the issue and the possible resolution steps. To retry the OMSA installation or SNMP configuration, use the **Tasks** list available on the device overview pane.

Next steps

Optionally, add the server in SupportAssist Enterprise by using the iDRAC details. In this case, SupportAssist Enterprise automatically correlates the alerts and collection of system information from both the operating system and the iDRAC. See Add iDRAC on page 33. For more information about how SupportAssist Enterprise correlates device information, see Device correlation on page 121.

Add software

Prerequisites

The device must be reachable from the server where SupportAssist Enterprise is deployed.

About this task

SupportAssist Enterprise can only collect system information from the following management and monitoring software:

- VMware vCenter
- Host Integration Toolkit for VMware (HIT Kit/Virtual Storage Manager)

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Software**.
4. From the **Software type** list, select the software type.
5. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. From the **Account Credentials** list, select the credentials account you want to assign to the device and click **Next**. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
   - If you selected a credentials account, the **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device. If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
   - If you clicked **Create New Account**, the **Add Account Credential** window is displayed. See Add account credentials on page 61.
8. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
9. Click **Finish**.
   The device is added to the device inventory and the **Summary** page is displayed.
10. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add virtual machine

Prerequisites

- The system hosting the virtual machine must be reachable from the server where SupportAssist Enterprise is deployed.
- The virtual machine you want to add must be created on VMware ESX, ESXi, and Microsoft Hyper-V.

About this task

SupportAssist Enterprise can only collect system information from virtual machines.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ⊞.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Virtual Machine**.
4. Enter the hostname or IP address of the device in the appropriate field.

   > ⓘ **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
6. From the **Account Credentials** list, select the credentials account you want to assign to the device and click **Next**. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
   - If you selected a credentials account, the **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device. If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
   - If you clicked **Create New Account**, the **Add Account Credential** window is displayed. See Add account credentials on page 61.
7. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
8. Click **Finish**.
   The device is added to the device inventory and the **Summary** page is displayed.
9. Click **OK**.
   The **Devices** page is displayed.

Add converged or hyperconverged infrastructure appliance

Prerequisites

The device must be reachable from the server where SupportAssist Enterprise is deployed.

About this task

SupportAssist Enterprise enables you to monitor and collect system information from converged or hyperconverged infrastructure appliances. However, the system information collection capability is available only for the web-scale model. For the list of supported converged or hyperconverged infrastructure appliances, see Device types and applicable devices on page 29.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ⊞.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Hyper-Converged Infrastructure**.
4. From the **Model type** list, select the required model.
   The appropriate fields are displayed.

5. To add a **Web Scale** appliance, see Add web-scale solution on page 40.
6. To add any other model, perform the following steps:
    a. Enter the IP address and serial number of the device in appropriate fields.
    b. From the **Extension** list, select the device extension.
    c. Click **Next**.
    The summary page is displayed with the device details.

    > **NOTE:** Certain device types are added to the device inventory and displayed on the **Devices** page only after they are validated. This process may take up to 24 hours.
7. Click **OK**.
   The **Devices** page is displayed.

Add web-scale solution

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Ports 9440 and 22 must be open on the device.
- For a web-scale solution, firmware version 4.x or later must be installed on the device for the collection of system information.

About this task

SupportAssist Enterprise can monitor hardware issues and collect system information from a web-scale hyperconverged appliance.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ⊞.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Hyper-Converged Infrastructure**.
4. From the **Solution/Model type** list, select **Web Scale**.
5. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.
6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
8. Perform one of the following steps:
    - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.
    - If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
9. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
10. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.
11. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add data storage device

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- For models other than the PS series, SC series, MD series, or NAS, at least one DNS server must be configured.

About this task

Monitor and collect system information from data storage devices. You can collect system information on demand and after deployment. However, the system information collection capability is available only for the following models of data storage devices:

- Storage PS Series (previously EqualLogic) arrays
- Storage SC Series
- Fluid File System (FluidFS) network attached storage (NAS)
- Storage MD Series arrays

For the list of data storage devices that you can add, see Device types and applicable devices on page 29.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ➕.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Storage**.
4. From the **Model type** list, select the required data storage model.
   The appropriate fields are displayed.
5. To add a **PeerStorage(PS) / Equallogic** device, see Add EqualLogic PS Series storage arrays on page 41.
6. To add a **Storage Center (SC) / Compellent** device, see Add a Compellent SC Series storage solution on page 42.
7. To add a **Fluid File System (Fluid FS)** device, see Add a Fluid File System NAS device on page 43.
8. To add a **PowerVault** device, see Add a PowerVault storage array on page 44.
9. To add any other model, perform the following steps:
   a. Enter the IP address and serial number of the device in appropriate fields.
   b. From the **Extension** list, select the device extension.
   c. Click **Next**.
      The summary page is displayed with the device details.

      > ⓘ **NOTE:** Certain device types are added to the device inventory and displayed on the **Devices** page only after they are validated. This process may take up to 24 hours.
10. Click **OK**.
    The **Devices** page is displayed.

Add EqualLogic PS Series storage arrays

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Ports 21, 22, and 161 must be open on the device.
- SSH and SNMP service must be running on the device.

About this task

SupportAssist Enterprise can only collect system information from the Storage PS Series (previously EqualLogic) arrays. By adding a Storage PS Series device, you will be able to collect system information on demand and after deployment.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Storage**.
4. From the **Model type** list, select **Peer Storage (PS) / EqualLogic**.
5. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
8. Perform one of the following steps:
   - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.
   - If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
9. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
10. If desired, from the **Assign Other Group** list, select a device group to which you want to assign the device.

    If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
11. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.
12. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add a Compellent SC Series storage solution

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Port 443 must be open on the device.
- REST service must be running on the device.
- For collecting system information, SupportAssist must be enabled in the Dell Compellent Enterprise Manager application for Compellent devices with SC Series storage solution 7.1 and below.

About this task

SupportAssist Enterprise can only collect system information from the Storage SC Series solutions. By adding a Storage SC Series device, you will be able to collect system information on demand and after deployment.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click +.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Storage**.
4. From the **Model type** list, select **Storage Center (SC) / Compellent**.
5. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. From the **Account Credentials** list, select the credentials account you want to assign to the device and click **Next**. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
   - If you selected a credentials account, the **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device. If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
   - If you clicked **Create New Account**, the **Add Account Credential** window is displayed. See Add account credentials on page 61.
8. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
9. Click **Finish**.
   The device is added to the device inventory and the **Summary** page is displayed.
10. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add a Fluid File System NAS device

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Ports 22 and 44421 must be open on the device.
- SSH service must be running on the device.

About this task

SupportAssist Enterprise can only collect system information from a Dell Fluid File System (FluidFS) network attached storage (NAS) device. By adding a FluidFS NAS device, you will be able to collect system information on demand and after deployment. For the list of Fluid File Systems (FluidFS) you can add, see Device types and applicable devices on page 29.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.

2. Click ➕.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Storage**.
4. From the **Model type** list, select **Fluid File System (FluidFS)**.
5. Enter the hostname or IP address of the device in the appropriate field.

   > ⓘ **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. From the **Account Credentials** list, select the credentials account you want to assign to the device and click **Next**. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
   - If you selected a credentials account, the **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device. If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
   - If you clicked **Create New Account**, the **Add Account Credential** window is displayed. See Add account credentials on page 61.
8. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
9. Click **Finish**.
   The device is added to the device inventory and the **Summary** page is displayed.
10. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add a PowerVault storage array

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- Port 2463 must be open on the device.

About this task

SupportAssist Enterprise can only collect system information from the Storage MD Series arrays. By adding a Storage MD Series device, you will be able to collect system information on demand and after deployment.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click ➕.
   The **Add single device** window is displayed.
3. From the **Device type** list, select **Data Storage**.
4. From the **Model type** list, select **PowerVault**.
5. Enter the hostname or IP address of the device in the appropriate field.

   > ⓘ **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.

6. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.
7. To discover and add other supported device types that may be associated with the chassis, select the **Perform deep discovery** check box. See Deep discovery on page 121.
   The **Credential profile** list is displayed.
8. Perform one of the following steps:
   - If you enabled deep discovery, select the credential profile that you want to assign to the device and its associated device types. To create a new credential profile, click **Create New Profile** and then click **Create**. See Create credential profile on page 63.
   - If you did not enable deep discovery, select the credentials account that you want to assign to the device from the **Account Credentials** list. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
9. Click **Next**.
   The **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device.

   If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
10. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

    If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
11. Click **Finish**.
    The device is added to the device inventory and the **Summary** page is displayed.
12. Click **OK**.
    The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Add device by duplication

Prerequisites

- The device must be reachable from the server where SupportAssist Enterprise is deployed.
- The required network ports must be open on the device.

About this task

Add a device that is of the same type as a device that you have already added.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select a device which is of the same type as the device that you want to add.
   The device overview pane is displayed.
3. Click **Duplicate**.
   The **Duplicate Device** wizard is displayed.
4. Enter the hostname or IP address of the device in the appropriate field.

   > **NOTE:** It is recommended that you enter the hostname of the device. If the hostname is not available, you can enter the IP address of the device.
5. If desired, enter a name for the device in the **Name** box.

   The name that you enter is used to represent the device in SupportAssist Enterprise. If you do not enter a name, the IP address or hostname is used to represent the device.

6. From the **Account Credentials** list, select the credentials account you want to assign to the device and click **Next**. To create a new set of account credentials, click **Create New Account** and then click **Create**. See Add account credentials on page 61.
   - If you selected a credentials account, the **Discovering Device** page is displayed until SupportAssist Enterprise identifies the device. If the device is discovered successfully, the **Assign Device Group (Optional)** page is displayed. Otherwise, an appropriate error message is displayed.
   - If you clicked **Create New Account**, the **Add Account Credential** window is displayed. See Add account credentials on page 61.
7. If desired, from the **Assign other group** list, select a device group to which you want to assign the device.

   If you do not select a device group, the device is assigned to the **Default** device group. For information about the **Default** device group, see Predefined device groups on page 54.
8. Click **Finish**.
   The device is added to the device inventory and the **Summary** page is displayed.
9. Click **OK**.
   The **Devices** page is displayed.

Next steps

If a message is displayed stating that the device is added to the **Staging** group:

1. Ensure that all prerequisites for adding the device are met.
2. Perform inventory validation on the device. See Start inventory validation manually on page 66.

Export device data

About this task

Use this option to save the following details from the **Devices** page to a CSV file:

- Hostname or IP address
- Serial number
- Service Tag
- Model
- Deployment status
- Serviceability status

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Click 📤.
   The device details are saved in a CSV file.

Delete device

About this task

You can delete one or more devices from SupportAssist Enterprise, if you do not want to monitor a device or for other reasons.

> ⓘ **NOTE:** Deleting a device only removes the device from the SupportAssist Enterprise user interface; it does not affect the functionality of the device.

> ⓘ **NOTE:** Devices that are inventoried and added in SupportAssist Enterprise through an adapter cannot be deleted. Those devices are deleted automatically from SupportAssist Enterprise when either the adapter is deleted or the devices are removed from the systems management console.

> ⓘ **NOTE:** If you add a device to SupportAssist Enterprise using the RESTful protocol, you must disable it from the device's user interface to delete it from SupportAssist Enterprise.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the devices that you want to delete.
3. Click 🗑 .
   The **Confirm Device Deletion** window is displayed.
4. Click **Yes**.
   The devices are deleted from the **Devices** page.

   ⓘ **NOTE:** When a device is deleted, the system information collected from the device is not deleted until the purge collections task deletes the collected system information. The purge collection task only deletes system information collections that are 30 days or older and collections that are older than the last five collections over the last 30 days.

Devices

The **Devices** page displays the devices that you have added, and the status of the SupportAssist Enterprise functionality for each device. The default view shows all the devices you have added.

The following table describes the options displayed on the **Devices** page and the automatically generated inventory information for the devices displayed on the **Devices** page.

Table 11. Devices page

Options/Column	Description
🌐	View the site ID of the account
Search by list	Search by a specific category of displayed data
Search term	Enter the search keyword ⓘ **NOTE:** You must enter a minimum of 3 characters to perform the search.
🔄 **Refresh**	Refresh the data displayed on the page.
View by	View the devices in a ☰ (list) view or ▦ (association) view
Registration ID	Registration ID of SupportAssist Enterprise appliance deployed
Serial Number	Serial number of SupportAssist Enterprise appliance deployed
⇄	Number of active remote sessions in-progress
🔌	Number of active connect home sessions in-progress
📈	Number of REST API calls invoked by SupportAssist Enterprise
🖥	Status of the SRS VE. The following status are displayed: ● ✓—Connected ● ✖—Disconnected
➕	Add a device
✏	Update the name, account credentials, or IP address depending on the device type
🗑	Delete a device
↗	Save the device details in a CSV file
Start Collection	Initiate a single device or multiple device collections

Table 11. Devices page (continued)

Options/Column	Description
Collection Purpose list	Select a reason for performing a multiple device collection
Assign Credential Profile list	Assign credentials for devices
Validate Inventory	Validate device inventory
Check box	Select single or multiple devices to perform device-specific tasks. The check box is disabled while the following SupportAssist Enterprise initiated tasks are in progress: ● SNMP configuration ● Installation or upgrade of OMSA ● Clear system event log ● Collection of system information immediately after an automatic support case creation as well as during a manually initiated collection ● Inventory validation
Name / IP Address	Displays the following information: ● Device name—Displays the name, host name, serial number, or IP address depending on the information you have provided for the device. ● Collection status—When a collection occurs, a progress bar and a corresponding message are displayed to indicate the status of the collection. The possible collection status messages are: ○ For a collection that you manually initiate: ⓘ **NOTE:** When a manually initiated collection is in progress, ✖ is displayed next to the progress bar. Click ✖ to cancel the collection, if necessary. ⓘ **NOTE:** You can cancel a collection only when SupportAssist Enterprise is collecting system information from the device. You cannot cancel a collection while the collected system information is being sent to the backend. ■ **Starting collection** ■ **Collection in progress** ■ **Sending collection** ■ **Canceling collection** ○ For an automated collection that is initiated because a support case was created for a detected hardware issue: ■ **Starting collection for support case** ■ **Collection for support case in progress** ■ **Sending collection for support case** ⓘ **NOTE:** If a hardware issue is detected on a device with a Dell Basic Service contract, an automated collection is initiated. However, a support case is not created for that device. ○ For an automated periodic collection based on the default or configured collection schedule: ■ **Starting periodic collection** ■ **Periodic collection in progress** ■ **Sending periodic collection** ⓘ **NOTE:** In some instances, when a collection is in progress (manual) on a device another collection (periodic) may be initiated. In such cases, the collection status is displayed in the following order of priority: ○ Manual collection ○ Support case collection ○ Periodic collection ● Maintenance mode—If the device is placed in maintenance mode, the maintenance mode icon 🔧 is displayed.
Model	Model of the device, for example, PowerEdge M820
Status	The status of inventory validation. The status can be categorized as follows:

Table 11. Devices page (continued)

Options/Column	Description
	- **Success**—Inventory validation of the device is successfully complete. - **Failed**—Inventory validation of the device is unsuccessful. - **In progress**—Inventory validation of the device is in progress. - When the inventory validation is yet to be initiated on the device, no status is displayed. For the following devices or device models, the **Success** status is displayed only if the **Connectivity Monitoring** and **Validation Status** fields in the device overview pane display **Online** and **Connected** statuses respectively: - Data protection - Data storage devices other than PeerStorage (PS) / Equallogic, Storage Center (SC) / Compellent, Fluid File System (Fluid FS), and PowerVault models - Hyperconverged infrastructure appliances - Converged infrastructure appliances other than Web Scale model

The **Refine By** pane enables you to refine the list of the devices displayed using the following filters:

- **Device Type**
- **Need Attention**
  - **Staging**—Displays a status icon and a rollup count of number of devices that are present in the **Staging** group.
  - **Inactive**—Displays a status icon and a rollup count of number of devices that are present in the **Inactive** group.
- **Inventory Validation**
  - **Success**—Displays a status icon and the rollup count of number of devices that were validated successfully.
  - **Failed**—Displays a status icon and the rollup count of number of devices that were not validated successfully.
- **Groups**
  - **Default**—Displays all devices.
  - Custom created groups are also displayed.
- **Collection Host**
- **Devices Added**

The **Devices** page also displays the following panes based on your actions:

- Device overview pane — When only a single device is selected. See Device overview pane on page 49.
- Multiple Device Collection pane — When a multiple device collection is in progress. See Multiple Device Collection pane on page 87.

Device overview pane

The device overview pane displays the details of a device and allows you to perform certain operations on that device. This pane is displayed when you select only a single device in the **Devices** page.

The following table describes the fields displayed in the device overview pane for the following devices or device models:

- Server or Hypervisor
- iDRAC
- Chassis
- Networking
- PeerStorage (PS) or EqualLogic
- Storage Center (SC) / Compellent
- Fluid File System (FluidFS)
- PowerVault

Table 12. Device overview pane

Field	Description
Tasks list	- **Clear System Event Log**—Clear the System Event Log (SEL) or Embedded System Management (ESM) log. - **Check for Cases**—Check for support cases that are present for a device.

Table 12. Device overview pane (continued)

Field	Description
	● **Perform deep discovery**—Discover a device and its associated device types. ● **Maintenance Mode** ○ **Enable**—Place the device in maintenance mode. ○ **Disable**—Place the device in normal mode. ● **Dependencies** ○ **Install / Upgrade OMSA**—Install or upgrade OMSA on the device. ○ **Configure SNMP**—Configure the SNMP settings of the device.
Hostname / IP address	IP address or host name of the device.
Model	Model of the device, for example, PowerEdge M820.
Service Tag	Unique, alphanumeric identifier that allows Dell EMC to recognize the device.
Monitoring	● **Enable**—Enable monitoring for hardware issues that may occur with the device. ● **Disable**—Disable monitoring for hardware issues that may occur with the device.
Software Version	Version of the firmware installed on the device.
Display Name	Name that you have provided for the device.
Device Type	Type of the device, for example, Server.
Collections list	List that contains the collection history. Select a date and time from the list to view the system information that was collected. **No Collections** is displayed when no collections was performed from the device.
Next Scheduled Collection	Date and time of the next scheduled collection.
Last Device Job Status	Status of the SupportAssist Enterprise functionality on the device, and the date and time the status was generated. The status can be categorized as follows: **Informational status** ● ✓ **OK**—The device is configured correctly for SupportAssist Enterprise functionality. ● 🕒 **Installing OMSA**—Installation or upgrade of Dell OpenManage Server Administrator (OMSA) is in progress. ● 🕒 **Configuring SNMP**—Configuring the SNMP settings of the device is in progress. ● 🕒 **Clearing System Event Log**—Clearing of the System Event Log is in progress. ● ✓ **System Event Log cleared**—System Event Log has been cleared successfully. ● 🕒 **Revalidating device**—SupportAssist Enterprise is validating the prerequisites and the credentials of the device.

Table 12. Device overview pane (continued)

Field	Description
	Warning status ● ⚠ **OMSA not installed**—OMSA is not installed on the device. ● ⚠ **SNMP not configured; OMSA not latest**—SNMP settings of the device is not configured and the OMSA version installed on the device is prior to the recommended version of OMSA for SupportAssist Enterprise. ● ⚠ **SNMP not configured**—SNMP settings of the device is not configured. ● ⚠ **New version of OMSA available**—A newer version of OMSA is available for installation on the device. ● ⚠ **OMSA installed, reboot the added device**—Installation of OMSA is complete on the device. Restart the device for the changes to take effect. **Error status** ● ⛔ **Unable to add device**—SupportAssist Enterprise has placed the device in the **Staging** group because the device did not meet certain prerequisites. For more information on the **Staging** group, see Predefined device groups on page 54. ● ⛔ **Unable to configure SNMP**—SupportAssist Enterprise is unable to configure the SNMP trap destination of the device. ● ⛔ **Unable to verify SNMP configuration**—SupportAssist Enterprise is unable to verify the SNMP configuration of the iDRAC. ● ⛔ **Unable to install OMSA**—Installation of OMSA could not be completed. ● ⛔ **OMSA not supported**—Installation of OMSA is not supported. ● ⛔ **Unable to reach device**—SupportAssist Enterprise is unable to communicate with the device. ● ⛔ **Authentication failed**—SupportAssist Enterprise cannot log in to the device. ● ⛔ **Unable to gather system information** —SupportAssist Enterprise is unable to collect system information from the device. ● ⛔ **Insufficient storage space to gather system information**—The server where SupportAssist Enterprise is deployed does not have sufficient space to gather system information from the device. ● ⛔ **Unable to export collection**—SupportAssist Enterprise is unable to process the collected system information.

Table 12. Device overview pane (continued)

Field	Description
	- ⛔ **Unable to send system information**—SupportAssist Enterprise is unable to send the collected system information to the backend. - ⛔ **Clearing System Event Log failed**—SupportAssist Enterprise is unable to clear the System Event Log or Embedded System Management logs on the device. - ⛔ **Maintenance Mode**—SupportAssist Enterprise has placed the device in automatic maintenance mode because of an alert storm. No new support cases are created while the device is in maintenance. For more information, see Maintenance mode overview on page 109. - ⛔ **Credentials not provided**—The username and password of the device has not been provided. - ⛔ **Credentials not correct**—The username and password provided for the device is incorrect. ⓘ **NOTE:** The ⛔ error status may be displayed as a link that you can click to view a description of the issue and the possible resolution steps.
Operating System	Operating system installed on the device.
Software (for Chassis, networking, and other devices)	Firmware version installed on the device.
iSM (for iDRAC)	iSM version installed on the device.
OMSA (for servers)	OMSA version installed on the device.
Duplicate	Add a device that is of the same type as a device that you have already added.
Device Inventory Validation	The following are displayed: - Date and time the periodic inventory validation was last performed. - Type of the inventory validation. It also displays the status of the inventory validation tests. If the validation tests fail, then an error message is displayed.

The following table describes the fields displayed in the device overview pane for the following device types models:

- Data protection
- Data storage devices other than PeerStorage (PS) / Equallogic, Storage Center (SC) / Compellent, Fluid File System (Fluid FS), and PowerVault models
- Hyperconverged infrastructure appliances
- Converged infrastructure appliances other than Web Scale model

Table 13. Device overview pane

Field	Description
Hostname / IP address	IP address or host name of the device.
Serial	Serial number of the device.
Model	Model of the device, for example, PowerEdge M820.
Connectivity Monitoring	Connectivity status of the device.
Deployment Status	Status of the device after you add them in SupportAssist Enterprise. The following status may be displayed.

Table 13. Device overview pane (continued)

Field	Description
	● **Managed**—Device is successfully added and monitored by SupportAssist Enterprise. ● **Unmanaged**—Device is being added to SupportAssist Enterprise. ● **Pending Add**—Device is pending validation from the backend. The device is not monitored for hardware issues in this status. ● **Pending Delete**—Device is pending approval to delete from SupportAssist Enterprise. ● **UnRegistered**—Device addition to SupportAssist Enterprise is initiated. ● **Validation Error**—Error occurred while adding the device to SupportAssist Enterprise.
Set Device Status	Enables you to place the device in offline mode. For more information about offline mode, see Offline mode overview on page 111.
Rules to Dell EMC	Enables you to set permissions for transferring files between the device and the backend.
Validations Status	The following are displayed: ● Date and time the connectivity and monitoring tests were last performed. ● Status of the tests performed.

8

Device grouping

SupportAssist Enterprise has two predefined device groups—**Default** and **Staging**—that help you in managing the devices that you add. Depending on your requirement, you can also create custom device groups to manage certain devices as a group. For example, you can create device groups that may include devices based on the following:

- Device type (server, storage, or networking)
- The individual who manages the devices (Administrator group)
- Organization or business unit (Marketing, Operations, Finance, and so on)
- Physical location of the devices (shipping address)
- Alerting or notification (individuals who must be notified if an issue is detected on certain devices).

The device grouping capability is not available for the following devices or device models. These devices cannot be moved to a custom device group from the **Default** group.

- Data protection
- Converged infrastructure appliances other than Web scale model
- Hyperconverged infrastructure appliance
- Data storage devices other than the Peer Storage (PS) / EqualLogic, Storage Center (SC) / Compellent, Fluid File System (FluidFS), and PowerVault models

After you create a device group, you can:

- 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 or delete the device group.

ⓘ **NOTE:** Device grouping does not have an impact on the monitoring and automatic case creation capabilities of SupportAssist Enterprise.

ⓘ **NOTE:** The contact information and parts dispatch information that is configured for a device group override the default credentials, contact information, and parts dispatch information configured through the **Settings** pages. For example, if you have created a device group and configured the primary contact for the device group, all SupportAssist Enterprise notifications for issues with any device in the device group are sent to the primary contact assigned to that device group.

Topics:

Predefined device groups

The predefined device groups available in SupportAssist Enterprise are as follows:

- **Default** group — Contains devices that you have assigned to the **Default** group. By default, all devices that are discovered successfully are assigned to this group unless you assign the device to any other group.
- **Staging** group — Contains devices that were only discovered partially while you tried to add them because certain requirements were not met. Devices in this group will be automatically moved to the **Default** group when you revalidate them after the requirement is met. SupportAssist Enterprise capabilities are not available for devices that are present in this group. Typically, a device is added to the staging group in the following cases:
  - For servers, the iDRAC does not have the required license installed
  - For Compellent devices, SupportAssist is not enabled in the Dell Compellent Enterprise Manager application
  - Certain prerequisites for adding the device are not met

Create device group

About this task

After you add devices in SupportAssist, you can group devices into a separate group. You can provide contact information, preferred contact time and method, and also part dispatch information for the devices in the group.

ⓘ **NOTE:** The device group parts dispatch information overrides the default parts dispatch information that is provided in the **Contact Information** page. If resolving a problem requires replacing a part, the replacement part is shipped with your consent to the device group parts dispatch address, not the default parts dispatch address.

ⓘ **NOTE:** If the Technical Support agent determines that a part must be replaced in your system to resolve a support case, the replacement part is dispatched with your consent to the provided address.

Steps

1. Go to **Devices** > **Manage Device Groups**.
   The **Device Groups** page is displayed.
2. Click **Create Group**.
   The **Group and Contact Information** page in the **Create Device Group** window is displayed.
3. In the **Group Details** section, enter the name and a description for the group.
4. Select **Contact Information**.
   The contact information fields are enabled.
5. Perform the following steps:
   a. Select the contact type.
   b. Enter the first name, last name, phone number, alternate phone number, and email address.
   c. Select the preferred contact method, preferred contact hours, and time zone.

   ⓘ **NOTE:** To copy the contact information provided in the **Contact Information** page, select the contact type and click the link displayed below the **Contact Information** check box.
6. Click **Next**.
   The **Set Up Parts Dispatch Preferences (Optional)** page is displayed.
7. Select **Enter address for dispatch**.
   The fields in the primary and secondary shipping contact sections are enabled.
8. Select one of the following:
   - **Parts dispatch only**—If you want only the replacement hardware component to be dispatched to your address.
   - **Parts dispatch with onsite service**—If you want an onsite technician to replace the dispatched hardware component.
9. Enter the primary and secondary contact information.

   ⓘ **NOTE:** To copy the contact information provided in the **Group and Contact Information** page, click the link displayed above the **Primary Shipping Contact** section.
10. Select the preferred contact hours, country or territory, time zone, and enter the shipping information where a replacement component must be dispatched.
11. Enter any dispatch specific information in the **Dispatch Notes** box.
12. Click **Create**.
    The device group is created and displayed on the **Device Groups** page.

Manage devices in device group

Prerequisites

Ensure that you have already created a device group. See Create device group on page 55.

About this task

After you create a device group, you can add or remove devices in the group.

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

NOTE: You cannot move devices between existing groups.

Steps

1. Go to **Devices** > **Manage Device Groups**.
   The **Device Groups** page is displayed.
2. Select a device group.
3. From the **Select Group Actions** list, select **Manage Devices**.
   The **Manage Devices** window is displayed.
4. To add devices to the device group, select the devices in the **Ungrouped Devices** pane and click [>].
   The selected devices are moved to the **Devices in current group** pane.
5. To remove devices from the device group, select the devices in the **Devices in current group** pane, and click [<].
   The selected devices are moved to the **Default** group and displayed on the **Ungrouped Devices** pane.
6. Click **Save**.

   NOTE: Including or excluding one listing of a correlated device from a device group results in the automatic inclusion or exclusion of the other associated listing. For more information about device correlation, see Device correlation on page 121.

Edit device group

About this task

You can update the contact information, preferred contact method and time, and the parts dispatch information of a device group. Updating the contact information for a device group enables SupportAssist Enterprise to send notifications to the device group contact.

Steps

1. Go to **Devices** > **Manage Device Groups**.
   The **Device Groups** page is displayed.
2. Select a device group.
3. From the **Select Group Actions** list, select **Edit Group**.
   The **Group and Contact Information** page in the **Edit Device Group** window is displayed.
4. Update the required details in the **Group Details** section and primary and secondary contact information.
5. Click **Next**.
   The **Set Up Parts Dispatch Preferences (Optional)** page is displayed.
6. Update the required primary and secondary shipping contact information and shipping address details.
7. Click **Update**.
   The device group details are updated.

Delete device group

About this task

You can delete device groups based on your preference. Deleting a device group only removes the device group and contact information. When you delete a group, the devices are automatically moved to the **Default** group. You cannot delete the **Default** and **Staging** groups that are automatically created by SupportAssist.

Steps

1. Go to **Devices** > **Manage Device Groups**.
   The **Device Groups** page is displayed.
2. Select a device group, and then click **Delete**.
   A message is displayed to confirm if you want to delete the group.

3. Click **Yes**.
   The group is deleted and the devices in the group are moved to the **Default** group.

9

Managing device discovery rules

A device discovery rule enables you to discover and add devices that are present within one or more IP address ranges. Creating a device discovery rule helps you add multiple devices, and reduces the effort involved in adding each device individually.

Topics:

Create device discovery rule

About this task

By creating a discovery rule, you can discover and add devices based on IP address ranges or hostname. While you create the discovery rule, you can select a credential profile that must be applied to the devices. After creating the device discovery rule, you can run the rule immediately or based on a schedule to discover devices.

Steps

1. Go to **Devices** and click **Manage Rules for Device Discovery**.
   The **Manage Discovery Rules** page is displayed.
2. Click **Create Discovery Rule**.
   The **Create Device Discovery Rule** window is displayed.
3. Enter a name for the discovery rule.
4. From the **Credential profile** list, perform one of the following: See Create credential profile on page 63.
   - Select a credential profile that contains the account credentials for the device types that are present within the IP address ranges.
   - To create a new credential profile, select **Create New Profile** and click **Create**. See Create credential profile on page 63.
5. To discover devices by using IP address ranges, perform the following steps:
   a. Select **IP address / range**.
   b. Enter the IP address or IP address range of the devices that you want to discover.

      ⓘ **NOTE:** 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:** Ensure that the IP address ranges that you have entered do not overlap with each other.

      ⓘ **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.

   c. To add another IP address range, click **Add another range** and enter the IP address range of the devices.
   d. Enter the Subnet Mask of the IP address range.

      ⓘ **NOTE:** By default, the subnet mask value is 255.255.255.0.
6. To discover devices by using the hostname or IP addresses:

   a. Select **Devices**.
   b. Enter the hostname or IP address of 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

7. Select one of the following:
   - **Run now**—To discover the devices immediately.
   - **Run once**—To discover the devices at a specific date and time.
   - **Recur**—To schedule the discovery of devices at periodic intervals.
8. Click **Next**.
   The **Discovering Devices** window is displayed. Based on the device types included in the credential profile, the device types are selected automatically.
9. If required, clear the device types that you do not want to discover.
10. In the **Configuration Settings** section, clear the following options based on your preference:
    - **Perform deep discovery**—Discover a device and its associated device types. See Deep discovery on page 121.
    - **Enable Monitoring**—Enable SupportAssist Enterprise to detect hardware issues that may occur on the discovered devices.
    - **Configure SNMP to receive alerts from this device**—Automatically configure the SNMP settings of the discovered device to forward alerts (SNMP traps) to SupportAssist Enterprise.
    - **Install latest version of OMSA**—Enables SupportAssist Enterprise to install the latest version of OMSA or iDRAC Service Module (iSM) on the discovered servers. OMSA or iSM is required for collecting system information and to generate alerts from the devices.
11. Click **Add Rule**.
    The discovery rule is added and listed on the **Manage Discovery Rules** page. If you selected **Run now**, discovery of devices is initiated.

Edit device discovery rule

About this task

You can edit the discovery rule based on your requirement.

ⓘ **NOTE:** You cannot edit a discovery rule when the device discovery is in progress.

Steps

1. Go to **Devices** and click **Manage Rules for Device Discovery**.
   The **Manage Discovery Rules** page is displayed.
2. Select the discovery rule that you want to edit and click **Edit**.
   The **Edit Device Discovery Rule** window is displayed.
3. To discover devices by using IP address ranges, perform the following steps:
   a. Select **IP address / range**.
   b. Enter the IP address or IP address range of the devices that you want to discover.

      ⓘ **NOTE:** 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:** Ensure that the IP address ranges that you have entered do not overlap with each other.

      ⓘ **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.

   c. To add another IP address range, click **Add another range** and enter the IP address range of the devices.
   d. Enter the Subnet Mask of the IP address range.

ⓘ **NOTE:** By default, the subnet mask value is 255.255.255.0.

4. To discover devices by using the hostname or IP addresses:
    a. Select **Devices**.
    b. Enter the hostname or IP address of 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. Click **Next**.
   The **Discovering Devices** window is displayed.
6. Select or clear the devices types and the configuration settings.
7. Click **Edit Rule**.
   The discovery rule is updated.

Delete device discovery rule

Steps

1. Go to **Devices** and click **Manage Rules for Device Discovery**.
   The **Manage Discovery Rules** page is displayed.
2. Select the discovery rule that you want to delete and click **Delete**.
   The **Delete Device Discovery Rule** window is displayed.
3. Click **Yes**.
   The discovery rule is deleted.

Run device discovery rule

Prerequisites

Internet Control Message Protocol (ICMP) must be enabled on the device.

About this task

After you create a discovery rule, you can run the rule any time to discover the devices.

Steps

1. Go to **Devices** and click **Manage Rules for Device Discovery**.
   The **Manage Discovery Rules** page is displayed.
2. Select the discovery rule that you want to run and click **Run now**.
   The devices associated with the discovery rule are discovered immediately.

   ⓘ **NOTE:** Devices that were discovered by the discovery rule, but are later unreachable are moved to the **Inactive** status. If a device is in **Inactive** status even after the discovery rule is run for three consecutive times, the device is automatically deleted.

10

Managing device credentials

SupportAssist Enterprise requires the device credentials to add devices and to collect system information.

You can enter or assign credentials to a device by using one of the following methods:

- While adding a device
- By using the **Edit** option
- By assigning an Account Credentials or a Credential Profile

Topics:

Account Credentials

An Account Credential consists of the credentials of a specific device type. The Account Credentials are used by SupportAssist Enterprise to connect to a device and collect system information. Depending on the number of device types in your environment, you may have to create one or more Account Credentials.

Add account credentials

About this task

Account credentials are required to add a device or to create a credential profile that you can apply to devices. Depending on your requirement, you can create account credentials for each device type in your environment.

Steps

1. Go to **Devices** > **Manage Credentials** > **Account Credentials**.
   The **Manage Account Credentials** page is displayed.
2. Click **Add Credentials**.
   The **Add Account Credentials** window is displayed.
3. Enter a unique name for the account credentials.
4. From the **Device Type** list, select the type of device.
5. Enter the credentials of the selected device type:

   NOTE: The credentials that you enter must have administrator rights.

   - For **Server / Hypervisor** devices, from the **Operating System type** list, select the operating system, and then type the user name and password of the device in the appropriate fields.

     The user name and password you enter must have root or sudo user rights. If you provide the user name and password of a sudo user, ensure that the sudo user is configured for SupportAssist Enterprise. For information about configuring the sudo user, see Configure sudo access for SupportAssist Enterprise on server running Linux on page 124.
   - For **Chassis**, **Fluid File System (FluidFS)**, **iDRAC**, and **Storage Center (SC) / Compellent** devices, type the user name and password of the device in the appropriate fields.
   - For **Software**, from the **Software type** list, select the software type, and then type the user name and password in the appropriate fields.
   - For **Solution** devices, enter the SSH and REST credentials in the appropriate fields.
   - For **Networking** devices, type the user name, password, community string, and enable password of the device in the appropriate fields.

     NOTE: Community string is required for the following network devices:

     ○ PowerConnect family 28xx and X series

    - Cisco
    - Wireless controller

  ⓘ **NOTE:** Enable password is required only when the networking device is configured with an enable password.

- For **PeerStorage(PS) / EqualLogic** devices, type the user name, password, and community string of the device in the appropriate fields.

  ⓘ **NOTE:**
    - Account credentials are mandatory for adding a Storage ME4 Series device.
    - Account credentials are not required for adding a Storage MD Series device.

6. Click **Save**.
   The account credentials are listed on the **Manage Accounts Credentials** page.

Edit account credentials

Prerequisites

Internet Control Message Protocol (ICMP) must be enabled on the device.

About this task

Edit the account credentials based on your requirement. For example, you must edit the account credentials whenever there is a change in the credentials of the associated device type.

ⓘ **NOTE:** Changing the device type is not supported.

ⓘ **NOTE:** Editing the name of the account credentials is possible only if the account credentials are not assigned to any device.

Steps

1. Go to **Devices** > **Manage Credentials** > **Account Credentials**.
   The **Manage Account Credentials** page is displayed.
2. Select the account credentials that you want to edit and click **Edit**.
   The **Edit Account Credentials** window is displayed.
3. Update the credentials as required.
4. Click **Update**.
   The account credentials are updated. Devices to which the account credentials are assigned are re-validated.

Reassign account credentials

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select a device and click **Edit**.
   The **Edit Account** window is displayed.
3. From the **Account Credentials** list, select an account credential.

   ⓘ **NOTE:** Only the account credentials that you have already created for the selected device type are present in the **Account Credentials** list.

4. Perform one of the following:
   - If the device is in the **Default** group, click **Save**.
   - If the device is in the **Staging** group, click **Revalidate**.

Delete account credentials

Prerequisites

The account credentials that you want to delete must not be assigned to any device.

Steps

1. Go to **Devices** > **Manage Credentials** > **Account Credentials**.
   The **Manage Account Credentials** page is displayed.
2. Select the account credentials that you want to delete and click **Delete**.
   The **Delete Account Credentials** window is displayed.
3. Click **Yes**.

Credential Profiles

A Credential Profile is a collection of Account Credentials of various device types. Credential Profiles enable you to assign a set of credentials to your devices, instead of entering the credentials for each device manually.

Create credential profile

About this task

Creating a credential profile enables you to assign credentials to your devices.

Steps

1. Go to **Devices** > **Manage Credentials** > **Credentials Profiles**.
   The **Manage Credential Profiles** page is displayed.
2. Click **Create Profile**.
   The **Create Credential Profile** window is displayed.
3. In the **Name** box, type a unique name for the credential profile.
4. Select the device type you want to include in the profile.

   For **Server / Hypervisor**, **Software**, and **Solution**, click + to expand the list of device types.

   The **Account Credentials** list is enabled for selection.
5. From the **Account Credentials** list, select the account credentials that you want to assign to the device type.

   ⓘ **NOTE:** The account credentials list displays Not available if you have not created an account credentials for the device type. To create a new account credentials, click **Add Account Credentials**. For more information on creating account credentials, see Add account credentials on page 61.

6. Repeat step 4 and 5 for each device type that you want to include in the credential profile.
7. Click **Save**.
   The credential profile is listed on the **Manage Credential Profiles** page.

Edit credential profile

Prerequisites

Internet Control Message Protocol (ICMP) must be enabled on the device.

About this task

You can update the credentials of a profile based on your requirement. For example, you may edit the Credential Profile to add a new Account Credentials or change the Account Credentials for a device type.

ⓘ **NOTE:** Updating the name of the credential profile is not supported.

Steps

1. Go to **Devices** > **Manage Credentials** > **Credentials Profiles**.
   The **Manage Credential Profiles** page is displayed.
2. Select the credential profile that you want to edit and click **Edit**.
   The **Edit Credential Profile** window is displayed.
3. Select the device type for which you want to edit account credentials.
   The **Account Credentials** list is enabled for selection.
4. From the **Account Credentials** list, select the account credentials that you want to assign to the device type.
5. Click **Update**.
   The credential profile is updated. Devices to which the credential profile is assigned are re-validated.

Assign credential profile

Prerequisites

Internet Control Message Protocol (ICMP) must be enabled on the device.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select one or more devices and from the **Assign Credential Profile** list, select a credential profile.
   The credential profile is assigned to the selected devices. Devices to which the credential profile is assigned are re-validated.

View devices associated with a Credential Profile

Steps

1. Go to **Devices** > **Manage Credentials** > **Credentials Profiles**.
   The **Manage Credential Profiles** page is displayed.
2. Select a credential profile.
   Devices that are associated with the credential profile are displayed on the credential profile overview pane.

Approximate time required to assign Credential Profile

Assigning a Credential Profile may be prolonged depending upon the device types, number of devices, and your network bandwidth.

The following table provides the approximate time required to assign a Credential Profile depending upon the number of devices.

Table 14. Device count and Credential Profile assignment duration

Number of devices	Time taken to assign a Credential Profile
5	3 minutes
50	15 minutes
100	30 minutes
1000	6 hours
1500	9 hours
2000	12 hours
3000	17 hours

Delete credential profile

Prerequisites

The credential profile that you want to delete must not be assigned to any device.

Steps

1. Go to **Devices** > **Manage Credentials** > **Credentials Profiles**.
   The **Manage Credential Profiles** page is displayed.
2. Select the credential profile that you want to delete and click **Delete**.
   The **Delete Credential Profile** window is displayed.
3. Click **Yes**.

11

Validating device inventory

Site inventory validation verifies the availability of the following capabilities of SupportAssist Enterprise for your devices:

- **Connectivity Status**—Verifies if the device has Internet connectivity and if the required ports are open on the device. It also verifies if the required credentials of the device are correct and available.
- **Collection Capability Status**—Verifies if the requirements for collecting system information are met on the device.
- **Monitoring Status**—Verifies if the latest version of OMSA is installed on servers. It also verifies if the SNMP trap destination and the iDRAC trap destination are configured.

  NOTE: Monitoring capability test is supported only on Linux, and iDRAC.

During inventory validation, the device status is updated.

- If the validation is successful, the device moves to the Default group.
- If the validation is unsuccessful, the device moves to the Staging or Inactive group.

NOTE: While inventory validation is in progress, the device is disabled. To view the status of the device operation, move your mouse pointer on the device.

NOTE: The total count of devices in Site Inventory Validation table may not match the total number of devices on the progress indicator. The device count on the progress indicator is assigned when periodic inventory validation begins or when SupportAssist Enterprise is upgraded to a newer version, whereas the device count in the Site Inventory Validation table is updated when:

- Some associated devices are discovered as a part of the deep discovery process
- New devices are added in SupportAssist Enterprise

Log in to SupportAssist Enterprise as administrator and go to **Devices** > **Site Inventory Validation** to view the **Site Inventory Validation** page. Inventory validation capability is available only for the following devices:

- Server / Hypervisor
- iDRAC
- Chassis
- Fluid File System (Fluid FS)
- Networking
- Storage Center (SC) / Compellent
- PowerVault
- Software
- Web-Scale appliance

Topics:

Start inventory validation manually

Prerequisites

Internet Control Message Protocol (ICMP) must be enabled on the device.

About this task

You can perform inventory validation on your devices to verify the status of the devices. Inventory validation capability is available only for the following devices or device models:

- Server / Hypervisor

- iDRAC
- Chassis
- Data storage:
  - Fluid File System (Fluid FS)
  - Storage Center (SC) / Compellent
  - PowerVault
  - PeerStorage (PS) / Equallogic
- Networking
- Software
- Converged infrastructure:
  - Web Scale

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select one or more devices and click **Validate Inventory**.
   SupportAssist Enterprise verifies the connectivity status of the devices.

   > **NOTE:** To view the count of devices that were successfully validated and the devices that failed validation, see the **Site Inventory Validation** page.

Schedule automatic inventory validation

About this task

By default, inventory validation is scheduled on a randomly determined day of every month at 11 PM. If necessary, you can change the schedule based on your requirement.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In **Automatically start inventory validation** section, select a day on which you want to want to initiate inventory validation.
3. Click **Apply**.

Site Inventory Validation

The **Site Inventory Validation** page displays the following sections:

- Validation test status—Displays the type of tests that are performed during inventory validation.
- Progress indicator—Indicates the status of the inventory validation.
- History—Displays the inventory validation test history.

The following table provides information about the items that are displayed in the **Validation test** section on the **Site Inventory Validation** page:

Table 15. Validation test status

Field	Description
Validation test	Type of tests performed during inventory validation.
Success	✓ and the rollup count of number of devices that were validated successfully.
Failed	⛔ and the rollup count of number of devices that were not validated successfully.
Others	Displays a status icon and the rollup count of number of:

Table 15. Validation test status (continued)

Field	Description
	● Devices that may not be supported or monitored by SupportAssist Enterprise ● Devices added or discovered in SupportAssist Enterprise through the adapter ● Devices for which the connectivity test has failed ● Devices for which you have disabled monitoring

The following table provides information about the items displayed in the history section on the **Site Inventory Validation** page.

Table 16. History of inventory validation

Field	Description
Started	Date and time the periodic inventory validation was started.
Completed	Date and time the periodic inventory validation was completed.
Last Updated	Date and time the periodic inventory validation was last performed.

12

SupportAssist Enterprise cases

A support case is automatically created when an issue is detected on devices that are monitored by SupportAssist. All the cases created by SupportAssist are displayed on the **Cases** page.

> ⓘ **NOTE:** SupportAssist Enterprise does not create a support case for every alert that is received from a monitored device. A support case is created only if the alert type and number of alerts that are received from the device match with the criteria defined by Dell EMC for support case creation.

Support case information is automatically available, for supported devices that have valid Service Tags when SupportAssist Enterprise connects to the Dell support case and service contract databases over the Internet. Support case information is refreshed only in the following situations:

- You open the **Cases** page.
- You click ⟳ **Refresh** the **Cases** page.
- The **Cases** page is open and you refresh the web browser window.

You can also request Technical Support to perform the following activities by using the available case management options:

- Suspend activities related to a support case
- Resume activities related to a support case
- Close a support case

The case management options are applicable only for support cases that were opened automatically by SupportAssist Enterprise for the following devices:

- Server / Hypervisor
- iDRAC
- Chassis
- Networking
- Data storage:
  - PeerStorage (PS) / EqualLogic
  - PowerVault

After SupportAssist Enterprise has completed its open support cases update, the **Cases** page displays the current support cases. For information about the fields and details displayed on the **Cases** page, see Cases on page 71.

Topics:

View support cases for a specific device

About this task

View the open support cases for a specific device monitored by SupportAssist Enterprise.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the device for which you want to check for support cases.
   The device overview pane is displayed.

   > ⓘ **NOTE:** The device overview pane is displayed only if a single device is selected in the **Devices** page.

3. From the **Tasks** list, select **Check for cases**.
    - If support cases are present for the device, the **Cases** page is displayed. All the support cases for the device are displayed on the top of the **Cases** page.
    - If no support cases are present for the device, an appropriate message is displayed.
    - If SupportAssist Enterprise is unable to retrieve support case information, a message is displayed.

Request to suspend case activities for 24 hours

About this task

You can request Technical Support to stop activities that are related to a support case for 24 hours, if necessary. For example, you may want Technical Support to suspend activities for a support case in the following cases:

- If you want to resolve the issue without any assistance from Technical Support
- If you do not want to receive any notifications that are related to the support case from Dell EMC during a planned maintenance activity

ⓘ **NOTE:** You can request Technical Support to stop activities that are related to a support case only if the support case is opened by SupportAssist.

Steps

1. Go to **Cases** and click **View Cases**.
   The **Cases** page is displayed.
2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.
   The list of all cases that were opened by SupportAssist are displayed.
3. Select the support case that you want to suspend.

   ⓘ **NOTE:** The **Case Options** list is enabled only if the support case that you have selected was opened by SupportAssist.

   ⓘ **NOTE:** The **Suspend Activity 24 hours** option is disabled if you have already requested to suspend notifications for the selected support case.

4. From the **Case Options** list, select **Suspend Activity 24 hours**.
   The **Suspend case activities for 24 hours** window is displayed.
5. Optionally, enter your reason for requesting to suspend activities for the support case.
6. Click **OK**.
   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.
7. Click **OK**.
   The support case displays a **Suspended** status.

   ⓘ **NOTE:** If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a case, you can run the case creation test to verify connectivity to Dell, and then retry the operation.

Request to resume support activities

About this task

You can request Technical Support to resume activities for a support case, if you had previously requested to suspend activities for the support case.

Steps

1. Go to **Cases** and click **View Cases**.
   The **Cases** page is displayed.
2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.
   The list of all cases that were opened by SupportAssist Enterprise are displayed.
3. Select the support case for which you want to Technical Support to resume case activities.

   ⓘ **NOTE:** The **Case Options** list is enabled only if the support case that you have selected was opened by SupportAssist Enterprise.

NOTE: The **Resume Activity** option is enabled only if you had previously requested to suspend notifications for the selected support case.

4. From the **Case Options** list, select **Resume Activity**.
   The **Resume Activity** window is displayed.
5. Optionally, enter the reason for requesting to resume activities for the support case.
6. Click **OK**.
   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.
7. Click **OK**.
   The support case displays the appropriate status.

   NOTE: If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a case, you can run the cases creation test to verify connectivity to Dell EMC, and then retry.

Request to close a support case

About this task

If you have resolved a problem with a device, you can request Technical Support to close the corresponding support case.

NOTE: You can request Technical Support to close a support case only if the support case was opened by SupportAssist Enterprise.

NOTE: You can request Technical Support to close a support case that is in any status, except the **Closed** and **Closure Requested** status.

Steps

1. Go to **Cases** and click **View Cases**.
   The **Cases** page is displayed.
2. In the **Refine by** pane, from the **Source Type** list, select **SupportAssist**.
   The list of all cases that were opened by SupportAssist Enterprise are displayed.
3. Select the support case that you want to close.

   NOTE: The **Case Options** list is enabled only if the support case that you have selected was opened by SupportAssist Enterprise.

4. From the **Case Options** list, select **Request to Close**.
   The **Request to close the case** window is displayed.
5. Optionally, enter your reason for requesting to close the support case.
6. Click **OK**.
   The **Updating Case** message is displayed. After the case is updated successfully, the **Case Status** message is displayed.
7. Click **OK**.
   The support case displays a **Closure requested** status.

   NOTE: After you request to close a support case, Technical Support may contact you to get more details before closing the support case.

   NOTE: If SupportAssist Enterprise is unable to process your request, an appropriate error message is displayed. In such a case, you can run the cases creation test to verify connectivity to Dell EMC, and then retry.

Cases

The **Cases** page displays the support cases for your devices added in SupportAssist Enterprise. For devices with a ProSupport, ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service plan, the **Cases** page displays case status irrespective of the case creation method. By default, the displayed support cases 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 case information was last retrieved from the backend.

The following table describes the options and support case information displayed on the **Cases** page.

Table 17. Cases page

Column name	Description
Search by list	Search cases by a specific category of displayed data.
Search term	Enter the search keyword. ⓘ **NOTE:** You must enter a minimum of 3 characters to perform the search.
Case Options list	Manage support cases that were opened by SupportAssist Enterprise based on your requirement. The following are the available options: ● **Suspend Activity 24 hours**—Request technical support to suspend activities related to a support case for 24 hours. After 24 hours, technical support automatically resumes activities related to the support case. See Request to suspend case activities for 24 hours on page 70. ● **Resume Activity**—Request technical support to resume activities related to a support case. See Request to resume support activities on page 70. ⓘ **NOTE:** The **Resume Activity** option is enabled only if you had previously requested to suspend activities related to a support case. ● **Request to Close**—Request Technical Support to close a support case. See Request to close a support case on page 71. The list is enabled only for cases opened by SupportAssist Enterprise for the following devices or device models: ● Server or hypervisor ● iDRAC ● Chassis ● Networking ● PeerStorage (PS) / EqualLogic ● PowerVault
⟳ **Refresh**	Refresh the case list displayed.
Fetching Cases	A progress indicator that is displayed when SupportAssist Enterprise is verifying if cases are present for your devices.
TechDirect	Opens the **Dell EMC TechDirect** home page in a new web browser window.
Check box	Select a support case for performing case management actions. ⓘ **NOTE:** The check box is displayed only for cases that were automatically created by SupportAssist Enterprise.
Name / IP Address	The name, host name, or IP address depending on the information you have provided for the device. The device name is displayed as a link that you can click to open the **Devices** page.
Number	Numeric identifier assigned to the support case.
Status	Current state of the support case. The status of a support case may be: ● **Submitted**—SupportAssist Enterprise has submitted the support case. ● **Open**—Technical support has opened the submitted support case. ● **In Progress** or **Working**—Technical support is working on the support case. ● **Assigning**—The support case has still not been assigned to a technical support agent. ● **Customer Deferred**—Technical support has deferred the support case at the customer's request. ● **Reopened**—The support case was previously closed, and has been reopened. ● **Suspended**—Technical support has suspended activities related to the support case for 24 hours based on your request. ● **Closure Requested**—You have requested technical support to close the support case. ● **Closed**—The support case is closed. ● **Not Applicable**—An issue was detected by SupportAssist Enterprise, but a support case was not created because the device has either an expired warranty or Basic Hardware warranty. ● **Unavailable**—The support case status could not be retrieved from Dell. ● **Unknown**—SupportAssist Enterprise is unable to determine the status of the support case.
Title	The support case name, which identifies:

Table 17. Cases page (continued)

Column name	Description
	● Support case generation method ● Device model ● Device operating system ● Alert ID, if available ● Alert description, if available ● Warranty status ● Resolution description
Date Opened	The date and time the support case was opened.
Service Contract	The Dell EMC service contract level under which the device is covered. The **Service Contract** column may display: ● **Unknown**—SupportAssist Enterprise cannot determine the service contract. ● **Invalid Service Tag**—The Service Tag of the device is invalid. ● **No Service Contract**—This device is not covered under a Dell EMC service contract. ● **Expired Service Contract**—The service contract of the device has expired. ● **Basic Support**—The device is covered under a Dell EMC Basic Hardware service contract. ● **ProSupport**—The device is covered under a Dell EMC ProSupport service contract. ● **ProSupport Plus**—The device is covered under a Dell EMC ProSupport Plus service contract. ● **ProSupport Flex for Data Center**—The device is covered under a Dell EMC ProSupport Flex for Data Center service contract. ● **ProSupport One for Data Center Or ProSupport Flex for Data Center**—The device is covered under a Dell EMC ProSupport One for Data Center Or ProSupport Flex for Data Center service contract.
Service Tag/Serial Number	Unique, alphanumeric identifier that enables Dell EMC to recognize the device.

ⓘ **NOTE:** When you check for support cases of a specific device, the support cases of that device are displayed at the top of the **Cases** page with a blue border for the appropriate rows. See View support cases for a specific device on page 69.

The **Refine By** pane enables you to refine the list of the devices displayed. You can refine the list based on device type, case status, service contract, or source type.

13

Viewing collections

SupportAssist Enterprise collects system information from each device that you have added and sends the information securely to the backend. Typically, the system information is collected as follows:

- Periodically—At regular intervals, depending on the predefined collection start date specified in the **Preferences** page.
- On case creation—When a support case is created for an issue that has been identified by SupportAssist Enterprise.
- Manual (on demand)—If requested by Technical Support, you can initiate the collection of system information from one or more devices at any time.

ⓘ **NOTE:** By default, SupportAssist Enterprise collects system information periodically and on case creation only after the registration is completed. For more information about registration, see Register SupportAssist Enterprise on page 22.

You can also use SupportAssist Enterprise to collect and send system information from multiple devices to Dell EMC. For more information about collecting system information from multiple devices, see Manually collect system information from multiple devices on page 85.

You can manually upload a collection to the backend or SupportAssist can automatically initiate a collection for the following devices or device models:

- Server or Hypervisor
- iDRAC
- Chassis
- Networking
- Data storage:
  - PeerStorage (PS) or EqualLogic
  - PowerVault

For the following devices or device models, collections are directly sent to the backend from the device and the collection details are not displayed on the **Collections** page.

- Data protection
- Data storage devices other than PeerStorage (PS) / Equallogic, Storage Center (SC) / Compellent, Fluid File System (Fluid FS), and PowerVault models
- Hyperconverged infrastructure appliances
- Converged infrastructure appliances other than Web Scale model

The collected system information is saved on the server that hosts the application that runs the collection task. Collections tasks that are run by SupportAssist Enterprise are saved on the server where SupportAssist Enterprise is deployed. You can access collections that are run by SupportAssist Enterprise from the **Devices** or **Collections** page. The system information available in a collection is displayed in the **Configuration Viewer** that is available in SupportAssist Enterprise.

ⓘ **NOTE:** You can only view the last five system information collections through the **Configuration Viewer**. System information collections that are 30 days or older and collections that are older than the last five collections within the last 30 days are automatically purged. The purge collections task runs automatically every day at 10 p.m. (time as on the server where SupportAssist Enterprise is deployed).

ⓘ **NOTE:** The **Configuration Viewer** does not support viewing the system information collected from storage devices with Fluid File System (FluidFS).

ⓘ **NOTE:** For collections from devices that are running a non-English operating system, the **Configuration Viewer** may not display certain attributes.

ⓘ **NOTE:** **Collections** page displays only the system information collected during the last seven days. To view collections that are older than seven days, use the date filter to display the list of collections.

Topics:

- Items reported in periodic collections from servers
- Download and view multiple device collections

View collection from the Devices page

About this task

The device overview pane lists the collections that have been performed on a specific device. You can select any collection that you want to view from the collections list.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the device for which you want to view collections.
   The device overview pane is displayed.

   NOTE: The **Collections** field displays **No Collections** when no collections have been performed from the device.
3. From the **Collections** list, select a collection date and time.

   The **Collections** field displays **No Collections** if no collections was performed from the device.

   If the device is a server, the **Configuration Viewer** is displayed in a new web browser window. For all other device types and multiple device collections, you are prompted to save the collection as a ZIP file. To view the downloaded collection, extract the ZIP file and click the `index.html` file.

View collection from Collections page

About this task

The **Collections** page lists all the collections that have been performed successfully. You can select any collection that you want to view from the collections list.

Steps

1. Go to **Collections** > **View Collections**.
   The **Collections** page is displayed.
2. Select a collection that you want to view.
   The collection overview pane is displayed.
3. Click **View** (for server collections) or **Download** (for all other device types and multiple device collections).
   If the collection is from a server, the **Configuration Viewer** is displayed in a new web browser window. For collections from all other device types and multiple device collections, download and save the collection as a ZIP file. To view the downloaded collection, extract the ZIP file and click the `index.html` file.

Configuration Viewer

The **Configuration Viewer** enables you to view the system information collected by SupportAssist Enterprise from your devices. The **Configuration Viewer** displays information in a tabbed format. The collected system information is displayed in the **Configuration Viewer** under various categories and sub categories.

In addition, the **Configuration Viewer** displays a **Summary** category. You can select the **Summary** category to view the following:

- The system information collection settings in SupportAssist Enterprise at the time of the collection
- Summary of errors that were detected in the collected system information
- Brief information about the device

The **Configuration Viewer** comprises of the following:

- Top pane—Displays the various categories and sub categories of collection data in a menu format. You can move the mouse pointer over the menu to see subcategories. You can click **Expand All** or **Collapse All** to quickly expand or collapse all categories. In addition, the top pane also displays the **Contacts** tab and the **Section Status** tab.

  - **Contacts**—Displays case details, customer information that you have provided while registering SupportAssist Enterprise, collections details, and the application information. The **Contacts** tab is the default tab.
  - **Section Status**—Displays an overview of the section-level information of a collection. This tab displays the status and description of each section of the collection. The number of items that are displayed in **Section Status** is dependent on the configuration of the device. The **Section Status** section also displays the count and status of the collection. The available statuses are:
    - **Success**
    - **Failed**
    - **Warning**
- Bottom pane—Displays the collection details. The bottom pane also displays the information available for the category or subcategory that is selected in the top pane. To view more details of the collection, click one of the subcategories. When you click a category, the category is expanded, enabling you to view its sub categories. The bottom pane also includes a navigation trail, which you can click to navigate backwards on the current trail.

Depending on the device types from which the collection was performed, the multiple device configuration viewer displays tabs for each device type.

NOTE: 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 in the collected system information. The tokenized values are represented as TOKEN*n*—for example, TOKEN0, TOKEN1, or TOKEN2.

NOTE: For a list of items that may be reported in collections from a server, see Items reported in periodic collections from servers on page 76.

NOTE: The **Configuration Viewer** does not support viewing the system information collected from storage devices with Fluid File System (FluidFS).

Log types

You can use the configuration viewer to access two types of logs from the system information that is collected by SupportAssist Enterprise:

Structured logs

Contain application logs, Embedded Server Management (ESM) logs, smart logs, and event logs. When you click the **Structured Logs** category, the configuration viewer displays the list of available structured logs. You can click any of the listed structured logs to view the details of the log in a new web browser window.

Unstructured logs

Contain a snapshot of the system files such as the Remote Access Controller (RAC) logs and other logs. When you click the **Unstructured Logs** category, the configuration viewer displays the list of available unstructured logs.

NOTE: Unstructured logs cannot be viewed within the configuration viewer. You can only save the unstructured logs and view the log details using an appropriate application.

Items reported in periodic collections from servers

The items reported in the system information collected from servers vary depending on the following:

- **Device Type** used to add the device in SupportAssist Enterprise
- Type of collection (manual, periodic, or support case)

The following table provides a summary of the items reported in the collected system information for a periodic collection from servers.

NOTE: The system information in a collection that is performed for a support case creation and a manually-initiated collection is more detailed in comparison with the system information collected in a periodic collection. For the complete list of items that are collected by SupportAssist Enterprise, see the *SupportAssist Enterprise Version 4.0 Reportable Items* document available at https://www.dell.com/serviceabilitytools.

NOTE: The system information from periodic collections enables Dell EMC to provide you an insight into your company's as-maintained environment configuration with proactive firmware recommendations and other reports.

Table 18. Items reported in periodic collections from servers

Items reported	Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor		Device added in SupportAssist Enterprise 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	✓	✗	✓

Table 18. Items reported in periodic collections from servers (continued)

Items reported	Device added in SupportAssist Enterprise with Device Type as Server / Hypervisor		Device added in SupportAssist Enterprise with the Device Type as iDRAC
	OMSA is installed on the device	OMSA is not installed on the device	
Network	✓	✗	✓
IPv4 Address	✓	✗	✗
IPv6 Address	✓	✗	✗
Network Team Interface	✓	✗	✗
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 installed on the server.

Download and view multiple device collections

About this task

View the system information available in the multiple device collections that you have performed. To view a multiple device collection, you must download the multiple device collection and open the collection by using a web browser.

Steps

1. Go to **Collections** > **View Collections**.
   The **Collections** page is displayed.
2. Select a multiple device collection that you want to view.
   The collection overview pane is displayed.
3. Click **Download** and save the collection file.
4. Extract the files and open the `index.html` file.
   The multiple device configuration viewer opens in a new web browser window. You can view the system information that is collected from each device by accessing the device type menu.

Configuring collection settings

SupportAssist Enterprise automatically collects system information from all devices at periodic intervals. SupportAssist Enterprise also collects system information automatically from a device when a support case is created for an issue with the device. Depending on your preference, you can configure the following:

- Automatic collection of system information when a support case is created or updated. See Enable or disable automatic collection of system information on support case creation on page 81.
- Periodic collection of system information. See Enable or disable periodic collection of system information on page 81.
- Collection of identity information. See Enable or disable collection of identity information on page 81.
- Collection of software information and the system log. See Enable or disable collection of system information on page 82.
- Automatic upload of collections. See Enable or disable automatic upload of collections on page 82.

Topics:

Prerequisites for collecting system information

- The local system must have sufficient hard drive space to save the collected system information.
- The local system and remote devices must meet the network port requirements.
- If you have added a server using the operating system, IP address, or hostname (agent-based monitoring):
  - The server must preferably have Dell OpenManage Server Administrator (OMSA) installed.
  - If the server is running a Linux operating system:
    - The device credentials that you have entered in SupportAssist Enterprise must have administrator rights on the device.
    - No resource (network share, drive, or ISO image) must be mounted on the `/tmp` folder.
    - If OMSA is installed on the device, the latest version of OpenSSL must also be installed on the device. For more information about OpenSSL, see the resolution for *OpenSSL CCS injection vulnerability (CVE-2014-0224)* available in the support website of the operating system.

    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**, ensure that OS to iDRAC Pass-through is enabled. For steps to enable the enable OS to iDRAC Pass-through, see the *iDRAC User's Guide* available at www.dell.com/idracmanuals .
- If you have added a 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 system information to the backend.
- For collecting system information from ESX and ESXi only, ensure that SFCBD and CIMOM are enabled.

Enable or disable automatic collection of system information on support case creation

About this task

By default, SupportAssist Enterprise automatically collects system information from the device when a support case is created and sends the information securely to the backend. If required, you can enable or disable the automatic collection based on your preference.

> ⓘ **NOTE:** To receive the full benefits of the support, reporting, and maintenance offering of the ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract for a device, automatic collection of system information must be enabled.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In the **Collect system state information** section, select or clear **When a new support case is created**.

   > ⓘ **NOTE:** By default, this option is selected.

3. Click **Apply**.

Enable or disable periodic collection of system information

About this task

By default, SupportAssist Enterprise starts collecting system information from all monitored devices at periodic intervals and sends it to the backend. The collection start time is a user-defined day of every month at 11 PM. If required, you can enable or disable the periodic collection of system information from all monitored devices based on your preference.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In the **Collect system state information** section, select or clear **On day n of every month at 11 PM**.
3. Click **Apply**.

Enable or disable collection of identity information

About this task

By default, SupportAssist Enterprise collects identity information (PII) such as the complete configuration snapshot of systems, hosts, and network devices that can contain host identification and network configuration data. Usually, part or all this data is required to properly diagnose issues. If your company's security policy restricts sending identity data outside of the company network, you can disable SupportAssist Enterprise from collection such data.

The following identity information can be filtered when collecting the system information from a device:

- 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

ⓘ **NOTE:** When you disable collection of identification information, some of the data about your company network (including the system log) is not transmitted to the backend. This may impede technical support from resolving issues that may occur on your devices.

ⓘ **NOTE:** If your devices have an active ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract and you have disabled collection of identification information, you will not receive some reporting information about your devices.

ⓘ **NOTE:** If you have disabled the collection of identity information from the devices, the identity information such as hostname, IP address, and so on, are replaced by tokenized values. The tokenized values are represented as TOKEN *n* - for example, TOKEN0, TOKEN1, or TOKEN2.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. By default, the **Include identification information in data sent to Dell EMC** check box in the **Identification information settings** section is selected. Depending on your requirement, select or clear the check box.

   ⓘ **NOTE:** If you disable collection of identification information, the settings for collection of logs, diagnostic data, and support data are disabled automatically. Therefore, collections that are sent to the backend from your devices do not include certain categories of data.
3. Click **Apply**.

Enable or disable collection of system information

About this task

By default, the system information that is collected and sent to the backend by SupportAssist Enterprise includes software information and system logs. If required, you can configure SupportAssist Enterprise to exclude the collection of software information and system logs from all devices.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In the **Collection data settings** section, select or clear the available options for each device type.

   ⓘ **NOTE:** For information about the logs that are collected by SupportAssist Enterprise, see the *SupportAssist Enterprise Version 4.0 Reportable Items* document available at https://www.dell.com/serviceabilitytools.
3. Click **Apply**.

Enable or disable automatic upload of collections

About this task

By default, the system state information is collected from your devices by SupportAssist Enterprise and sent to Dell EMC. If required, you can disable the automatic upload of collections.

ⓘ **NOTE:** Auto upload setting is not applicable for multiple device collections.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In the **Upload** section, select or clear **System state information collected from devices to Dell EMC**.
3. Click **Apply**.

15

Using SupportAssist Enterprise to collect and send system information

SupportAssist Enterprise automates the collection of system information from your devices both periodically and on case creation. If required, you can also manually start the collection and upload of system information to Dell EMC at any time. You can choose to start the collection of system information from a single device or multiple devices.

ⓘ **NOTE:** For information on the devices from which SupportAssist Enterprise can collect and send system information to the backend, see the *SupportAssist Enterprise Version 4.0 Support Matrix* at https://www.dell.com/serviceabilitytools.

Topics:

Set up SupportAssist Enterprise to collect and send system information

About this task

Deploying and registering SupportAssist Enterprise enables you to use SupportAssist to collect and send system information from the local system. To collect and send system information from remote devices, you must add each remote device in SupportAssist Enterprise.

ⓘ **NOTE:** The following steps are only required if you have not deployed SupportAssist Enterprise. If you have already deployed SupportAssist, follow the instructions in Manually collect system information from specific device on page 85 to manually start the collection and upload of system information to the backend.

Steps

1. Deploy SupportAssist Enterprise.
2. Register SupportAssist Enterprise. See Register SupportAssist Enterprise on page 22.
   SupportAssist Enterprise is now ready to collect system information from the local system.
3. Add each remote device in SupportAssist Enterprise.

   ⓘ **NOTE:** System information that is collected from servers running OMSA contains more troubleshooting information that may not be available in the data that is collected from servers that are not running OMSA. Therefore, it is recommended that you install OMSA on the servers that you have added in SupportAssist Enterprise.

   SupportAssist Enterprise is now ready to collect system information from remote devices.

Manually collect system information from specific device

Prerequisites

Ensure that you have completed setting up SupportAssist Enterprise. See Set up SupportAssist Enterprise to collect and send system information on page 84.

About this task

When a support case is opened or updated for a device, SupportAssist Enterprise automatically collects and uploads the system information to the backend. If necessary, you can also manually start the collection of system information from a device.

You may manually start the collection:

- If an issue occurs during automatic collection and upload of system information
- If requested by technical support

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the device from which you want to collect system information.
   The **Start collection** link is enabled.
3. Click **Start collection**.
   The **Name/IP Address** column on the **Devices** page displays a progress bar and a message that indicates the status of the collection and upload of system information.

   NOTE: If you want to cancel the collection of system information, click ✖ that is displayed next to the progress bar.

   NOTE: Until the collection is complete, the check box that is used to select the device is disabled. Therefore, you cannot initiate any other tasks on the device until the collection is complete.

Manually collect system information from multiple devices

About this task

Create and upload a collection bundle that contains the collected system information from multiple devices.

NOTE: System information is not collected from devices in the **Staging** group.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the devices from which you want to collect system information.
   The **Start collection** link is disabled when you select more than one device.
3. From the **Collection purpose** list, select a reason for the collection.
   The **Start collection** link is enabled.
4. Click **Start collection**.
   The **Multiple device collection** window is displayed.
5. Optionally, enter a name for the collection bundle, support case number, and the email address of the technical support agent.
6. If you want SupportAssist Enterprise to upload the collection bundle to the backend, ensure that the **Upload collection** check box is selected.

   NOTE: If you clear the **Upload collection** check box, the collection bundle is saved, but not uploaded to the backend. You can upload the collection bundle later through the **Collections** page.

7. Click **OK**.
   The collection progress status is displayed in the **Multiple Device Collection** pane. If the collection is completed successfully, the **Collections** page displays the details of the collection. You can also download the multiple device collection from the **Collections** page. For information about viewing a multiple device collection, see Download and view multiple device collections on page 78.

   ⓘ **NOTE:** You cannot initiate any other task on the devices until the collection is complete.

Upload collection

About this task

Use the **Upload** option available in the **Collections** page to upload collections to the backend. You may choose to upload a collection in the following cases:

- Collection of system information was successful, but upload of the collection was unsuccessful.
- While starting a multiple device collection, you had chosen not to upload the multiple device collection to the backend. Such collections display a `Never Uploaded` status in the **Collections** page.
- You want to upload a collection to the backend once again.

Steps

1. Go to **Collections** > **View Collections**.
   The **Collections** page is displayed.
2. Select one or more collections that you want to upload and click **Upload**.

   ⓘ **NOTE:** The total size of the collections that you can upload is 5 GB.

   The **Upload status** column displays the status of the upload.

Upload collection from disconnected site

About this task

When Internet connectivity is available, SupportAssist Enterprise automatically collects and sends system information from your devices to the backend. If the server where SupportAssist Enterprise is deployed does not have Internet connectivity, you can manually upload collections.

Steps

1. Perform a collection from the device. See Manually collect system information from specific device on page 85.
2. If the collection was performed by SupportAssist Enterprise:
   - For data storage, networking, or multiple device collections—On the **Collections** page, select the collection, and in the collection overview pane, click **Download**.
   - For other device collections, go to `/var/lib/docker/volumes/saede_data/_data/reports` to access the collection .ZIP file.
3. Copy and paste the collection `.zip` file to another system that has Internet connectivity.
4. Go to https://techdirect.dell.com/fileUpload/
   The **Dell EMC Technical Support File Upload** page is displayed.
5. Enter the Service Tag of the device.
6. Enter your company name, contact name, service request number, email address, contact email, and address.

   ⓘ **NOTE:** If you do not have a Service Request number, contact technical support to open a service request.

7. Click **Choose File** and browse to select the collection `.zip` file.
8. Click **Submit**.

Multiple Device Collection window

The **Multiple Device Collection** window enables you to provide details about the multiple device collection that you want to initiate.

The following table describes the items displayed in the **Multiple Device Collection** window.

Table 19. Multiple Device Collection window

Field	Description
Collection Name (Optional)	Name that you want to assign to the collection.
Dell EMC Support Request/case number (Optional)	Case identifier that you want to associate with the collection.
Dell EMC Technician Email (Optional)	Email address or name of the technical support contact.
Project ID (Optional)	Project identification information.
Upload collection	● Select this option to upload the collection to the backend after the collection is completed. ● Clear this option to only save the collection on the local system.

Multiple Device Collection pane

The **Multiple Device Collection** pane is displayed on the **Devices** page while the collection from multiple devices is in progress.

The **Multiple Device Collection** pane displays the following:

- Progress bar that indicates the collection status
- Collections status message
- Number of completed collections and the total number of collections
- Name that is assigned to the collection

NOTE: After the collection is completed, the **Multiple Device Collection** pane closes automatically, and the collection details are displayed on the **Collections** page.

16

Extensions

Extensions enable you to inventory and add devices that you manage using a systems management console such as Dell EMC OpenManage Enterprise.

An adapter is an extension available in SupportAssist Enterprise. It acts as an interface between SupportAssist and the systems management console. It enables SupportAssist to inventory and retrieve alerts from supported devices that you manage by a systems management console, instead of adding each device individually. After inventorying and adding the devices, SupportAssist can monitor the devices for hardware issues and also collect and upload system information to the backend.

To inventory and add devices that are managed by a systems management console, perform the following:

1. Add account credentials for the devices that you want to add from the systems management console. See Add account credentials on page 61.
2. Create one or more credential profiles depending on the type of devices that you want to add. See Create credential profile on page 63.
3. Set up the adapter in SupportAssist Enterprise. See Set up adapter on page 88.

Topics:

Set up adapter

Prerequisites

- You must have administrator privileges on the system running OpenManage Enterprise.
- You must have created account credentials and a credential profile that contains the credentials of the devices that are inventoried by the adapter. See Add account credentials on page 61 and Create credential profile on page 63.

About this task

Setting up an adapter enables you to inventory devices that are managed by a system management console such as OpenManage Enterprise. During the setup, SupportAssist Enterprise sets up the adapter on the system running SupportAssist Enterprise and then inventories the devices.

You can only inventory and add the following devices through the adapter:

- iDRAC of yx2x to yx5x series of PowerEdge servers
- Servers running Linux, ESXi, and HyperV
- Chassis
- Storage SC Series devices (previously Compellent)
- Dell EMC Networking devices—OS9 and OS10

  NOTE: OS10 support is limited only to PowerEdge MX7000 switches.
- OEM devices
- IOM devices
- PowerVault devices

NOTE: One OpenManage Enterprise adapter can inventory and add devices from multiple OpenManage Enterprise instances.

Steps

1. Go to **Extensions** > **Manage Adapters**.

The **Manage Adapters** page is displayed.

2. Click **Set Up Adapter**.
   The **Set up adapter** window is displayed.
3. From the **Adapter type** list, select the required adapter type.
4. Perform the following:
   a. Enter the hostname or IP address of the server where the systems management console is installed.
   b. Optionally enter a name for the adapter.

      The name that you enter is used to represent the adapter in SupportAssist Enterprise. If you do not enter a name, the hostname or IP address that you have entered is used to represent the adapter.
   c. Enter the user name and password.

      NOTE: The password must not exceed 50 characters.
5. From the **Credential profile** list, select a profile with the account credentials for the device types to be inventoried by the adapter.
6. From the **Update device inventory** list, select the desired frequency for inventorying devices through the adapter.
7. Click **OK**.
   The **Adapter Details** overview pane is displayed and devices that are managed by OpenManage Enterprise are inventoried in SupportAssist Enterprise.

Next steps

If the credential profile that you selected contains the correct credentials for the inventoried devices, the devices are added to the **Default** group. Devices for which the credentials are either not correct or not available are moved to the **Staging** group.

NOTE: By default, monitoring is enabled for devices that are added successfully through the adapter.

NOTE: The automated support capabilities of SupportAssist Enterprise are not available for devices that are placed in the **Staging** group.

To add devices that are placed in the **Staging** group:

1. In the **Refine by** pane, expand **Groups** and select **Staging**. You can also select the adapter under **Devices Added** in the **Refine by** pane to view devices that are inventoried by an adapter. If necessary, use the **Search by** option to filter the displayed list of devices.
2. Perform one of the following:
   - Select the devices and assign a credential profile that contains the credentials of the selected devices.
   - Select a device and click **Edit** to assign a credential account.
3. Repeat step 2 until you have assigned the correct credential profile or account credentials to all devices.

NOTE: When the OpenManage Enterprise services are suspended and resumed, the OpenManage Enterprise adapter retrieves alerts that have occurred in the last 12 hours for devices that are added in SupportAssist Enterprise through the OpenManage Enterprise adapter.

NOTE: After synchronization of the OpenManage Enterprise adapter, some of the iDRACs may not be displayed in SupportAssist Enterprise. This may occur if the iDRAC version cannot be retrieved from OpenManage Enterprise.

Edit adapter

About this task

You can update the following details of an adapter:

- Credentials of the server where the adapter is set up
- Inventory frequency
- Display name

Steps

1. Go to **Extensions** > **Manage Adapters**.
   The **Manage Adapters** page is displayed.
2. Select the adapter that you want to edit and click **Edit**.

The **Edit Adapter** window is displayed.

3. Edit the required details and click **Update**.
   The details of the adapter are updated.

Delete adapter

About this task

Deleting an adapter results in the following:

- Removes the adapter from SupportAssist Enterprise user interface
- Removes the devices that are associated with the adapter
- Uninstalls the adapter application from the server where it was set up

  > ⓘ **NOTE:** The adapter is uninstalled from the server on which it was installed only after all the adapters are deleted in SupportAssist Enterprise.

Steps

1. Go to **Extensions** > **Manage Adapters**.
   The **Manage Adapters** page is displayed.
2. Select the adapter that you want to delete, and then click **Delete**.
   A message is displayed to confirm if you want to delete the adapter.
3. Click **Yes**.
   The adapter and the devices added in SupportAssist Enterprise through the adapter are deleted from SupportAssist Enterprise.

Synchronize adapter

About this task

The adapter automatically inventories devices from the system management console depending on the frequency selected while setting up the adapter. You can also manually initiate the inventory of devices at any time.

Steps

1. Go to **Extensions** > **Manage Adapters**.
   The **Manage Adapters** page is displayed.
2. Select an adapter.
   The adapter overview pane is displayed.
3. Click **Sync now**.

Adapters

Adapter is an application that acts as an interface between SupportAssist Enterprise and systems management consoles.

The following table describes the information that is displayed on the **Adapters** page:

Table 20. Adapters

Field	Description
➕ **Set Up Adapter**	Set up an adapter. See Set up adapter on page 88.
✎ **Edit**	Edit the details of an adapter. See Edit adapter on page 89.
🗑 **Delete**	Delete an adapter. See Delete adapter on page 90.

Table 20. Adapters (continued)

Field	Description
Name	Name that you have provided for the adapter and the hostname or IP address of the server where the adapter is set up.
Type	Adapter type.
Managed devices	Total number of devices that are added through the adapter.
Console Version	Version of the system management console.
Status	Status of the adapter. The status of an adapter may be: ● **Connected**—SupportAssist can connect successfully to the adapter. ● **Disconnected**—SupportAssist is unable to connect to the adapter. ● **Initial Synchronization**—Initial inventory of devices in progress. ● **Periodic Synchronization**—Automatic periodic inventory of devices is in progress. ● **Manual Synchronization**—Manually initiated inventory of devices is in progress. ● **Connection lost**—The server running SupportAssist is unable to connect to the server where the adapter is set up. ● **Copy in progress**—The adapter installer package is being copied to the system. ● **Installation in progress**—Installation of the adapter is in progress. ● **Validation in progress**—SupportAssist is verifying if the adapter meets the prerequisites for setting up the adapter. ● **Configuration in progress**—SupportAssist is configuring the settings of the adapter. ● **Starting service**—SupportAssist had installed the adapter and the adapter service is started. ● **Awaiting connection**—SupportAssist is waiting for the adapter service to start. ● **Connection in progress**—SupportAssist is trying to connect to the adapter. ● **Assigning Profile**—The credential profile is being applied to the inventoried devices. The total number of inventoried devices and the count of devices to which the profile is applied is also displayed.

17

Active sessions

When a technical support agent remotely accesses your device to run scripts or transfer files, the session information is displayed in SupportAssist Enterprise while it is in progress.

Topics:

Active remote sessions

The **Active remote sessions** tab displays information about troubleshooting or device-specific tasks that are being performed by a technical support agent.

Click ⟳ to update the details displayed on the page. Click ⚙ to select the columns you want to view.

The following table describes the information that is displayed in the **Active remote sessions** tab:

Table 21. Active remote sessions

Column	Description
Started at	Date and time the remote session was initiated.
Model	Model of the device.
Serial number	Serial number of the device.
Device IP	IP address of the device.
Application name	Remote application of the device.
Port	Port through which the device is being accessed.
User	Name of the user who initiated the session.
Duration (mins)	Duration of the session displayed in minutes.

Active file transfer sessions

The **Active file transfer sessions** tab displays information about the files that are being manually or automatically transferred to the backend from a device or from the SupportAssist Enterprise user interface. After the file transfer is complete, the details are displayed on the **Audit** > **File Transfer** page.

Click ⟳ to update the details displayed on the page. Click ⚙ to select the columns you want to view.

The following table describes the information that is displayed in the **Active file transfer sessions** tab:

Table 22. Active file transfer sessions

Column	Description
Started at	Date and time the remote session was initiated.
Model	Model of the device.
Serial number	Serial number of the device.

Table 22. Active file transfer sessions (continued)

Column	Description
File name	Name of the file being transferred.
File size (kb)	Size of the file being transferred.
Transfer type	Channel through which file transfer is being initiated.
Transfer rate (MiBs)	Rate at which the file is being transferred.
Remaining time	Time remaining to complete the file transfer.
Percentage complete	Progress of file transfer.

Active remote scripts

The **Active remote scripts** tab displays information about the files being transferred between a device and the backend using the Managed File Transfer (MFT) service remote scripting capability. After the file transfer is complete, the details are displayed on the **Audit** > **Remote Script** page.

Click ⟳ to update the details displayed on the page. Click ⚙ to select the columns you want to view.

The following table describes the information that is displayed in the **Active remote scripts** tab:

Table 23. Active remote scripts

Column	Description
Model	Model of the device.
Serial number	Serial number of the device.
Script name	Type of the script being used, for example, PUT.
Remote script status	Status of the script.
Start time	Date and time the script was initiated.
End time	Date and time the script was completed.

Active connect homes

The **Active connect homes** tab displays the details of the files being transferred between a device and the backend using the Connect Home service. The page also displays the total number of files being transferred and the maximum duration that is taken to transfer a file in minutes.

After the file transfer is complete, the details of the transfer are displayed on the **Audit** > **Connect Home** page.

Click ⟳ to update the details displayed on the page. Click ⚙ to select the columns you want to view.

The following table describes the information that is displayed in the **Active connect homes** tab:

Table 24. Active connect homes

Column	Description
Started at	Date and time the file transfer was initiated.
File name	Name of the file transferred.
File size (kb)	Size of the file transferred.
Age (mins)	Time taken to transfer the file.

18

Configuring SupportAssist Enterprise settings

The **Settings** tab enables you to configure the following:

- Collection of system information
- Email notifications
- Internet connection settings for the servers on which SupportAssist Enterprise is deployed
- Internet connection settings for the servers on which Policy Manager is installed
- SMTP server
- Connect Home
- Contact and shipping information
- TechDirect integration
- VMware tools

Topics:

Configure proxy server settings

If the server on which SupportAssist Enterprise is deployed connects to the Internet through a proxy server, you must configure the proxy settings in SupportAssist Enterprise.

Steps

1. Go to **Settings** > **Proxy Settings**.
   The **Proxy Settings** page is displayed.
2. Select **Use proxy server**.

   NOTE: SupportAssist Enterprise supports Windows NT LAN Manager (NTLM) and basic proxy authentication protocols.

   The proxy server fields are enabled.
3. Enter the hostname or IP address and port number of the proxy server.
4. If a user name and password are required to connect to the proxy server, select **Requires authentication**.

   NOTE: If you do not provide the user name and password, SupportAssist Enterprise connects to the proxy server as an anonymous user.

   The user name and password fields are enabled.
5. Enter the username and password.
6. Click **Test**.
   SupportAssist Enterprise verifies the connection to the proxy server and displays a message indicating the connectivity status.
7. Click **Apply**.
   The proxy settings are saved.

ⓘ **NOTE:** The proxy settings are saved only if SupportAssist Enterprise can connect to the proxy server.

Policy Manager

Policy Manager is an application that enables you to set permissions for the following devices:

- Data protection
- Converged infrastructure appliances other than Web scale model
- Hyperconverged infrastructure appliances
- Data storage devices other than the Peer Storage (PS) or EqualLogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models

Policy Manager is not installed on the same server on which SupportAssist Enterprise is deployed and can be configured 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

For more information about the operations and configuration of policy manager, see the *Secure Remote Services Policy Manager Operations Guide* available at https://support.emc.com/products/37716_EMC-Secure-Remote-Services-Virtual-Edition/Documentation/.

Configure Policy Manager settings

About this task

Provide the Internet connection details to allow SupportAssist Enterprise to connect to the server on which policy manager is installed.

Steps

1. Go to **Settings** > **Policy Manager**.
   The **Policy Manager** page is displayed.
2. In the **Connection** section, select **Enable remote policy manager**.
3. Enter the hostname or IP address and port number.

   ⓘ **NOTE:** If the port is secured by SSL, the port number must be 8443. If the port is not secured by SSL, the port number must be 8090.

4. If the server on which Policy Manager is installed is secured by SSL, select **Enable SSL**.
5. From the **Strength** list, select the strength of the encryption.
6. If the server on which Policy Manager is installed connects to the Internet through a proxy server, perform the following:
   a. In the **Customer Proxy Server** section, select **Enable Proxy Server for Policy Manager only**.
      The proxy details fields are enabled.
   b. Enter the hostname or IP address and port number.
   c. If the proxy server requires authentication, select **Proxy requires authentication**.
      The username and password fields are enabled.
   d. Enter the username and password for the proxy server.
7. Click **Test**.
   SupportAssist Enterprise verifies the connection to the proxy server and displays a message indicating the connectivity status.
8. Click **Apply**.
   The settings are saved.

   ⓘ **NOTE:** The proxy settings are saved only if SupportAssist Enterprise can connect to the proxy server.

Preferences

The **Preferences** page enables you to configure collection settings and email notification settings.

The following table describes information about the options that are displayed in the **SupportAssist Enterprise Application** pane:

Table 25. SupportAssist Enterprise Application pane

Section	Description
Collect system state information	● Select a day of a month when SupportAssist Enterprise can automatically collect system information at 11 p.m. from all the devices. ● Select **When a new support case is created** to enable SupportAssist Enterprise to automatically collect system information when a support case is created.
Upload	Select **System state information collected from devices to Dell EMC** to enable SupportAssist Enterprise to automatically upload collections to the backend.
Validate	Select a date to automatically get the validation information from each device type every month at 11 PM.
API interface	Select **Enable API Interfaces for SupportAssist Enterprise** to enable API interfaces for SupportAssist Enterprise.
Identification information settings	Select **Include identification information in data sent to Dell EMC** to enable SupportAssist Enterprise to send the system identification information along with other data to the backend. If you clear this check box, collection of logs and diagnostic data are automatically disabled.
Email settings	Select **Receive email notification when a new support case is opened** to receive an email notification when a new support case is opened for a device.
Preferred email language list	Select the preferred language for email notifications.
Email notifications	Select the notifications that you want to receive through email: ● **Adapter connectivity status** ● **Connection test** ● **Maintenance mode** ● **Device validation status** ● **Periodic inventory validation** ● **Staging and inactive devices** ● **Auto dispatch preferences**

The following table provides information about the options that are displayed in the **Device and Network** pane:

Table 26. Device and Network pane

Field	Description
Server/Hypervisor	● Select **Software** to collect software-related information from the device. ● Select **System logs** to collect logs from the device. ● Select **SMART Logs** to collect smart CTL logs from the device. ⓘ **NOTE:** For information about the logs that are collected by SupportAssist Enterprise, see the *SupportAssist Enterprise Version 4.0 Reportable Items* document at https://www.dell.com/serviceabilitytools.
Data storage: Fluid File System (FluidFS)	Select **Logs** to collect logs from the device.

Table 26. Device and Network pane (continued)

Field	Description
Data storage: Peer Storage (PS)/ EqualLogic	● Select **Diagnostic data (Diags collection)** to collect diagnostic information from the device. ● Select **Inter array connectivity test (Ping Test)** to collect the ping test result from the device.
Data storage: PowerVault	Select **Support data** to collect support data from the device.
Software: HIT Kit/VSM for VMware	Select **Advanced logs** to collect logs from the device.
Solution: Nutanix	Select **Logs** to collect logs from the device.
Virtual machine	Select **System logs** to collect logs from the device.

Configure email notification settings

About this task

Enable or disable automatic email notifications from SupportAssist Enterprise and also select the preferred language for email notifications.

Steps

1. Go to **Settings** > **Preferences**.
   The **Preferences** page is displayed.
2. In the **Email settings** section, perform the following: .
   a. Select the events for which you want to receive an email notification.

      NOTE: Disabling email notifications for support cases disables emails that are sent while a collection is in progress and when the collection is sent to the backend.

   b. From the **Preferred email language** list, select a language in which you want to receive email notifications.

      NOTE: The list is enabled only when you select **Receive email notification when a new support case is opened**.
3. Click **Apply**.

Types of email notifications

The following table provides a summary of the different types of email notifications that are sent by SupportAssist Enterprise:

Table 27. Types of email notifications

Type of email notification	When the email notification is sent	Origin of the email notification
Registration confirmation and welcome email	Registration of SupportAssist Enterprise is completed successfully.	SupportAssist server hosted by Dell EMC
Case created	A hardware issue is detected and a support case is created for the issue.	SupportAssist server hosted by Dell EMC
Unable to create a case	A hardware issue is detected, but a support case could not be created because of technical difficulties.	SupportAssist server hosted by Dell EMC
Unable to collect system information	A support case is created automatically for a device, but SupportAssist Enterprise is unable to collect system information from the device.	SupportAssist server hosted by Dell EMC
Unable to send the collected system information	A support case is created automatically for a device, but SupportAssist Enterprise is unable to send the	SupportAssist server hosted by Dell EMC

Table 27. Types of email notifications (continued)

Type of email notification	When the email notification is sent	Origin of the email notification
	collected system information from the device to the backend.	
Inactive notification	SupportAssist Enterprise is not monitoring any device and no device has been added in the past 30 days.	SupportAssist server hosted by Dell EMC
Connectivity test alert	At 11 p.m. each day (date and time as on the server where SupportAssist Enterprise is deployed). ⓘ **NOTE:** The connectivity test alert notification is sent only if an issue is detected with connectivity to dependent resources.	SupportAssist Enterprise application
Automatic maintenance mode	An alert storm that is received from a device has resulted in SupportAssist Enterprise placing the device automatically in maintenance mode.	SupportAssist Enterprise application
Device status alert	At 11 p.m. each day (date and time as on the server where SupportAssist Enterprise is deployed). If less than 10 devices have issues, the email includes details about the issues and the possible resolution steps. If more than 10 devices have issues, the email only includes a summary of the issues. ⓘ **NOTE:** The device alert notification is sent only if an issue exists (warning or error status) with the setup or configuration of the devices.	SupportAssist Enterprise application
Issue with the adapter	● Within five minutes after an adapter connectivity issue is detected. ● If the issue is not resolved, another email notification is sent six hours after the first email was sent.	SupportAssist Enterprise application
Resumed normal operations with the adapter	If the issue is resolved within six hours, after the issue was detected.	SupportAssist Enterprise application
Final message regarding unresolved issue with the adapter	If the issue is not resolved within six hours, after the issue was detected.	SupportAssist Enterprise application
Inventory validation summary	SupportAssist Enterprise has completed validating your device inventory for its automated support capabilities-support case/incident creation and collection of system information.	SupportAssist Enterprise application
Alert from devices in **Staging** and **Inactive** groups	SupportAssist Enterprise has detected that the monitoring and automatic support request/incident creation capabilities are limited for some of your devices.	SupportAssist Enterprise application
Parts dispatch address validation	SupportAssist Enterprise has detected a hardware issue on one of your devices and a part replacement is required to resolve the issue.	SupportAssist Enterprise application

Table 27. Types of email notifications (continued)

Type of email notification	When the email notification is sent	Origin of the email notification
Parts dispatch address confirmation	Replacement part is ready to be dispatched.	SupportAssist Enterprise application
Administrator account status	Administrator account is locked after five failed attempts. An email notification is also sent when the account is unlocked.	Customer defined SMTP server
Update available	Updates are available for docker, operating system, or application configuration files.	Customer defined SMTP server
Remote session status	Technical support has initiated or ended a remote session on a device.	Customer defined SMTP server
Policy Manager status	SupportAssist Enterprise is unable to connect to the server on which Policy manager is installed.	Customer defined SMTP server
File transfer status	SupportAssist Enterprise is unable to send the file to the backend.	Customer defined SMTP server
File transfer status notification	SupportAssist Enterprise successfully sent the alert or collection file to the backend.	Customer defined SMTP server
Connect Home failover options test status	SupportAssist Enterprise successfully transferred a file to the backend while testing the Connect Home failover methods configured on the **Connect Home Configuration (Outgoing)** page.	Customer defined SMTP server
SMTP configurations test	SupportAssist Enterprise successfully connected to the SMTP server while testing the connectivity from the **SMTP settings** page	Customer defined SMTP server
SMTP configurations saved	SupportAssist Enterprise successfully saved the settings that are configured on the **SMTP settings** page.	Customer defined SMTP server
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.	Customer defined SMTP server

Enable or disable API interface settings

About this task

Enabling REST API interfaces enables you to integrate SupportAssist Enterprise with your data center tools and applications. For more information, see the *SupportAssist Enterprise Version 4.0 REST API Guide* available at https://www.dell.com/serviceabilitytools.

NOTE: You can perform a maximum of 10 operations such as adding devices and collecting system information, 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** > **Preferences**.
   The **Preferences** page is displayed.

2. In the **API interface** section, depending on your requirement, select, or clear **Enable API interfaces for SupportAssist**.
3. Click **Apply**.

Contact Details

The **Contact Details** page enables you to view and edit the primary and secondary contact information. You can also enable or disable automated parts dispatches of replacement parts..

To configure your contact details, see Configure contact information on page 100.

To configure your parts dispatch preferences, see Configure automated parts dispatch preferences on page 100.

Configure contact information

Enter or update your primary and secondary contact information after you register SupportAssist Enterprise. If the primary contact is unavailable, Dell EMC contacts your company through the secondary contact. If both the primary and secondary contacts are configured with valid email addresses, both receive SupportAssist Enterprise emails.

Steps

1. Go to **Settings** > **Contact Details**.
2. In the left pane, perform the following:
   a. Select the contact type.
   b. Enter the first name, last name, phone number, alternate phone number, and email address.
   c. Select the preferred contact method, contact hours, and time zone.
3. Click **Apply**.

Configure automated parts dispatch preferences

About this task

Entering your dispatch preferences and shipping information enables Dell EMC to dispatch a replacement part for your server. If you enter your preferences and shipping information during the registration, the information is automatically displayed on the **Contact Details** page. You can edit the information, if required.

ⓘ **NOTE:** Parts dispatch is available only for servers that have an active ProSupport, ProSupport Plus, ProSupport One, or ProSupport Flex service entitlement.

ⓘ **NOTE:** If a device is moved to a different location, ensure that the dispatch preferences and shipping information are updated.

By default, Dell EMC automatically ships the replacement parts. However, if you do not want to automatically receive the replacement parts, clear the **I want my replacement parts shipped automatically** check box.

Steps

1. Go to **Settings** > **Contact Details**.
2. In the **Primary shipping contact** section in the right pane, perform the following:
   a. Enter first name, last name, phone number, email address, and select the time zone.

      ⓘ **NOTE:** To copy the details from the left pane, click the link that is displayed.

   b. Select the preferred shipping contact hours and country or territory.
   c. Enter the shipping details.
   d. In the **Dispatch notes** section, enter dispatch specific related information.
3. In the **Secondary shipping contact** section, enter the first name, last name, phone number, and email address.

   ⓘ **NOTE:** To copy the details from the left pane, click the link that is displayed.

ⓘ **NOTE:** Contact details of the primary and secondary contact must be unique.

4. Click **Apply**.

Sign in to TechDirect from SupportAssist Enterprise

Steps

1. Go to **Settings** > **TechDirect login**.
   The **TechDirect Integration** page is displayed.
2. Click **Sign In**.
   The **Dell Account Sign In** window is displayed.
3. Enter the email address and password and click **Sign In**.
   The OTP is displayed.

   ⓘ **NOTE:** If you had already signed in to any Dell EMC portal on the web browser, the OTP for the signed in account is displayed. To continue signing in to the same account, enter the OTP and click **Submit**. If you want to use a different account to sign in, then sign out from the Dell EMC portal and then try again.
4. Enter the OTP and click **Apply**.
   The TechDirect account is verified and a message is displayed on the page.

Configure SMTP server settings

About this task

If your company utilizes an SMTP server (Email server), it is recommended that you configure the SMTP server settings. Configuring the SMTP server settings enables SupportAssist Enterprise to send email notifications.

ⓘ **NOTE:** Transport Layer Security (TLS) version 1.0 must be enabled on the SMTP server.

ⓘ **NOTE:** Configuring the SMTP server settings is optional.

Steps

1. Go to **Settings** > **SMTP Settings**.
   The **SMTP Settings** page is displayed.
2. Optionally, select **Enable on success notification** to receive an email when an alert file is sent to the backend.
3. Optionally, select **Enable device Connection notification** to receive an email when a technical support agent connects to a device.
4. Enter the hostname or IP address and port number of the SMTP server.
5. If the SMTP server requires authentication for sending emails, select **Requires authentication**.
6. Enter the username and password.
7. Click **Test**.
   SupportAssist Enterprise verifies the connection to the SMTP server and displays a message indicating the connectivity status.
8. Click **Apply**.

Connect Home overview

When an alert is generated, the alert file is sent to SupportAssist Enterprise through the Connect Home service. The file is received by one of the following listener services:

- HTTPS
- FTP
- Email (SMTP)

The alert file is then compressed and sent to the backend using one of the following methods:

- Managed File Transfer (MFT)—By default, alert files are sent to the backend through MFT.
- ESRS—If file transfer is unsuccessful through MFT, the files are sent through ESRS.
- FTPS or Email—If both MFT and ESRS are unavailable, the files are uploaded to the backend through FTPS or email. The files are uploaded through FTPS or email only if they are enabled for the Connect Home service.

You can configure the following for the Connect Home service:

- Failover methods. See Configure Connect Home failover methods on page 102.
- Email notifications. See Configure Connect Home email notifications on page 102.
- Listener services. See Configure Connect Home listener services on page 102.
- Permissions. See Configure Connect Home permissions on page 103.

Configure Connect Home failover methods

About this task

Enable and test the Connect Home failover methods.

ⓘ **NOTE:** By default, the **Enable File Transfer** and **Enable Failover ESRS** methods are enabled. You cannot disable these methods.

Steps

1. Go to **Settings** > **Connect Home**.
   The **Connect Home Configuration (Outgoing)** page is displayed.
2. Click the **Configuration** tab.
3. Select the failover method.

   ⓘ **NOTE:** SMTP settings must be configured to enable the email failover method.

4. Click **Test** to verify the failover method.
5. Click **Apply**.

Configure Connect Home email notifications

About this task

Configure Connect Home email notification settings to receive an email when an alert file is sent to the backend from a REST enabled device. You can also choose to receive the alert data along with the email. The notification is sent to your primary and secondary contact email address.

Steps

1. Go to **Settings** > **Connect Home**.
   The **Connect Home Configuration (Outgoing)** page is displayed.
2. Click the **Advanced Settings** tab.
3. In the **Connect Home Notification Configuration** section, perform the following:
   a. From the **Device Model** list, select the required device model.

      ⓘ **NOTE:** If you select **Default**, the settings are applied for all device models.

   b. Select **Enable on Success Notification** to receive an email when an alert file is sent to the backend.
   c. Select **Include Call Home Data** to receive the alert data as attachment to the email.
4. Click **Apply**.

Configure Connect Home listener services

About this task

When an alert is generated, SupportAssist Enterprise receives the alert details through one of the following listener services:

- HTTPS

- FTP
- Email

By default, all the services are enabled. You can disable the services depending on your requirement.

ⓘ **NOTE:** Before you disable a service, ensure that none of your devices are using that service.

Steps

1. Go to **Settings** > **Connect Home**.
   The **Connect Home Configuration (Outgoing)** page is displayed.
2. Click the **Advanced Settings** tab.
3. In the **Connect Home Listener Configuration** section, clear the service that you want to disable.
   A message is displayed to confirm if you want to disable the service.
4. Click **OK**.
   The **Advanced Settings** tab is displayed.
5. Click **Apply**.

Configure Connect Home permissions

About this task

Connect Home service must be enabled to send files between the devices, SupportAssist Enterprise and the backend. However, you can disable the service depending on your requirements.

Steps

1. Go to **Settings** > **Connect Home**.
   The **Connect Home Configuration (Outgoing)** page is displayed.
2. Click the **Advanced Settings** tab.
3. In the **Connect Home Permission Configuration** section, select **Disable Connect Home**.
   A message is displayed to confirm if you want to disable Connect Home.
4. Click **OK**.
   The **Advanced Settings** tab is displayed.
5. Click **Apply**.

VMware tools

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's 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 eliminates or improves the following issues:

- Low video resolution
- Inadequate color depth
- Incorrect display of network speed
- Restricted movement of the mouse
- Inability to copy and paste and drag-and-drop files
- Missing sound

It also provides the ability to take quiesced snapshots of the guest operating system and synchronizes the time in the guest operating system with the time on the host.

Configure VMware tools

About this task

Enable or disable VMware tools on the virtual machine. For information about VMware tools, see VMware tools on page 103.

ⓘ **NOTE:** VMware tools can be enabled or disabled only if you have deployed SupportAssist Enterprise on a VMware ESXi hypervisor.

Steps

1. Go to **Settings** > **VMware Tools**.
   The **VMware Tools Configuration** page is displayed.
2. Select **Enable** or **Disable** depending on your requirement.
3. Click **Apply**.

19

Audit overview

SupportAssist Enterprise records and saves all the events and activities performed using SupportAssist for your reference. The records are classified as **Activity**, **Connect Home**, **File Transfer**, **File Transfer Permission**, and **Remote Script** audits.

Topics:

Activity

The **Activity** page displays details of the REST API calls invoked by SupportAssist Enterprise, for example, user authentication, file upload, retrieve device serial number, and so on.

From the **Refine By** pane, you can search for logs by a specific date range, activity type, user, source, description, or status. When you click a log, the **Additional details** pane is displayed with the following details:

- **Time stamp**
- **Type**
- **Url**
- **Method**

Click ↗ to save the data displayed on the page in a CSV file. Click ⟳ to refresh the data displayed on the page.

The following table describes the information that is displayed on the **Activity** page:

Table 28. Activity

Column	Description
Date	Data and time when the activity was performed.
Activity type	Type of activity performed, for example, **esrsauth**.
User	Name of the user account used to invoke the API call.
Source	IP address of the system from which the activity was performed.
Description	Details about the API call invoked, for example, Get Policy Mgr Details.
Status	Status of the activity.

Connect home audit

When an alert is generated by a device, an alert file is generated and sent to the backend through the Connect Home service to format the files and request a transfer to the backend. Later, the file is sent to the backend through one of the following transport types:

- Managed File Transfer (MFT)—This is the default and primary channel for uploading files to the backend.
- ESRS—If MFT is unable to send a file, Connect Home automatically uploads the files to the backend through the ESRS channel.
- FTPS or Email—If both MFT and ESRS are unavailable, the files are uploaded to the backend through FTPS or email. The files are uploaded through FTPS or email only if they are enabled for the Connect Home service. See Configure Connect Home failover methods on page 102.

The **Connect home audit** page displays the details of files that are transferred through the Connect Home service to the backend.

From the **Refine by** pane, you can search for the logs by a specific date range, file name, transport type, notification type, or result. Click a log to view additional details such as date, model, and serial number.

Click ⇪ to save the data displayed on the page in a CSV file. Click ↻ to refresh the data displayed on the page.

The following table describes the information that is displayed on the **Connect home audit** page:

Table 29. Connect home audit

Column	Description
Date	Date and time the file was transferred.
File name	Name of the file that was transferred.
Transport type	Transport type used for file transfer.
Notification type	Method used for file transfer, for example, primary or failover
Result	Status of file transfer, for example, **Success**.
Success	● If file was transferred to the backend, **1** is displayed. ● If file was not transferred to the backend, **0** is displayed.
Failure	● If file was transferred to the backend, **0** is displayed. ● If file was not transferred to the backend, **1** is displayed.

File transfer audit

The **File transfer audit** page displays the details of the files that are transferred to the backend using the Managed File Transfer (MFT) transport type.

Click ↻ to update the data displayed on the page

The following table describes the information that is displayed on the **File transfer audit** page:

Table 30. File transfer audit

Column	Description
Source	Device model from which the file was transferred.
Serial number	Serial number of the device.
File name	Name of the file that is transferred to the backend.
File size (kb)	Size of the file that is transferred to the backend.
Start time	Date and time the file transfer was initiated.
End time	Date and time the file transfer was completed.
Transfer rate	Rate at which the file was transferred.
Remaining time	If the file transfer is in progress, the time remaining to complete the transferred.
Percentage complete	Progress of the file transfer in percentage.

File transfer permission audit

After you add a device in SupportAssist Enterprise, you can enable or disable the following file transfer permissions from the device overview pane:

- File Transfer to Dell EMC
- File Transfer from Dell EMC

- Remote Scripting

File transfer permissions are available only for the following devices types and device models:

- Data protection
- Converged infrastructure appliances other than Web scale model
- Hyperconverged infrastructure appliances
- Data storage devices other than the Peer Storage (PS) or EqualLogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models

The **File transfer permission audit** page displays details about the changes that are performed in these permissions. Click ↗ to save the data displayed on the page in a CSV file. Click ↻ to refresh the data displayed on the page.

The following table describes the information that is displayed on the **File transfer permission audit** page:

Table 31. File transfer permission audit

Column	Description
Product serial number	Serial number of the device.
Product family	Model of the device.
To Dell EMC	• Displays **TRUE** if file transfer to the backend from the device is enabled. • Displays **FALSE** if file transfer to the backend from the device is disabled.
From Dell EMC	• Displays **TRUE** if file transfer to the device from the backend is enabled. • Displays **FALSE** if file transfer to the device from the backend is disabled.
Remote scripting	• Displays **TRUE** if remote scripting is enabled for the device. • Displays **FALSE** if remote scripting is disabled for the device.
Created time	Date and time the device was added in SupportAssist Enterprise.
Modified time	Date and time the permissions were updated.
User name	Name of the user account used to modify the permissions.

Remote script audit

The **Remote script audit** page displays the details of files that are transferred to the devices from the backend.

Click ↗ to save the data displayed on the page in a CSV file. Click ↻ to refresh the data displayed on the page.

The following table describes the information that is displayed on the **Remote script audit** page:

Table 32. Remote script audit

Column	Description
Script request ID	The identification name or number of the script used.
Model	Model of the device.
Serial number	Serial number of the device.
Script name	Name of the script used to send the files, for example, PUT.
Remote script status	Status of the script.
Start time	Date and time when the script was initiated.
End time	Date and time when the script was completed.

20

Logs

The **Download Logs** page provides logs of the following SupportAssist services:

- ConnectEMC
- REST services
- ESRS agent
- Apache
- SAE application and REST services

The log files contain the date and time the log file was generated as the file name. The log files are automatically compressed and saved every 24 hours. Click the log file to initiate the download process.

ⓘ **NOTE:** The **Download Logs** page displays logs for the services run during the last 30 days.

21

Maintenance mode overview

The maintenance mode functionality suspends the alert processing and automatic case creation capability of SupportAssist Enterprise, thereby preventing the creation of unnecessary support cases during an alert storm or a planned maintenance activity. If an alert storm is received from a monitored device, SupportAssist Enterprise automatically places the device in maintenance mode. You can also manually enable the maintenance mode functionality before a planned maintenance activity to temporarily suspend the automatic case creation capability.

The maintenance mode functionality is applicable only for the following devices or device models:

- Server or Hypervisor
- iDRAC
- Chassis
- Networking
- Data storage:
  - PeerStorage (PS) or EqualLogic
  - Storage Center (SC) / Compellent
  - Fluid File System (FluidFS)
  - PowerVault

The following sections provide more information about the maintenance mode functionality.

Global-level maintenance mode

Global-level maintenance mode places all monitored devices in maintenance mode, suspending alert processing and automatic case creation. In this mode a yellow **Maintenance Mode** banner is displayed on top of the page. Enable this mode to prevent the creation of unnecessary support cases during downtime or a routine maintenance activity. For instructions to enable global-level maintenance mode, see Enable or disable global-level maintenance mode on page 110.

Device-level maintenance mode

Device-level maintenance mode suspends alert processing and automatic case creation for a specific device. For all other monitored devices, SupportAssist Enterprise continues to process alerts and create support cases, if the alerts qualify for case creation. Device-level maintenance mode is implemented as follows:

- **Automated device-level maintenance mode**—By default, if SupportAssist Enterprise receives 10 or more valid hardware alerts within 1 hour from a specific device, SupportAssist Enterprise automatically places that device in maintenance mode. The device remains in maintenance mode for 30 minutes, enabling you to resolve the issue without creating additional support cases for the device. An email notification is also sent to the primary and secondary contacts, and the device displays the maintenance mode icon 🔧 on the **Devices** page. After 30 minutes, the device is automatically removed from maintenance mode, enabling SupportAssist Enterprise to resume normal alert processing for the device. If required, you can retain the device in maintenance mode until you resolve the issue, by manually enabling maintenance mode. You can also remove a device from automated maintenance mode before the 30-minute period. For instructions to enable or disable the device-level maintenance mode, see Enable or disable device-level maintenance mode on page 110.
- **Manual device-level maintenance mode**—If you have a planned maintenance activity for a device, and do not want SupportAssist Enterprise to automatically create support cases, you can place that device in maintenance mode. While in maintenance mode, the device displays the maintenance mode icon 🔧 on the **Devices** page. After the maintenance activity is completed, you can remove the device from maintenance mode, enabling SupportAssist Enterprise to resume processing alerts from the device normally. For instructions to enable device-level maintenance mode, see Enable or disable device-level maintenance mode on page 110.

The global-level and device-level maintenance mode functionalities work independent of each other. For example:

- If a device is placed in manual maintenance mode, the device continues to remain in manual maintenance mode even if global-level maintenance mode is enabled and then disabled.

- If a device is placed in automated maintenance mode, the device continues to remain in automated maintenance mode for 30 minutes even if the global-level maintenance mode is enabled and then disabled.

Topics:

Enable or disable global-level maintenance mode

Steps

1. In the SupportAssist header area, click **About**.
   The **About** page is displayed.
2. In the **Maintenance mode** section, perform one of the following:
   - To enable maintenance mode, click **Enable**.
   - If maintenance mode is already enabled, click **Disable**.

   If maintenance mode is enabled, a **Maintenance mode** banner is displayed on the SupportAssist Enterprise user interface.

Enable or disable device-level maintenance mode

If you have a planned maintenance activity for a specific device and do not want SupportAssist Enterprise to process alerts from that device, you can place that device in maintenance mode. After the maintenance activity is completed, you can remove the device from maintenance mode, enabling SupportAssist Enterprise to process alerts from the device normally.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select a device on the **Devices** page.
   The device overview pane is displayed.
3. From the **Tasks** list, under **Maintenance mode**, select **Enable** or **Disable** depending on your requirement.

   If maintenance mode is enabled for a specific device, 🔧 is displayed with the name of the device on the **Devices** page. If you disable maintenance mode for a device, the maintenance mode icon is removed from the device name.

22

Offline mode overview

The offline mode feature suspends the alert processing and automatic case creation capability of SupportAssist Enterprise, thereby preventing the creation of unnecessary support cases during planned maintenance activity. Offline mode functionality is applicable to the following devices or device models:

- Data protection
- Converged infrastructure appliances other than Web scale model
- Hyperconverged infrastructure appliances
- Data storage devices other than the Peer Storage (PS) or EqualLogic, Storage Center (SC) or Compellent, Fluid File System (Fluid FS), and PowerVault models

You can enable offline mode for all devices or for a specific device.

Topics:

Enable or disable global-level offline mode

Steps

1. In the SupportAssist Enterprise header area, click **About**.
   The **About** page is displayed.
2. In the **Setup details** section, perform one of the following:
   - To enable offline mode, click **Set offline**.
   - If you have already enabled offline mode, click **Set online**.

Enable or disable device-level offline mode

About this task

If you have a planned maintenance activity for a specific device and do not want SupportAssist Enterprise to process alerts from that device, you can place that device in offline mode. After the maintenance activity is completed, you can set the device online to process alerts from the device.

Enable or disable offline mode for a specific device. When you set a device to offline mode, the alert generated from the device is not processed for case creation.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select a device.
   The device overview pane is displayed.
3. Perform one of the following:
   - To place the device in offline mode, click **Set offline**.
   - If the device is already placed in offline mode, click **Set online**.

23

Manually configuring SNMP settings

Configuring the SNMP settings (alert destination) of a device ensures that SupportAssist Enterprise receives alerts from the device. SupportAssist Enterprise can automatically configure the SNMP settings of Dell EMC servers. For Dell EMC chassis and networking devices, you must manually configure the SNMP settings.

For information about configuring alert destinations for PowerEdge VRTX, PowerEdge FX2, and PowerEdge M1000E chassis, go to www.dell.com/cmcmanuals. For information about configuring alert destination for PowerEdge MX7000 chassis, go to www.dell.com/openmanagemanuals and then click **Dell OpenManage Enterprise**.

Topics:

Manually configure alert destination of server

By default, when you add a server you can allow SupportAssist Enterprise to automatically configure the alert destination of the server. If the automatic SNMP configuration is unsuccessful, you can configure the SNMP settings of a device by using the following methods:

- Running a script file—The SupportAssist Enterprise deployment folder includes script files that you can use to configure the alert destination of a server.
- Manually configure the SNMP settings—Configure settings by accessing the SNMP trap service.

NOTE: You can retry the automatic configuration of the alert destination at any time using the **Configure SNMP** option available in SupportAssist Enterprise. For information about using the **Configure SNMP** option, see Configure SNMP settings using SupportAssist Enterprise on page 116.

Manually configure alert destination of server running Linux

Perform the following steps to manually configure the alert destination of a server running Linux operating system:

Steps

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

Manually configure alert destination of server running Linux using the script file

Prerequisites

- Net-SNMP must be installed on the system.
- Ensure that you have root privileges on the device.

The script file is supported only on devices running the following operating systems:

- Red Hat Enterprise Linux 5.5 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.7 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.8 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.9 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.10 (32-bit and 64-bit)
- Red Hat Enterprise Linux 5.11 (32-bit and 64-bit)
- Red Hat Enterprise Linux 6.1 (64-bit)
- Red Hat Enterprise Linux 6.2 (64-bit)
- Red Hat Enterprise Linux 6.3 (64-bit)
- Red Hat Enterprise Linux 6.4 (64-bit)
- Red Hat Enterprise Linux 6.5 (64-bit)
- Red Hat Enterprise Linux 6.7 (64-bit)
- Red Hat Enterprise Linux 6.8 (64-bit)
- Red Hat Enterprise Linux 7.0 (64-bit)
- Red Hat Enterprise Linux 7.1 (64-bit)
- Red Hat Enterprise Linux 7.2 (64-bit)
- SUSE Linux Enterprise Server 10 SP3 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 (64-bit)
- SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 11 SP2 (64-bit)
- SUSE Linux Enterprise Server 11 SP3 (64-bit)
- SUSE Linux Enterprise Server 11 SP4 (64-bit)
- SUSE Linux Enterprise Server 12 (64-bit)
- SUSE Linux Enterprise Server 12 SP1 (64-bit)
- CentOS 7.0
- CentOS 6.0
- Oracle Linux 7.1
- Oracle Linux 6.7

Steps

1. On the server where SupportAssist Enterprise is deployed, browse to the `<Drive where SupportAssist Enterprise is deployed>:/opt/dell/supportassist/scripts/` folder.
2. Copy the script file (`LinuxSNMPConfig.sh`) located in the folder and paste the file at a desired location (for example, `\root`) on the device.
3. Open the terminal window and log in as a user with root privileges.
4. Run the script file on the device using the following syntax: `sh LinuxSNMPConfig.sh -d <IP address of the server where SupportAssist Enterprise is installed>`, for example, `sh LinuxSNMPConfig.sh -d 10.10.10.10`.

Manually configure alert destination of iDRAC using the web interface

Perform the following steps to manually configure the alert destination of an iDRAC:

Steps

1. Log in to the iDRAC web interface.
2. Go to **Overview** > **Server** > **Alerts**.
3. In the **Alerts** section, ensure that the **Enabled** option is selected.
4. In the **Alerts Filter** section, ensure that the following options are selected:
   - **System Health**
   - **Storage**

- **Configuration**
- **Audit**
- **Updates**
- **Warning**
- **Critical**

5. In the **Alerts and Remote System Log Configuration** section, ensure that all fields in the **SNMP Trap** column are selected.
6. Click **SNMP and Email Settings**.
7. In the **IP Destination List** section, select the **State** option to enable the alert destination field.

   You can specify up to eight destination addresses. For more information about the options, see the *iDRAC Online Help*.
8. In the **Destination Address** field, type the IP address of the server where SupportAssist Enterprise is installed.
9. Type the iDRAC SNMP community string (public) and the SNMP alert port number (for example, 162) in the appropriate fields.

   For more information about the options, see *iDRAC Online Help*.

   > ⓘ **NOTE:** The community string value indicates the community string to be used in a Simple Network Management Protocol (SNMP) alert trap sent from iDRAC. Ensure that the destination community string is the same as the iDRAC community string. The default community string is Public.

10. Click **Apply**.
    The alert destination is configured.
11. In the **SNMP Trap Format** section, ensure that either **SNMP v1** or **SNMP v2** is selected, and click **Apply**.

    iDRAC is now configured to forward alerts to the server where SupportAssist Enterprise is installed.

    > ⓘ **NOTE:** For information about configuring the alert destination of an iDRAC using other methods, see “Configuring IP Alert Destinations” in the *iDRAC User's Guide* available at www.dell.com/idracmanuals .

Manually configure alert destination of networking device

About this task

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

Steps

1. Log in to the networking device by using a terminal emulator such as PuTTY.
   The terminal window is displayed.
2. Enter **`configure`** and press Enter.
3. Enter **`snmp-server host <IP address of the server where SupportAssist Enterprise is installed> traps version 1`**.
4. To verify if the alert destination is configured successfully, enter **`show running-config snmp`** and press Enter.
   The list of alert destinations that are configured on the device is displayed.

24

Maintaining SupportAssist Enterprise capability

The changes that occur in your company IT setup over a period may require configuration or updates in SupportAssist Enterprise. To maintain SupportAssist Enterprise capability over a period for all your devices, you may be required to:

- Enable monitoring of devices. See Enable or disable device monitoring on page 115.
- Edit the credentials (user name and password) of a device, if the device credentials were changed because of your company security policy or for other reasons. See Edit account credentials on page 62.
- Install or upgrade dependent components such as Dell OpenManage Server Administrator (OMSA). See Install or upgrade OMSA using SupportAssist Enterprise on page 116.
- Configure the SNMP settings of a device. See Configure SNMP settings using SupportAssist Enterprise on page 116.
- Update the proxy server settings in SupportAssist Enterprise, if applicable. See Configure proxy server settings on page 94.
- Update the SMTP server (email server) settings in SupportAssist Enterprise, if applicable. See Configure SMTP server settings on page 101.
- Perform the connectivity test to ensure that SupportAssist Enterprise can connect to all dependent network resources. See Network Connectivity Test on page 23.
- Perform the case creation test to verify the automatic case creation capability of SupportAssist Enterprise. See Test the case creation capability on page 24.
- Clear the System Event Log of a server. See Clear system event log on page 117.
- Upgrade or update SupportAssist Enterprise. See Update SupportAssist Enterprise on page 125.

You may also want to delete a device, if you do not want SupportAssist Enterprise to monitor a device or for other reasons. See Delete device on page 46.

Topics:

Enable or disable device monitoring

About this task

For devices that SupportAssist Enterprise can monitor, you can enable monitoring while adding the device. Depending on your requirement, you can also enable or disable monitoring of a device at any time from the **Devices** page. For SupportAssist Enterprise to automatically create a support case when a hardware issue occurs on a device, monitoring must be enabled for that device.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the device for which you want to enable or disable monitoring.
   The device overview pane is displayed in the right side on the **Devices** page.
3. In **Monitoring**, select **Enable** or **Disable** depending on your requirement.

   NOTE: To enable SupportAssist Enterprise to monitor a device, besides enabling monitoring, the SNMP settings of the device must also be configured. For instructions to configure the SNMP settings of a device, see Configure SNMP settings using SupportAssist Enterprise on page 116 and Manually configuring SNMP settings on page 112.

Install or upgrade OMSA using SupportAssist Enterprise

Prerequisites

You must have read-write access to the system drive of the target device.

About this task

To monitor a server for hardware issues, the Dell OpenManage Server Administrator (OMSA) agent must be installed and running on the server. If OMSA is either not installed or requires an upgrade on a device, the **Status** column on the **Devices** page displays an appropriate message. You can use the **Install / Upgrade OMSA** option to automatically download and install the recommended version of OMSA on a device.

ⓘ **NOTE:** The SupportAssist Enterprise recommended version of OMSA may vary depending on the PowerEdge server and the operating system running on the server. For information about the recommended versions of OMSA, see the *SupportAssist Enterprise Version 4.0 Support Matrix* at https://www.dell.com/serviceabilitytools.

ⓘ **NOTE:** Installation or upgrade of OMSA by using SupportAssist Enterprise is not supported on servers running the following operating systems or hypervisors:

- Oracle Enterprise Linux
- CentOS
- Citrix XenServer
- VMware ESX or ESXi
- Oracle Virtual Machine
- Debian 7.*x*
- Debian 8.*x*
- Ubuntu 14.*x*
- Ubuntu 16.*x*
- Ubuntu 18.*x*

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the server where you want to install or upgrade OMSA.
   The device overview pane is displayed in the right side on the **Devices** page.
3. From the **Tasks** list, select **Install / Upgrade OMSA**.

   ⓘ **NOTE:** If SupportAssist Enterprise does not support the installation or upgrade of OMSA on the server that you have selected, the **Install / Upgrade OMSA** option is disabled.

   The **Status** column on the **Devices** page displays the status of the OMSA installation or upgrade.

Configure SNMP settings using SupportAssist Enterprise

Prerequisites

You must have read-write access to the system drive of the target device.

About this task

Configuring SNMP settings sets the alert destination of a device, and ensures that alerts from the device are forwarded to the server where SupportAssist Enterprise is deployed. If the SNMP settings of a device are not configured, the status column on the **Devices** page displays an appropriate message. You can use the **Configure SNMP** option to automatically configure the SNMP settings of a device.

NOTE: Configuring SNMP by using SupportAssist Enterprise is not supported on devices running the following operating system or hypervisors:

- Oracle Enterprise Linux
- VMware ESXi
- Oracle Virtual Machine

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the device where you want to configure the SNMP settings.

   NOTE: If SupportAssist Enterprise does not support the configuration of SNMP on the device that you have selected, the **Configure SNMP** option is disabled.

   The device overview pane is displayed in the right side on the **Devices** page.
3. From the **Tasks** list, select **Configure SNMP**.
   The **Status** column on the **Devices** page displays the status of the SNMP configuration.

Clear system event log

About this task

The System Event Log (SEL) or hardware log, also known as the Embedded System Management (ESM) log, reports potential hardware problems in Dell PowerEdge servers. You can use the **Clear System Event Log** option available in SupportAssist Enterprise to clear the SEL in the following cases:

- An error message is displayed on a server even after the problem is resolved.
- An SEL full error message is displayed.

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

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.
2. Select the server where you want to clear the System Event Log.

   NOTE: If OMSA is not installed on a device that you have added in SupportAssist Enterprise with the **Device type** as **Server**, the **Clear system event log** option is disabled.

   The device overview pane is displayed in the right side on the **Devices** page.
3. From the **Tasks** list, select **Clear system event log**.

   While the SEL is cleared from a device, the device displays a 🕓 **Clearing System Event Log** status in SupportAssist Enterprise. After the SEL is cleared successfully, the device displays a ✓ **System Event Log cleared** status.

Perform deep discovery

Prerequisites

A credential profile must be assigned to the device.

About this task

Deep discovery enables you to discover a device and its associated device types. See Deep discovery on page 121.

Steps

1. Go to **Devices** > **View Devices**.
   The **Devices** page is displayed.

2. Select the device for which you want to perform deep discovery.
   The device overview pane is displayed.
3. From the **Tasks** list, select **Perform deep discovery**.
   The **Perform deep discovery** window is displayed.

   NOTE: If deep discovery is not applicable for a device, the **Perform deep discovery** option is disabled.
4. Select a credential profile and click **Next**.
   The device is revalidated and the associated devices are discovered.

25

Other useful information

This chapter provides additional information that you may require while using SupportAssist Enterprise.

Topics:

Hardware issue monitoring on servers

SupportAssist Enterprise can monitor Dell EMC servers through the following methods:

- **Agent-based monitoring**—This method is used to monitor devices that are added with the **Device Type** as **Server / Hypervisor**. In this method, an agent acts as an interface between the device and SupportAssist Enterprise. The agent generates an alert (SNMP trap) whenever a hardware event occurs on the device. For monitoring a device using the agent-based method, SupportAssist Enterprise depends on the Dell OpenManage Server Administrator (OMSA) agent. The OMSA agent is an application that monitors the health of various components of the device where it is installed. Whenever a hardware event occurs on the device, the OMSA agent generates an alert. SupportAssist Enterprise processes the alert to determine if the alert qualifies for creating a support case. For instructions to add a device for agent-based monitoring, see Add server or hypervisor on page 36.

  NOTE: Without OMSA, SupportAssist Enterprise cannot monitor a device through the agent-based monitoring method.

  NOTE: Installation of OMSA may not be supported on certain operating systems. SupportAssist Enterprise may be able to monitor devices running such operating systems only through the agentless monitoring method. For information about the operating system requirements for agent-based monitoring, see the *SupportAssist Enterprise Version 4.0 Support Matrix* at https://www.dell.com/serviceabilitytools.

- **Agentless monitoring**—This method is used to monitor iDRAC devices. In this method, the iDRAC available on the device acts as an interface between the device and SupportAssist Enterprise. Whenever a hardware event occurs on the device, the iDRAC generates an alert. SupportAssist Enterprise processes the alert to determine if the alert qualifies for creating a support case. For instructions to add a device for agentless monitoring, see Add iDRAC on page 33.

  NOTE: Agentless monitoring is supported only for the yx2x and later PowerEdge servers (iDRAC 7 and later).

  NOTE: The iDRAC can be configured to send alerts through SNMP and IPMI. However, SupportAssist Enterprise can only receive alerts sent through SNMP. To ensure that SupportAssist Enterprise receives alerts sent from an iDRAC, you must ensure that all **SNMP Trap** options are selected in the **Alerts and Remote System Log Configuration** section of the iDRAC web console.

Benefits of agent-based monitoring

Although the yx2x and later PowerEdge servers can be monitored through the agentless (iDRAC) method, agent-based (OMSA) method has the following benefits:

- Alert generation capabilities of OMSA and iDRAC are not the same. In the yx3x or later PowerEdge servers, the alert generation capabilities of OMSA and iDRAC are almost similar. However, alerts from chipset and software RAID are available only through OMSA.
- Recommendations for operating system and software component versions are available only if the devices with a ProSupport Plus, ProSupport Flex for Data Center, or ProSupport One for Data Center service contract is monitored through OMSA.
- OMSA is the only option available for monitoring the nx9x to yx1x PowerEdge servers.

Support to automatically install or upgrade OMSA

To monitor a device through the agent-based method, the Dell OpenManage Server Administrator (OMSA) agent must be installed and running on the device. The OMSA agent is an application that monitors the health of various components of the device where it is installed. When OMSA is installed and running on a device, the OMSA agent generates an alert whenever a hardware event occurs on the device. SupportAssist Enterprise processes the alert to identify if the alert indicates a hardware issue. For more information about OMSA, go to Delltechcenter.com/OMSA.

> **NOTE:** The SupportAssist Enterprise recommended version of OMSA may vary depending on the PowerEdge server and the operating system running on the server. For information about the recommended versions of OMSA, see the *SupportAssist Enterprise Version 4.0 Support Matrix* available at https://www.dell.com/serviceabilitytools.

SupportAssist Enterprise has the capability to automatically download and install the recommended version of OMSA on a device. By default, when a server is added for agent-based monitoring, SupportAssist Enterprise verifies if the recommended version of OMSA is installed on the device.

- If OMSA is not installed on the device, SupportAssist Enterprise prompts for your confirmation to download and install the recommended version of OMSA on the device. On confirmation, SupportAssist Enterprise downloads and installs OMSA in the background. The OMSA installation status is displayed in the **Status** column on the **Devices** page. If you choose not to install OMSA, the status of the device is displayed as ⚠ **OMSA not installed**. To install OMSA later, you can use the **Tasks** > **Install / Upgrade OMSA** option on the device overview pane.
- If OMSA is already installed on the device, SupportAssist Enterprise verifies if the version of OMSA matches with the recommended OMSA version for SupportAssist Enterprise. If the existing version of OMSA is not the recommended version, but supports direct upgrade to the recommended version of OMSA, SupportAssist Enterprise prompts for your confirmation to download and upgrade OMSA on the device. The OMSA upgrade status is displayed in the **Status** column on the **Devices** page. If you choose not to upgrade OMSA, the status of the device is displayed as ⚠ **New version of OMSA available**. To upgrade OMSA later, use the **Tasks** > **Install / Upgrade OMSA** option on the device overview pane.

  > **NOTE:** Direct upgrade to OMSA version *n* is supported only from the two previous versions *(n-2)* of OMSA. If direct upgrade is not supported, you must manually download and upgrade OMSA on the device. For example, if OMSA version 7.0 is already installed on the device, but the recommended version of OMSA is 7.4, you must manually upgrade from OMSA version 7.0 to 7.2. After upgrading to OMSA version 7.2, you can upgrade to OMSA version 7.4 using the **More Tasks** > **Install/Upgrade OMSA** option on the device overview pane or you can manually download and upgrade to OMSA version 7.4.

> **NOTE:** When you enable or use SupportAssist Enterprise to install or upgrade OMSA, the downloaded packages of OMSA are retained in the SupportAssist Enterprise installation folder. If a compatible version of OMSA was already downloaded during an earlier operation, SupportAssist Enterprise does not download OMSA again. In this case, SupportAssist Enterprise only installs or upgrades OMSA on the device using the already downloaded version of OMSA.

> **NOTE:** The time taken to download OMSA depends on the Internet download speed and network bandwidth.

If the recommended version of OMSA is installed and running on the device, the status of the device is displayed as ✓ **Success**.

> **NOTE:** Automatic installation of OMSA through SupportAssist Enterprise is not supported on devices running Citrix XenServer, VMware ESXi, or ESX. To enable SupportAssist Enterprise to detect hardware issues on these devices, you must manually download and install OMSA.

Support to automatically configure SNMP settings

To enable SupportAssist Enterprise to monitor a device, the device must be configured to forward alerts (SNMP traps) to the server where SupportAssist Enterprise is deployed. Configuring the SNMP settings sets the alert destination of a device and ensures that alerts from the device are forwarded to the server where SupportAssist Enterprise is deployed. SupportAssist Enterprise can also automatically configure the SNMP settings of a device such that the device forwards alerts to the server where SupportAssist Enterprise is deployed. You can allow SupportAssist Enterprise to configure the SNMP settings of the device while adding the device or later. The status of the SNMP configuration is displayed in the **Status** column on the **Devices** page. While SupportAssist Enterprise configures the SNMP settings of a device, the device displays a **Configuring SNMP** status. You can also use the **Tasks** > **Configure SNMP** option on the device overview pane to automatically configure the SNMP settings of a device at any time.

NOTE: When you allow SupportAssist Enterprise to automatically configure the SNMP settings of a device, the alert destination of the device is set to the IP address of the server where SupportAssist Enterprise is deployed.

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 to the discovery task. You can choose to perform deep discovery while discovering the primary device or after the primary device is discovered.

NOTE: Deep discovery may result in an increase in the duration of the overall discovery process.

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

Table 33. Primary device and its associated devices discovered by deep discovery

Primary Device	Associated devices discovered by deep discovery
Chassis	● iDRAC* ● Networking switches
Storage PS Series group	● Storage PS Series members ● Storage PS Series FluidFS
Storage MD Series Enclosure	● JBODs
Networking - management switch	● Member switches
Web-scale appliance	● Controller VM ● Node (iDRAC / ESX)

* On deep discovery of chassis, discovery of the iDRAC (modular servers) is supported only for iDRAC7 or later.

NOTE: On deep discovery of a chassis, networking devices associated with the chassis are also discovered. However, you can collect system information only from networking devices that are supported by SupportAssist Enterprise. For the list of supported networking devices, see the *SupportAssist Enterprise Version 4.0 Support Matrix* at https://www.dell.com/serviceabilitytools.

Device correlation

You can add (discover) a server in SupportAssist Enterprise by using both 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. SupportAssist Enterprise receives alerts from the device through both the operating system and the iDRAC. However, for operational purposes, SupportAssist Enterprise correlates the operating system IP address and iDRAC IP address of the device and considers the device as a single device. The following are the expected behaviors when a device is correlated:

- Alerts originating from the operating system and the iDRAC are correlated and a support case is created for the Service Tag of the device.
- When system information is collected, the **Devices** page displays the same status for both the listings.
- For a manually-initiated collection of system information—System information is gathered through the selected device listing in the **Devices** page. For example, if the operating system listing is selected, system information is gathered through the operating system. However, if SupportAssist Enterprise is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.
- For periodic collections and on case creation—System information is typically gathered through the operating system. However, if SupportAssist Enterprise is unable to connect to the device by using the operating system IP address, system information is gathered through the iDRAC.

Association view

The **Devices** page supports two types of views for displaying the list of devices:

- Default view—Displays all available devices as a list
- Association view—Displays all available devices as groups based on their association. This view enables you to view a primary device and its associated devices as a group

The following table lists the grouping of devices in the association view:

Table 34. Device grouping in association view

Primary Device	Associated devices
Server	● iDRAC ● vCenter
Chassis	● iDRAC* ● Networking switches
Storage PS Series group	● Storage PS Series members ● Storage PS Series FluidFS
Storage MD Series Enclosure	JBODs
Networking - management switch	Member switches
Web-scale appliance	● Controller VM ● iDRAC

* Only iDRAC7 or later is displayed under the Chassis node.

NOTE: Starting the collection of system information is not supported for the following devices that may be displayed in the Association view:

- JBODs
- Storage PS Series members
- Stacked switches
- Devices that are listed in SupportAssist Enterprise with an IP address as 0.0.0.0

Detection of hardware issues in attached storage devices

In addition to monitoring PowerEdge servers, SupportAssist Enterprise can also process alerts that are received from Storage MD Series arrays that may be attached to a server. Alert generation from an attached storage device occurs through the OpenManage Storage Services (OMSS) application that is installed on the server. When you allow SupportAssist Enterprise to automatically install OMSA on the server, by default, OMSS is also installed. If you manually download and install OMSA on the server, ensure that you also install OMSS. Otherwise, SupportAssist Enterprise cannot detect hardware issues that may occur on the attached storage device. When a hardware issue is detected on an attached storage device, SupportAssist Enterprise automatically creates a support case for the associated server.

Support for OEM devices

Dell EMC OEM-ready devices (either rebranded or debranded Dell EMC hardware), when added, are classified under the rebranded name and not the original Dell hardware name. All the functionality available for Dell EMC 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 SupportAssist Enterprise user interface.

Automatic case creation is supported through Dell EMC Enterprise Technical Support and not available for other support case service request management systems.

As with any system that is modified for custom solutions, it is recommended that all SupportAssist Enterprise features are validated to ensure proper operation with those modifications.

Access SupportAssist Enterprise application logs

About this task

SupportAssist Enterprise saves system events and log messages in the following locations:

- var logs
- The deployment logs folder: `/var/lib/docker/volumes/saede_logs/_data`

A new log file is created daily at 11:59 p.m. based on the time zone configured on the system, and the log is stored in the logs folder. The log file contains log information for the current day. At the end of each day, the log file is renamed as `application.log` *<date format in yyyymmdd>*. If the log file is older than two days, the log file is zipped automatically. This enables you to identify the exact log file stored for a given date when alerts occur. For example, log files similar to the following can be seen:

- `application.log`
- `application.log.` *20171101*
- `application.log.` *20171102* `.zip`
- `application.log.` *20171103* `.zip`

The log files are purged from storage after 30 days.

The log file contains log messages that correspond to the following values (or higher) in the `log4j.xml` file: FATAL, ERROR, WARN, INFO, and DEBUG, with special values of OFF and ALL. The `log4j.xml` file is available at `/opt/dell/supportassist/config`. A value of ERROR in the `log4j.xml` file results in log messages of FATAL, and ERROR, since FATAL is a higher level than ERROR.

To download logs from the SupportAssist Enterprise user interface, log in to SupportAssist Enterprise and go to **Logs** > **Download Logs**. For more information, see Logs on page 108.

Identify series of PowerEdge server

PowerEdge servers are represented as *xnxx* or *yxnx* series of servers, where:

- *x* denotes numbers 0 through 9
- *n* denotes the series of the server
- *y* denotes alphabets M, R, and T. The alphabets denote the type of server as follows: M = Modular; R = Rack; T = Tower

The following table provides information about the various series of PowerEdge servers and their model representation:

Table 35. PowerEdge server examples

Series of servers	Representation of the server model	Examples of server models
9th	PowerEdge *x9xx*	PowerEdge 2900 Power Edge 6950
10th	PowerEdge *yx0x*	PowerEdge M600 PowerEdge R300 Power Edge T105
11th	PowerEdge *yx1x*	PowerEdge M610 PowerEdge R310 PowerEdge T110
12th	PowerEdge *yx2x*	PowerEdge M620 PowerEdge R620

Table 35. PowerEdge server examples (continued)

Series of servers	Representation of the server model	Examples of server models
		PowerEdge T620
13th	PowerEdge *yx3x*	PowerEdge M630 PowerEdge R630 PowerEdge R730 PowerEdge FC630 PowerEdge T320
14th	PowerEdge *yx4x*	PowerEdge R740 PowerEdge T640 PowerEdge M640 PowerEdge R7415 DSS 9620
15th	PowerEdge *yx5x*	

Event storm handling

SupportAssist Enterprise intelligently handles event storm conditions, allowing up to nine separate alerts from a device within a 60-minute timespan. However, if 10 or more separate alerts are received from a device, SupportAssist Enterprise automatically places the device in maintenance mode. Maintenance mode prevents any further processing of alerts from the device, enabling you to make infrastructure changes without creating unnecessary support cases. After 30 minutes in maintenance mode, SupportAssist Enterprise automatically removes the device from maintenance mode and resumes normal alert processing for the device. For more information about maintenance mode, see Maintenance mode overview on page 109.

Configure sudo access for SupportAssist Enterprise on server running Linux

In Linux operating systems, users with sudo access may be granted administrative privileges to run certain commands. If you have added a remote device in SupportAssist Enterprise using the credentials of a sudo user, you must perform the following steps to allow SupportAssist Enterprise to monitor and collect system information from the device.

Prerequisites

Ensure that you are logged in to the remote device as a user with root privileges.

Steps

1. Open the terminal window.
2. Set the home directory path for the user — Type `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.

Update SupportAssist Enterprise

SupportAssist Enterprise checks if any updates are available when you log in to SupportAssist Enterprise.

If you have deployed SupportAssist Enterprise version 4.0 or later, a banner is displayed for the following updates:

- Docker updates—Includes fixes or updates for the backend components
- Operating system or JRE updates—Includes updates from SUSE for the operating system
- Configuration updates—Includes updates for the device configuration and policy files

> **NOTE:** To update to SupportAssist Enterprise version 4.0 or later from SupportAssist Enterprise version 2.x, you must manually download and deploy SupportAssist Enterprise. See Downloading SupportAssist Enterprise on page 11 and Deploying SupportAssist Enterprise on page 14.

The following options are displayed on the banner:

- **Download Now**—Click to download the updates to the local folder.
- **Update now**—Displayed after the download is complete. Click to install the downloaded update.

  > **NOTE:** During a docker or an operating system update, you are logged out of SupportAssist Enterprise. After the update is complete, the SupportAssist Enterprise services are automatically restarted.
- **Remind me later**—Click to close the banner. The banner is not displayed until you log in to SupportAssist Enterprise again.
- **Learn More**—Provides details about the updates.