Dell EMC iDRAC Service Module 4.2.0.0

User's Guide

June 2022
Rev. A02

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

Introduction

The iDRAC Service Module (iSM) is a lightweight software module that you can install on Dell EMC PowerEdge yx2x or later servers. The iSM complements iDRAC interfaces—the user interface (UI), RACADM CLI, Redfish, and Web Services-Management (WS-Man)—with additional monitoring data. You can configure the iSM features from within the supported operating system depending on the features you install and the unique integration needs of your environment.

Topics:

New in this release

New supported operating systems

iDRAC Service Module 4.2.0.0 supports the following new operating systems:

- Red Hat Enterprise Linux 8.5
- Ubuntu Server 20.04.3 LTS

New and enhanced features

The following are the new and enhanced features of iDRAC Service Module 4.2.0.0:

- Isolation of OS to iDRAC Pass-through Independent feature - When iSM is unable to establish communication with iDRAC over the OS to iDRAC Pass-through interface, the iSM runs in Limited Functionality mode.
- Software RAID enumeration - iSM enables enumeration of Software RAID PERC S130 and later series of controllers.
- Transport Layer Security (TLS) 1.3 protocol support - iSM communicates with iDRAC over the TLS 1.3 protocol.
- Hyper Converged Infrastructure (HCI) log collection is available as part of SupportAssist Collection (SAC).
- Enhanced NVMe Passthrough feature - Prepare to Remove feature on NVMe devices is enabled in the Passthrough mode on VMware ESXi operating system.

Operating system supported feature matrix

The table lists the iDRAC Service Module 4.2.0.0 features, operating systems, and the supported Dell EMC PowerEdge yx2x to yx5x servers.

Table 1. Features supported by each supported operating system

Features	Servers	Operating systems		
-	Supported PowerEdge series	Microsoft Windows (including HyperV systems)	Linux	Virtualization (VMware ESXi)
Sharing operating system information	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes

Table 1. Features supported by each supported operating system (continued)

Features	Servers	Operating systems		
-	Supported PowerEdge series	Microsoft Windows (including HyperV systems)	Linux	Virtualization (VMware ESXi)
Lifecycle Controller Log replication	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Automatic system recovery/watchdog	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Windows Management Instrumentation Providers	yx2x, yx3x, yx4x, yx5x	Yes	NA	NA
Prepare to remove NVMe device through iDRAC.	yx3x, yx4x, yx5x	Yes	Yes	Yes
SupportAssist collection from host operating system	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Operating system and application data	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes (only for PowerEdge yx4x and later servers)
Remote iDRAC hard reset	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes (command line utility is supported only on VMware ESXi 7.x)
iDRAC access via Host OS	yx2x, yx3x, yx4x, yx5x	Yes	Yes	NA
In-Band support for iDRAC SNMP alerts	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Network interface monitoring support through Redfish client	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Enable WS-Man remotely.	yx2x, yx3x, yx4x, yx5x	Yes	NA	NA
FullPowerCycle	yx4x, yx5x	Yes	Yes	VMware ESXi 7.x: Yes
In-Band SNMP get	yx2x, yx3x, yx4x, yx5x	Yes	Yes	NA
Live VIB installation	yx3x, yx4x, yx5x	NA	NA	Yes
SupportAssist-anonymous collection report	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
iDRAC UI launcher	yx3x, yx4x, yx5x	Yes	Yes	NA
IPv6 support	yx3x, yx4x, yx5x	Yes	Yes	NA
Auto dispatch for selective events	yx4x, yx5x	Yes	Yes	Yes
SupportAssist collection with selective PII	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes

Table 1. Features supported by each supported operating system (continued)

Features	Servers	Operating systems		
-	Supported PowerEdge series	Microsoft Windows (including HyperV systems)	Linux	Virtualization (VMware ESXi)
Single Sign-on (SSO)	yx4x, yx5x	Yes	Yes	NA
Auto-update iSM installation	yx4x, yx5x	Yes	Yes	NA
Server storage(S2D) correlation	yx3x, yx4x, yx5x	Yes	NA	NA
S.M.A.R.T monitoring in AHCI Mode	yx3x, yx4x, yx5x	Yes	Yes	Yes
S.M.A.R.T monitoring in software RAID mode	yx3x, yx4x, yx5x	Yes	NA	NA
OMSA SNMP alerts mapping	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes
Software RAID	yx3x, yx4x, yx5x	Yes	NA	NA
Isolation of OS to iDRAC Pass-through Independent feature	yx2x, yx3x, yx4x, yx5x	Yes	Yes	Yes

NA - Not applicable

Supported platforms

iDRAC Service Module 4.2.0.0 supports PowerEdge yx2x to yx5x generation of servers. For more information, see Identifying the series of your Dell EMC PowerEdge servers.

Table 2. iDRAC Service Module 4.2.0.0 supported platforms

Supported Dell EMC platforms			
yx5x servers	yx4x servers	yx3x servers	yx2x servers
PowerEdge C6520	PowerEdge C4140	PowerEdge C4130	PowerEdge FM120
PowerEdge C6525	PowerEdge C6420	PowerEdge C6320	PowerEdge M420
PowerEdge MX750c	PowerEdge FC640	PowerEdge FC430	PowerEdge M520
PowerEdge R250	PowerEdge FD332	PowerEdge FC630	PowerEdge M620
PowerEdge R350	PowerEdge M640	PowerEdge FC830	PowerEdge M820
PowerEdge R450	PowerEdge M640-VRTX	PowerEdge M630	PowerEdge R220
PowerEdge R550	PowerEdge MX740c	PowerEdge M630-VRTX	PowerEdge R320
PowerEdge R650	PowerEdge MX840c	PowerEdge M830	PowerEdge R420
PowerEdge R650XS	PowerEdge R240	PowerEdge R230	PowerEdge R620
PowerEdge R6515	PowerEdge R340	PowerEdge R330	PowerEdge R720
PowerEdge R6525	PowerEdge R440	PowerEdge R430	PowerEdge R720XD
PowerEdge R750	PowerEdge R540	PowerEdge R530	PowerEdge R820
PowerEdge R750xa	PowerEdge R640	PowerEdge R630	PowerEdge R920
PowerEdge R750XS	PowerEdge R6415	PowerEdge R730	PowerEdge T320
PowerEdge R7515	PowerEdge R740	PowerEdge R730xd	PowerEdge T420

Table 2. iDRAC Service Module 4.2.0.0 supported platforms (continued)

Supported Dell EMC platforms			
yx5x servers	**yx4x servers**	**yx3x servers**	**yx2x servers**
PowerEdge R7525 PowerEdge T150 PowerEdge T350 PowerEdge T550 PowerEdge XR11 PowerEdge XR12 PowerEdge XE8545	PowerEdge R740xd PowerEdge R740xd2 PowerEdge R7415 PowerEdge R7425 PowerEdge R840 PowerEdge R940 PowerEdge R940xa PowerEdge T140 PowerEdge T340 PowerEdge T440 PowerEdge T640 PowerEdge XE2420 PowerEdge XE7420 PowerEdge XE7440 Precision R7920	PowerEdge R830 PowerEdge R930 PowerEdge T130 PowerEdge T330 PowerEdge T430 PowerEdge T630	PowerEdge T620

Coexistence of OpenManage Server Administrator and iDRAC Service Module

OpenManage Server Administrator (OMSA) and iDRAC Service Module (iSM) can coexist on a single system. If you enable the monitoring features during the iSM installation, and, after the installation is complete, if the iSM detects the presence of OMSA, iSM disables the AutoSystemRecovery and Lifecycle Log Replication features that overlap. If the OMSA service stops, the iSM features that had been disabled are enabled.

ⓘ **NOTE:** The overlapping features are **AutoSystemRecovery** and **Lifecycle Log Replication**.

Software availability

iDRAC Service Module software is available at:

- *Dell EMC OpenManage Systems Management Tools and Documentation* DVD
- https://www.dell.com/support

Downloading iSM

To download the iDRAC Service Module, complete the following steps:

1. Go to https://www.dell.com/idracmanuals.
2. Click **iDRAC Service Module**, and click to open the required version of iDRAC Service Module.
3. Click **Drivers and Downloads**.

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.

- Direct links:
  - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—https://www.dell.com/esmmanuals
  - For Dell EMC Virtualization Solutions—www.dell.com/virtualizationsolutions
  - For Dell EMC OpenManage—https://www.dell.com/openmanagemanuals
  - For iDRAC—https://www.dell.com/idracmanuals
  - For Dell EMC OpenManage Connections Enterprise Systems Management—https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Dell EMC Serviceability Tools—https://www.dell.com/serviceabilitytools
- Dell EMC support site:
  1. Go to https://www.dell.com/support.
  2. Click **Browse all products**.
  3. From the **All products** page, click **Software**, and then click the required link.
  4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.

Other documents you may need

You can find information on how to configure iSM security as well as information on using iDRAC, RACADM, DUP, event messages, and the Dell Lifecycle Controller 2 Web Services at Dell.com/support.

- The *iDRAC Service Module Security Configuration Guide* provides the security configurations related to iDRAC Service Module (iSM).
- The *Integrated Dell Remote Access Controller (iDRAC) User's Guide* provides detailed information about configuring and using the iDRAC.
- The *Dell Remote Access Controller RACADM User's Guide* provides information about using the RACADM command-line utility.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell Event Messages Reference Guide* provides information about the event and error information that is generated by firmware and other agents that monitor system components.
- The *Dell Lifecycle Controller 2 Web Services Interface Guide* provides information and examples for using the Web Services for Management (WS-Man) protocol.

Software license agreement

The software license for supported versions of the operating system of iSM is available on the installer. Read the `license_agreement.txt` file. By installing or copying any of the files on the media, you agree to the terms in `license_agreement.txt` file.

Preinstallation setup

Before installing iDRAC Service Module (iSM), ensure that you fulfill the following requirements:

- Have administrator privileges.
- Have access to PowerEdge yx2x or later servers. For the list of supported platforms, see Supported platforms.
- Read the installation instructions for the operating system.
- Read the applicable Release Notes and the Systems Software Support Matrix.
- Read the installation requirements to ensure that the system meets the minimum requirements.
- Close all applications running on the system before installing the iSM application.

Topics:

Installation requirements

For the list of operating systems that are supported on iDRAC Service Module (iSM), see Supported operating systems.

Prerequisites specific to an operating system are listed as part of the installation procedures. The iSM can be installed using the UI. The installer also supports silent installation.

Supported operating systems and hypervisors

iDRAC Service Module 4.2.0.0 supports the following 64–bit operating systems:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.5
- Red Hat Enterprise Linux 8.4
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP3
- Ubuntu Server 20.04.3 LTS
- VMware vSphere (ESXi) 7.0 U3 supported on PowerEdge yx3x, yx4x, and yx5x servers.
- VMware vSphere (ESXi) 6.7 U3 supported on PowerEdge yx3x, yx4x, and yx5x servers.

iDRAC Service Module 4.2.0.0 supports the following client operating systems on Dell EMC Precision R7920:

- Microsoft Windows 10 RS5
- Microsoft Windows 10 Pro (20H2)
- Microsoft Windows 11
- Red Hat Enterprise Linux 8.0
- Ubuntu Desktop 20.04 LTS

Supported platforms

iDRAC Service Module 4.2.0.0 supports Dell EMC PowerEdge yx2x, yx3x, yx4x and yx5x servers.

Supported platforms on Linux operating systems

The following table lists the platforms that are supported by iDRAC Service Module 4.2.0.0 on Linux operating systems.

Table 3. Supported platforms on Linux operating systems

Dell EMC devices	Ubuntu Server 20.04.3 LTS	SUSE Linux Enterprise Server 15 SP3	Red Hat Enterprise Linux 7.9	Red Hat Enterprise Linux 8.4	Red Hat Enterprise Linux 8.5
PowerEdge yx5x servers	Yes	Yes	Yes	Yes	Yes
PowerEdge yx4x servers	Yes	Yes	Yes	Yes	Yes
PowerEdge yx3x servers	No	Yes	Yes	Yes	Yes
PowerEdge yx2x servers	No	No	Yes	No	No

NOTE: Only limited PowerEdge yx3x servers support the Red Hat Enterprise Linux 8.x operating system. For the list of supported Dell EMC PowerEdge servers, see Red Hat Enterprise Linux Certification Matrix for Dell EMC PowerEdge Servers.

For the list of Dell EMC PowerEdge servers that support Ubuntu Server, see Ubuntu Server LTS Certification Matrix for Dell EMC PowerEdge Servers.

For the list of Dell EMC PowerEdge servers that support SUSE Linux Enterprise Server, see SUSE Linux Enterprise Server Certification Matrix for Dell EMC PowerEdge Servers.

Supported platforms on Microsoft Windows operating systems

The following table lists the platforms that are supported by iDRAC Service Module 4.2.0.0 on Microsoft Windows operating systems.

Table 4. Supported platforms on Microsoft Windows operating systems

Dell EMC devices	Microsoft Windows Server 2016	Microsoft Windows Server 2019	Microsoft Windows Server 2022
PowerEdge yx5x servers	Yes	Yes	Yes
PowerEdge yx4x servers	Yes	Yes	Yes
PowerEdge yx3x servers	Yes	Yes	No
PowerEdge yx2x servers	Yes	No	No

NOTE: Only limited PowerEdge yx4x servers support the Microsoft Windows Server 2022 operating system. For the list of supported Dell EMC PowerEdge servers, see Microsoft Windows Server Support Matrix for Dell EMC PowerEdge Servers.

Supported platforms on virtualization hypervisor

The following table lists the platforms that are supported by iDRAC Service Module 4.2.0.0 on virtualization operating systems.

Table 5. Supported platforms on virtualization hypervisor

Dell EMC PowerEdge servers	VMware ESXi	
	vSphere 7.0 U3	vSphere 6.7 U3
PowerEdge yx5x servers	Yes	Yes
PowerEdge yx4x servers	Yes	Yes

Table 5. Supported platforms on virtualization hypervisor (continued)

Dell EMC PowerEdge servers	VMware ESXi	
	vSphere 7.0 U3	vSphere 6.7 U3
PowerEdge yx3x servers	Yes	Yes
PowerEdge yx2x servers	No	No

NOTE: Only limited PowerEdge yx3x servers support VMware ESXi 7.0 U2. For the list of supported PowerEdge yx3x servers, see VMware vSphere 7.x on Dell EMC PowerEdge Servers Compatibility Matrix

Supported operating systems on Dell EMC Precision Rack System

The following table lists the operating systems that are supported on Dell EMC Precision Rack System.

Table 6. Supported operating systems on Dell EMC Precision Rack System

Dell EMC device	Supported operating system
R7920	Microsoft Windows 10 RS5 Microsoft Windows 10 Pro (20H2) Microsoft Windows 11 Red Hat Enterprise Linux 8.0 Ubuntu Desktop 20.04 LTS

System requirements

Following are the system requirements to install iDRAC Service Module:

- One of the supported operating systems. For the list of supported operating systems, see Supported operating systems.
- Minimum 2 GB RAM.
- Minimum 512 MB hard drive space.
- Administrator rights.
- The Remote Network Driver Interface Specification (RNDIS) capability for discovering a network device over USB.

Installing iDRAC Service Module

The iDRAC Service Module (iSM) can be installed on any of the following operating systems:

- Microsoft Windows
- Linux
- VMware ESXi

For the list of operating systems that are supported on iSM, see Supported operating systems.

ⓘ **NOTE:** From iDRAC Service Module version 4.x.x.x, the default USB NIC IP address set by iDRAC Service Module is 169.254.1.1.

Topics:

Initial installation of iDRAC Service Module through iDRAC Enterprise or Datacenter or iDRAC Express on Microsoft Windows and Linux

You can install iDRAC Service Module (iSM) from the iDRAC Enterprise or Datacenter or iDRAC Express interface. The installation procedure is same for installing iSM through iDRAC or iDRAC Express on Microsoft Windows and Linux operating systems. You can install iSM with a single-click using the iDRAC installer packager on the host operating system, rather than downloading the installer from the Dell EMC support site or the OpenManage DVD. Using this method ensures that you install a version of iSM that is compatible with your iDRAC firmware.

iSM must be installed on the host operating system. It is mandatory that an operating system is installed and running on the host device.

1. Start the virtual console.
2. Log in to the host operating system as an administrator.
3. From the device list, select the mounted volume that is identified by SMINST, and then click the corresponding script to start the installation. To install iSM, run the appropriate command for your system:

   For Windows: `ISM_Win.bat`

   For Linux: `sh ISM_Lx.sh` or `. ISM_Lx.sh`

   For Ubuntu: `bash ism_Lx.sh`

   After the installation is completed, iDRAC indicates that the iSM is installed and specifies the latest installation date.

   ⓘ **NOTE:** The installer is accessible by the host operating system for 30 minutes, within which you must start the installation operation. Otherwise, you have to restart the iDRAC Service Module Installer.

Installing iDRAC Service Module on Microsoft Windows operating systems

The iDRAC Service Module (iSM) installer for supported operating systems is available on the *Systems Management Tools and Documentation* DVD. You can also download the iSM installer from Dell.com/support.

You can perform a manual or an automated installation using appropriate command-line switches. You can install the iSM through the **push** mechanism using consoles like OpenManage Essentials (OME).

ⓘ **NOTE:** Perform the following steps only if a third-party PowerShell module path is missing in the operating system environment:

1. Browse to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard** is displayed.
2. Click **Next**.
   The **License Agreement** is displayed.
3. Read the software license agreement, select **I accept the terms in the license agreement**, and then click **Next**.
4. Select the **Setup Type** from the following options, and click **Next**:
   - **Typical** – All program features are installed (requires the most disk space).
   - **Custom** – Customize the installation by choosing the program features you want to install along with the location (recommended for advanced users).

   ⓘ **NOTE:** The following steps are applicable, only if you select the **Custom** option in the **Setup Type** window:

   ⓘ **NOTE:** By default, the **In-Band SNMP Traps, iDRAC access via Host OS, SNMP Get via Host OS, SNMP Alerts via Host OS, Enable WS-Man** features are not enabled.

   a. Choose the program features you want to install and click **Next**.
   The **Lifecycle Controller Log Replication** window is displayed.
   b. Specify the location where the Lifecycle Controller logs are to be replicated. By default, the **Typical (Windows Logs/ System)** option is selected and the Lifecycle Controller logs are replicated in the **System** group of the **Windows Logs** folder in the **Event Viewer**. Click **Next**.

   ⓘ **NOTE:** You can also create a custom group in the **Application and Services Log** folder by selecting the **Custom** option in the **Lifecycle Controller Log Replication** window.

   c. Select the authentication mode to enable WS-Man remotely and also choose to install a self-signed certificate if the authentication certificate is not found. Provide a WINRM port number to establish communication. By default, the port number is 5986.
5. To enable the **iDRAC access via Host OS** feature, provide a unique port number ranging from 1024 to 65535.

   ⓘ **NOTE:** If the port number is not provided, then 1266 or if there is an earlier configured port number available, that is assigned by default.

   The **Ready to Install the Program** window is displayed.
6. Click **Install** to continue the installation.

   You can also click **Back** to change the preferences.

   At times, although the iSM is installed, the following message is displayed in the host log file: **The communication between iDRAC Service Module and iDRAC could not be established. Refer to the latest iDRAC Service Module installation guide.** For more information about troubleshooting, see Frequently asked questions.

   At times, during the iSM installation, an alert message is displayed: **iDRAC Service Module Object has timed out. Please check iDRAC Service Module services has gracefully started.** This warning message is due to the delay in enablement of a USB NIC and the start of iSM service. It is recommended that the user must check that the status of iSM service after the installation is completed.

   The iSM is successfully installed.
7. Click **Finish**.

   On Microsoft Windows 2016 and Windows 2019 operating systems, the iDRAC USB NIC device description is displayed as **Remote NDIS Compatible Device**.

Silent installation of iDRAC Service Module on Microsoft Windows

You can install the iDRAC Service Module (iSM) using silent installation without an interactive console.

- To install iDRAC Service Module using silent installation, type `msiexec /i iDRACSvcMod.msi /qn` on the command prompt.
- To generate the install log files, type `msiexec /i iDRACSvcMod.msi /L*V` *<logname with the path>*
- To replicate the Lifecycle Controller logs in an existing group or a custom folder, type `msiexec /i iDRACSvcMod.msi CP_LCLOG_VIEW="`*<existing group name or custom folder name>"*
- To install the following feature using silent installation, type `msiexec /i` *<location of the installer file>*`/iDRACSvcMod.msi /qn ADDLOCAL=<xxxx>`

  NOTE: <XXXX> can be any feature that is mentioned in the following table. You can install more than one feature by using a comma. For example:

  ```
  msiexec /i <location of the installer file>/iDRACSvcMod.msi /qn ADDLOCAL=IBIA2,
  SupportAssist, SM
  ```

Table 7. Parameters and Features

Parameters	Features
`OSInfo`	Operating system information
`Watchdog`	Automatic system recovery
`LCLog`	Lifecycle log replication
`IBIA2`	iDRAC access via host operating system
`WMIPOP`	Windows Management Instrumentation (WMI) providers
`iDRACHardReset`	iDRAC hard reset
`SupportAssist`	SupportAssist
`iDRAC_GUI_Launcher`	iDRAC UI launcher
`FullPowerCycle`	Full power cycle
`SDSEventCorrelation`	SDS event correlation
`SM`	S.M.A.R.T monitoring
`OmsaSNMPTraps`	SNMP OMSA traps
`SWRAID`	Software RAID

- To install WS-Man, type `msiexec.exe /i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2" CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1" /qn`
- To view the UI in the supported languages, type `msiexec /i iDRACSvcMod.msi TRANSFORMS=` *<locale number>*`.mst`, where locale number is:

Table 8. Locale number and their supported languages

Locale number	Language
1031	German
1033	English (US)
1034	Spanish
1036	French
1041	Japanese
2052	Simplified Chinese

Modifying iDRAC Service Module components on Microsoft Windows operating systems

To modify iDRAC Service Module (iSM) components:

1. Go to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard** is displayed.
2. Click **Next**.
3. Select **Modify**.
4. Enable or disable features as required and then click **Next**.
   The **Lifecycle Controller Log Replication** window is displayed.
5. Specify the location where you need the LC log files to be replicated. By default, the **Typical (Windows Logs/System)** option is selected and the LC logs are replicated in the **System** group of the **Windows Logs** folder in the **Event Viewer**.
6. Click **Next**.

   NOTE: You can also create a custom group in the **Application and Services Log** folder by selecting the **Custom** option in the **Lifecycle Controller Log Replication** window.

   NOTE: You will have to restart the system in the following scenarios:

   - If you switch between **Typical (Windows Logs/System)** and **Custom** options.
   - If you switch from one custom folder to another folder.

   The **Ready to install** screen is displayed.
7. For iDRAC access via Host OS feature, provide a unique port number ranging from 1024 to 65535.

   NOTE: If the port number is not provided, then 1266 or if there is an earlier configured port available, that is assigned by default.

8. Click **Install** to continue the process.

   You can also click **Back** to change your preferences.

   iDRAC Service Module is successfully modified.
9. Click **Finish**.

Repairing iDRAC Service Module running on Microsoft Windows operating systems

If you want to repair the iDRAC Service Module (iSM) component that is faulty or nonfunctional:

1. Go to **SYSMGMT** > **iSM** > **Windows**, and then run `iDRACSvcMod.msi`.
   The **iDRAC Service Module - InstallShield Wizard** screen is displayed.
2. Click **Next**.
3. Select **Repair** and click **Next**.
   The **Ready to install** is displayed.
4. Click **Repair** to continue the process.

   You can also click **Back** to change your preferences.

   iDRAC Service Module component is successfully repaired.
5. Click **Finish**.

Uninstalling iDRAC Service Module running on Microsoft Windows operating systems

iDRAC Service Module (iSM) can be uninstalled using two different methods:

- Unattended uninstall using the product ID
- Uninstalling using the add or remove option

Unattended iDRAC Service Module uninstallation using the product ID

Type `msiexec /x {0F7BE359-142D-4AE4-A0E2-08187598F5CC} /qn` to uninstall iDRAC Service Module using the product ID.

Uninstalling iDRAC Service Module using the add or remove option

To uninstall iSM using the Add or Remove option from the control panel, go to **Start** > **Control Panel** > **Programs and Features**.

ⓘ **NOTE:** You can also uninstall by selecting **Uninstall** after running the `iDRACSvcMod.msi` command.

ⓘ **NOTE:** You can view the iSM log files in the **Application** group of the **Windows Logs** folder in the Windows **Event Viewer**.

Installing iDRAC Service Module on VMware ESXi

VMware ESXi is factory-installed on some systems. For a list of these systems, see the latest *Systems Software Support Matrix* at https://www.dell.com/support.

Preinstallation requirements for VMware ESXi

Before installing iSM on systems running supported VMware ESXi, ensure that VMware ESXi sfcbd-watchdog service startup policy is set to **Start and stop with host** option.

To check the VMware ESXi sfcbd-watchdog service startup policy configuration, complete the following steps:

1. Log in to the VMware ESXi host using your root credentials.
2. From the **Host** navigator menu, click **Manage**.
3. Click **Services** and select the **CIM Server** service name (also labeled as **sfcbd-watchdog**).
4. Click **Actions** and then click **Policy** from the drop-down list.
   The service policy options are listed.
5. Ensure that the policy is set to **Start and stop with host** option.

Installing iDRAC Service Module on VMware ESXi using CLI

iSM is available in a ZIP file for installing on systems running VMware ESXi. The ZIP file follows the naming convention `ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>i-Live.zip`, where <version> is the supported ESXi version.

The ZIP files for the supported ESXi versions are:

- For VMware ESXi 7.x: `ISM-Dell-Web-4.2.0.0-`*`<bldno>`*`.VIB-ESX7i-Live.zip`
- For VMware ESXi 6.x: `ISM-Dell-Web-4.2.0.0-`*`<bldno>`*`.VIB-ESX6i-Live.zip`

If VMware ESXi is not installed on your system, follow these steps to install iSM on VMware ESXi:

1. Copy iSM offline bundle ZIP file to the `/var/log/vmware` location on the host operating system.
2. Run the following command:
   - For VMware ESXi 7.x: `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`
   - For VMware ESXi 6.x: `esxcli software vib install -d /var/log/vmware/<iDRAC Service Module file>`

To upgrade the iSM on VMware ESXi, do the following:

1. Copy the iSM offline bundle ZIP file to the `/var/log/vmware` location on the host operating system.
2. Run the following command:
   - For VMware ESXi 7.x: `esxcli software component apply -d /var/log/vmware/<iDRAC Service Module file>`

- For VMware ESXi 6.x: `esxcli software vib update -d /var/log/vmware/<iDRAC Service Module file>`

The feature configuration of iDRAC Service Module is not retained as is after a forced or ungraceful reboot. A backup of the configuration files is created by the ESXi hypervisor through the `script /sbin/auto-backup.sh` that runs periodically every 60 minutes. If you want to retain the configuration, manually run the backup.sh script before you reboot the system.

NOTE: Reboot of the host operating system is not required after installing or uninstalling the iDRAC Service Module Live VIB package.

NOTE: On repository-based installs such as VMware Update Manager (VUM) and apt-repository, not all features are enabled by default.

Installing iDRAC Service Module using the vSphere CLI

To install the iSM software on VMware ESXi using the vSphere CLI, complete the following steps:

1. Copy the `ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>i-Live.zip` file to a directory on the system.
2. Shut down all guest operating systems on the ESXi host and put the ESXi host in maintenance mode.
3. If you are using vSphere CLI on Windows, go to the directory where you have installed the vSphere CLI utilities. If you are using vSphere CLI on Linux, run the following command from any directory:

   For VMware ESXi 7.x:

   ```
   esxcli --server <IP Address of ESXi 7.x host> software component apply -d /var/log/
   vmware/<iDRAC Service Module file>
   ```

   For VMware ESXi 6.x:

   ```
   esxcli --server <IP Address of ESXi 6.x host> software vib install -d /var/log/vmware/
   <iDRAC Service Module file>
   ```

   NOTE: The PL extension is not required if you are using the vSphere CLI on Linux.

4. Type the root username and password of the ESXi host when prompted.
   The command output displays a successful or a failed status.

Installing iDRAC Service Module using VMware Update Manager

To install iSM using VMware Update Manager (VUM), complete the following steps:

1. Install VMware vSphere 6.5 or later versions—vCenter Server, vSphere Client, and VMware vSphere Update Manager—on a supported Microsoft Windows operating system.
2. On the desktop, double-click **VMware vSphere Client** and log in to vCenter Server.
3. Right-click **vSphere Client host** and click **New Datacenter**.
4. Right-click **New Datacenter** and click **Add Host**. Provide information for the ESXi server as requested.
5. Right-click the **ESXi host** added in **step 4** and click **Maintenance Mode**.
6. From **Plug-ins**, select **Manage Plug-ins** > **download VMware Update Manager**. The status is enabled if the download is successful. Follow the instructions to install the VUM client.
7. Select the **ESXi host**. Click **Update Manager** > **Admin view** > **Patch Repository** > **Import Patches** and follow the online instructions to upload the patch successfully.
   The offline bundle is displayed.
8. Click **Baselines and Groups**.
9. Click **Create from Baselines** tab, enter the baseline name, select **Host Extension** as baseline type, and provide the requested information.
10. Click **Admin View**.
11. Click **Add to Baseline** against the uploaded patch name and select the baseline name that you created in step 8.
12. Click **Compliance view**.
13. Select the **Update Manager** tab.

14. Click **Attach** and select the **Extension Baseline** created in step 8 and follow the instructions.
15. Click **Scan**, select **Patches and Extensions** if not selected by default, and click **Scan**.
16. Click **Stage**, select created **Host Extension**, and follow the instructions.
17. Click **Remediate** and follow the instructions after the staging is completed.
    iSM installation is complete.

    For more information about VMWare Update Manager, see the VMWare website.

    ⓘ **NOTE:** You can install iSM from the VUM repository, vmwaredepot.dell.com/.

Upgrading iDRAC Service Module on VMware ESXi

To upgrade iDRAC Service Module using VMware Update Manager (VUM), complete the following steps:

1. Install VMware vSphere 6.5 or later versions (vCenter Server, vSphere Client, and VMware vSphere Update Manager) on a supported Microsoft Windows operating system.
2. On the desktop, double-click **VMware vSphere Client** and log in to vCenter Server.
3. Right-click **vSphere Client host** and click **New Datacenter**.
4. Right-click **New Datacenter** and click **Add Host**. Provide information for the ESXi server per online instructions.
5. Right-click the **ESXi host** added in **step 4** and click **Maintenance Mode**.
6. From **Plug-ins**, select **Manage Plug-ins** and click **Download VMware Update Manager**. (The status is enabled if the download is successful.) Follow the instructions to install the VUM client.
7. Select the ESXi host. Click **Update Manager** > **Admin view** > **Patch Repository** > **Import Patches** and follow the online instructions to upload the patch successfully.
   The offline bundle is displayed.
8. Click **Baselines and Groups**.
9. Click **create** from Baselines tab, mention baseline name, and select **Host Extension** as baseline type.

   ⓘ **NOTE:** Select the latest iDRAC Service Module version to create the baseline.

   Complete the rest as per instructions.
10. Click **Admin View**.
11. Click **Add to Baseline** (against the uploaded patch name) and select the baseline name that you have created in **step 8**.
12. Click **Compliance view**. Select the **Update Manager** tab. Click **Attach** and select the **Extension Baseline** created in **step 8** and follow the instructions.
13. Click **Scan** and select **Patches and Extensions** (if not selected by default) and click **Scan**.
14. Click **Stage**, select created **Host Extension** and follow the instructions.
15. Click **Remediate** and follow the instructions after the staging is completed.
    iDRAC Service Module upgrade is complete.

    ⓘ **NOTE:** The host operating system reboots while upgrading iSM using VMware Update Manager. For more information about VMware Update Manager, see the VMware official website.

    ⓘ **NOTE:** You can upgrade iDRAC Service Module from the VMware Update Manager repository vmwaredepot.dell.com.

Installing iDRAC Service Module using vSphere Lifecycle Manager in vSphere Client

ⓘ **NOTE:** Before installing, ensure that the downloaded iSM version is compatible with VMware ESXi 7.x.

To install iSM using vSphere Lifecycle Manager (vLCM) in vSphere Client (VC), complete the following steps:

1. Install vSphere Client (VCSA) on a supported Microsoft Windows operating system.
2. Log in to a vSphere Client using web.
3. Right-click **vSphere Client host**, and click **New Datacenter**.
4. Right-click **New Datacenter**, and click **Add Host**. Provide information for the ESXi server based on the online instructions.
5. Click **Menu** > **Lifecycle Manager** > **Settings** > **Patch Setup** > **NEW**, and enable the online repository.

6. Click **ACTIONS** and then click **Sync Updates**.
   iSM VIB is downloaded into VC.
7. Select the ESXi host. Click **Baselines** > **Attached Baselines** > **ATTACH** > **Create** > **Attach Baseline**, and follow the online instructions to upload the patch.
8. Click **STAGE** and follow the instructions.
9. After staging is complete, click **REMEDIATE** and follow the instructions.
   iSM installation is complete.

Using the Power CLI

To install the iSM using Power CLI, complete the following steps:

1. Install the supported PowerCLI of ESXi on the supported Microsoft Windows operating system.
2. Copy the `ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>i-Live.zip` file to the ESXi host.
3. Navigate to the bin directory.
4. Run Connect-VIServer and provide the server and other credentials.
5. Log on to the ESXi host using supported vSphere CLI of ESXi 6.x U3, or ESXi 7.x and create a datastore.
6. Create a folder **ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>I** on ESXi 6.x U3, or ESXi 7.x host under **/vmfs/volumes/<datastore_name>** directory.
7. Copy the ESXi ZIP file on ESXi 6.x U3, or ESXi 7.x host to **/vmfs/volumes/<datastore_name>ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>I** directory.
8. Unzip the ZIP file in the above specified directory.
9. Run the following command in Power CLI:

   For ESXi 7.x:

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>i/metadata.zip
   ```

   For ESXi 6.x:

   ```
   Install-VMHostPatch -VMHost <VMHost I.P address> - HostPath /vmfs/volumes/
   <datastore_name>name>/ISM-Dell-Web-4.2.0.0-<bldno>.VIB-<version>i/metadata.zip
   ```

10. Run the following command to verify if the iSM is installed successfully on the host:

    For ESXi 7.x: `esxcli software component get -n DEL-dcism`.

    For ESXi 6.x: `esxcli software vib get -n dcism`.

    iSM is displayed.
11. Reboot the host operating system after installing iSM using the above Power CLI command.
    For more information on Power CLI, see the VMware website.

Uninstalling iDRAC Service Module on VMware ESXi

To uninstall iSM on VMware ESXi, use the following command:

- For VMware ESXi 7.x: `esxcli software component remove -n DEL-dcism`
- For VMware ESXi 6.x: `esxcli software vib remove -n dcism`

Installing iDRAC Service Module on supported Linux operating systems

The complete iSM is packaged in a single Red Hat Package Manager (rpm). The package, which is accompanied by a shell script, can install, uninstall, or enable or disable the features available.

Before installing iSM, you must install the OSC package collector using `rpm -ivh dcism-osc*.rpm`.

As the installer on Linux is a single rpm install, there is no granular install support. You can enable or disable the features through the scripted installs only.

ⓘ **NOTE:** The installer is available for all iSM supported 64-bit versions of Linux operating systems.

Preinstallation requirements for Linux operating systems

To install iSM on systems running a supported Linux operating system, run the command `setup.sh`.

Ensure that the basic functional requirements are met, including:

- **OS to iDRAC Pass-through** is enabled automatically after installing iSM
- The IPv4/IPv6 network stack is enabled in the host operating system
- The USB subsystem is enabled
- `udev` is enabled; required to start iSM automatically

For more information about iDRAC, see the latest *Integrated Dell Remote Access Controller User's Guide* at Dell.com/support.

Linux install dependencies

The following are the list of dependent packages and executables that need to be installed to complete the installation.

Table 9. Linux install dependencies

Executable commands	Package name
/sys	fileSystem
grep	grep
cut, cat, echo, pwd,	coreutils
lsusb	usbutils
find	findutils
shell script commands	bash
ifconfig	net-tools
ping	Iputils
chkconfig	Red Hat Enterprise Linux ● chkconfig SUSE Linux Enterprise Server ● aaa_base
install_initd	Red Hat Enterprise Linux ● redhat-lsb-core SUSE Linux Enterprise Server ● insserv
systemctl	systemd
curl	libcurl
openssl	libssl

Installing the iDRAC Service Module on Linux operating systems

To install the iDRAC Service Module on Linux operating systems using the scripted install (`setup.sh`), complete the following steps:

1. Open the application and review the features that are displayed on the screen.

```
    [x] 1. Watchdog Instrumentation Service
    [x] 2. LifeCycle Log Information
    [x] 3. Operating System Information
    [ ] 4. iDRAC access via Host OS
            [ ] a. Access via GUI, WS-man, Redfish, Remote Racadm
            [ ] b. In-band SNMP Traps
            [ ] c. SNMP OMSA Traps
            [ ] d. Access via SNMP Get
    [x] 5. iDRAC SSO Launcher
            [x] a. Read only
            [ ] b. Administrator
    [ ] 6. Chipset S.M.A.R.T Monitoring
            [ ] a. Periodic S.M.A.R.T Log Collection
        7. iDRAC Hard Reset
        8. Support Assist
        9. Full Power Cycle
    [ ] 10. All Features
```

2. Type the number of each of the features you want to install and use comma to separate the numbers. For example, to install the subfeatures, type 4.a, 4.b, 4.c and so on.
3. Type **i** to install the selected features. If you do not want to continue the installation, type **q** to quit the installation.

   NOTE: After installing different features, you can also modify them.

4. To verify the iSM service status, run the command: `systemctl status dcismeng.service`.
   If iSM is installed and running, the status **running** is displayed.

   You must provide a unique port number in the range 1024 to 65535 if you want to install the **iDRAC access via Host OS** feature. If you do not provide a port number, *port number 1266* or a previously configured port (if any) is assigned by default. If OpenManage Server Administrator is already installed on port 1311, the same port cannot be used for iSM.

   When iSM 3.4.0 or later is installed on Linux operating systems, a gnome warning is observed similar to: *failed to rescan: Failed to parse /usr/share/applications/iDRACGUILauncher.desktop file: cannot process file of type application/x-desktop*.

   NOTE: When OSC package is already installed before iSM installation, the warning message `Package dcism-osc-* is already installed` is displayed. Make sure to uninstall the OSC package and then retry iSM installation.

Silent installation of iDRAC Service Module on Linux

You can install iSM silently in the background without a user console. This can be achieved by using `setup.sh` with parameters.

The parameters that can be passed to use `setup.sh` are:

Table 10. Silent installation parameters

Parameter	Description
-h	Help: Displays help
-i	Install: Installs and enables selected features
-x	Express: Installs and enables all available features
-d	Delete: Uninstalls iSM
-w	Watchdog: Enables the Watchdog instrumentation service
-l	Lifecycle Controller Log: Enables Lifecycle log information
-o	Operating system information: Enables operating system information

Table 10. Silent installation parameters (continued)

Parameter	Description
-a	Autostart: Starts the service after installing the iSM component
-O	iDRAC access via Host OS: Enables the iDRAC access user interface, WS-Man, Redfish, Remote RACADM
-s	Enables In-Band SNMP traps
-So	Enables SNMP OMSA Traps
-g	Enables access via SNMP Get
-Sr	Enables iDRAC SSO login as a read-only user
-Sa	Enables iDRAC SSO login as Administrator
-Sm	Enables Chipset S.M.A.R.T Monitoring
-Sp	Enables Periodic S.M.A.R.T Log Collection

ⓘ **NOTE:** On Linux operating systems, if a feature-modifying operation with silent option is enabled from the Linux web pack using setup.sh, then the previously enabled feature states are overridden by the new features you select during the modifying operation.

Uninstalling iDRAC Service Module on Linux operating system

iSM can be uninstalled using any of the following methods:

- Using uninstall script
- Using RPM command

Uninstalling iDRAC Service Module using the uninstall script

The command that is used for uninstalling the iSM is `dcism-setup.sh`. Run the shell command and select *d* to uninstall the iSM.

To uninstall the iSM on silent mode, run `./setup.sh -d`.

Uninstalling iDRAC Service Module using the RPM command

iSM can be uninstalled using the RPM command `rpm -e dcism` at the command line.

ⓘ **NOTE:** Uninstalling iSM using the `rpm -e dcism` command does not uninstall the OSC package that is installed by iSM. You can uninstall the OSC package using the `rpm -e dcism-osc` command.

Uninstalling iDRAC Service Module using the dpkg command

In the Ubuntu operating system, iSM can be uninstalled using the dpkg command `dpkg --remove dcism` at the command line.

You can uninstall the OSC package using the `dpkg --purge dcism-osc` command.

Installing iDRAC Service Module when System Configuration Lockdown mode is enabled in iDRAC

When the System Configuration Lockdown mode feature is enabled through iDRAC, no configuration operations can be performed for iSM. All the features that were enabled before the System Configuration Lockdown mode feature was turned on continue to be enabled. If iSM is installed after the System Configuration Lockdown mode feature is enabled, then only the iSM features that were enabled earlier are available for the users. Whenever the System Configuration Lockdown mode feature is turned off in iDRAC, then all the configuration operations can be performed.

Support for iDRAC URI to get iDRAC Service Module installer

You can download iSM web packages using the URL `https:// <iDRACIP>/software/ism/package.xml`. You can download the packages only when iSM LC DUP is uploaded and available in iDRAC. You can also load it in iDRAC by enabling the iDRAC LC autoupdate.

The following is a sample XML code with an Image filename mentioned to download the package.

```
<PayloadConfiguration>
<Image filename="OM-iSM-Dell-Web-LX-4.2.0.0.tar.gz" id="5DD5A8BA-1958-4673-
BE77-40B69680AF5D" skip="false" type="APAC" version="4.2.0.0"/>
<Image filename="OM-iSM-Dell-Web-LX-4.2.0.0.tar.gz.sign" id="E166C545-82A9-4D5D-8493-
B834850F9C7A" skip="false" type="APAC" version="4.2.0.0"/>
<Image filename="OM-iSM-Dell-Web-X64-4.2.0.0.exe" id="5015744F-F938-40A8-
B695-5456E9055504" skip="false" type="APAC" version="4.2.0.0"/>
<Image filename="ISM-Dell-Web-4.2.0.0-VIB-ESX6i-Live.zip" id="1F3A165D-7380-4691-
A182-9D9EE0D55233" skip="false" type="APAC" version="4.2.0.0"/>
<Image filename="RPM-GPG-KEY-dell" id="0538B4E9-DA4D-402A-9D96-A4A55EE2234C"
skip="false" type="APAC" version=""/>
<Image filename="sha256sum" id="06F61B54-58E2-41FB-8CE3-B7137A60E4B7" skip="false"
type="APAC" version=""/>
</PayloadConfiguration>
```

To download the packages, use the image filename present in the XML code to append to the URL. For example:

- Microsoft Windows web packages can be downloaded from `https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-X64-4.2.0.0.exe`.

VMware ESXi Live VIB package from Lifecycle Controller can be downloaded from `https://<iDRACIP>/software/ism/ISM-Dell-Web-4.2.0.0-VIB-ESX6i-Live.zip`.

Red Hat Enterprise Linux web pack can be downloaded from `https://<iDRACIP>/software/ism/OM-iSM-Dell-Web-LX-4.2.0.0.tar.gz`.

Support for idrac.local and drac.local as iDRAC FQDN

You can connect iSM to the iDRAC UI from the host operating system by typing `drac.local` or `idrac.local` in the web browser regardless of whether the host operating system supports multicast Domain Name System.

ⓘ **NOTE:** This feature is supported only over IPv4 address.

4

Configuring iDRAC Service Module

iDRAC Service Module features can be configured remotely using various iDRAC interfaces such as UI, CLI, and WS-Man.

Topics:

Configuring iDRAC Service Module from the iDRAC web interface

Log in to the iDRAC UI using the iDRAC IP address as a root or administrator user.

To use iSM from the iDRAC web interface for PowerEdge yx2x and yx3x servers, go to **Overview** > **Server** > **Service Module**.

To use the iSM from the iDRAC web interface for PowerEdge yx4x and yx5x servers, go to **iDRAC settings** > **Settings** > **iDRAC Service Module setup**.

Configuring iDRAC Service Module from RACADM

iSM can be accessed and configured through RACADM CLI commands. To verify the status of the features that are provided by iSM, use the `racadm get idrac.servicemodule` command. The features are:

- ChipsetSATASupported
- HostSNMPAlert
- HostSNMPGet
- HostSNMPOMSAAlert
- iDRACHardReset
- iDRACSSOLauncher
- LCLReplication
- OSInfo
- ServiceModuleEnable
- SSEventCorrelation
- WatchdogRecoveryAction
- WatchdogResetTime
- WatchdogState
- WMIInfo

To set or configure the features, use the command `racadm set idrac.servicemodule. <feature name> <enabled or disabled>`.

NOTE: Feature names and attributes that start with a # symbol cannot be modified.

To use iSM from RACADM, see the objects in the **Service Module** group in the *RACADM Command Line Reference Guide for iDRAC8, iDRAC9, and CMC* available at Dell.com/support.

Configuring iDRAC Service Module from WS-Man

iSM can be accessed and configured through WS-Man using the following command:

```
winrm i ApplyAttributes http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/
DCIM_iDRACCardService?
CreationClassName=DCIM_iDRACCardService+Name=DCIM:iDRACCardService+SystemCreationClassNam
e=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:{username} -p:{password}
-r:https://<Host IP address>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic
@{Target="iDRAC.Embedded.1";AttributeName="AgentLite.1#<feature>";AttributeValue="1"}
```

To use iSM from WS-Man, see the *Dell Lifecycle Controller 2 Web Services Interface Guide*. This guide provides information and examples for using WS-Man, and is available at Dell.com/support.

5

Security configurations and compatibility

iDRAC Service Module (iSM) is deployed with the default security configuration to protect against certain incidents like DLL hijacking, DLL tampering, information disclosure. This section briefs about the security configurations in iSM.

Topics:

- Enhanced security between iSM and iDRAC communication using the Transport Layer Security protocol
- Authenticate DLLs and shared objects before loading

Enhanced security between iSM and iDRAC communication using the Transport Layer Security protocol

Data communication between iSM and iDRAC uses Transport Layer Security (TLS) protected USBNIC INET sockets. This ensures protection of all the data that transports from iDRAC to iSM over USBNIC. iSM and iDRAC use self-signed certificates to control authentication. The self-signed certificates are valid for 10 years. New self-signed certificates are generated at each new installation of new iSM every time. Reinstall or upgrade the iSM when the certificates expire.

NOTE: iSM reinstall (repair) does not work on Linux operating systems. You must uninstall and then install iSM on Linux operating systems.

NOTE: When iSM's TLS-client certificate expires, communication between iSM and iDRAC fails and an operating system audit log is generated. You are then required to reinstall iSM on the host operating system.

Both iDRAC and the host TLS versions must be 1.1 or later. Communication between iSM and iDRAC fails if the TLS protocol version negotiation fails. If iSM with TLS capability is installed on an iDRAC firmware which does not support TLS communication over USBNIC, it will work with the non-TLS channel as in the earlier versions of iSM.

If iSM is installed or upgraded to version 3.4.0 or later before iDRAC is upgraded to version 3.30.30.30 or later, then iSM must be uninstalled and reinstalled to establish new TLS certificate. iSM with TLS capability is supported on iDRAC firmware versions 3.30.30.30 and later.

iSM without TLS capability does not function on a TLS-capable version of iDRAC firmware. For example, iSM 3.3 or earlier which are not TLS-capable is not supported on iDRAC firmware 3.30.30.30 and later. If iSM 3.3.0 is installed on iDRAC 3.30.30.30 firmware, multiple events with ISM0050 are observed in Lifecycle Controller log file.

NOTE: When Federal Information Processing Standards (FIPS) mode is enabled either on the host operating system or iDRAC, the communication between iSM and iDRAC is not established.

iSM support for TLS 1.3 protocol

Starting from iSM 4.2.0.0, iSM enables communication with iDRAC over the TLS 1.3 protocol. However, to successfully complete a handshake using TLS 1.3, the host operating system must support the TLS 1.3 version.

All iSM supported Linux operating systems (with OpenSSL version 1.1.1 or later) and Microsoft Windows Server 2022 support the TLS 1.3 protocol to communicate with iDRAC. If the host operating system does not support TLS 1.3 capability, iSM attempts communication with the TLS 1.2 protocol.

Table 11. TLS 1.3 protocol compatibility matrix

Products supporting TLS 1.3 protocol	Release version
iDRAC	5.10.00.00
iDRAC Service Module	4.2.0.0

The iDRAC has a web server setting to enable only the TLS 1.3 protocol. All the requests from clients with earlier versions of TLS 1.3 are not accepted. The following are some of the iSM features that are not supported with this configuration:

- Invoke-iDRAC GUI Launcher—This feature is functional when iDRAC is configured to support only the TLS 1.3 protocol and when the host operating system and the browser in the system support the TLS 1.3 protocol.
- In-Band iDRAC Access (operating system to iDRAC)—This feature is functional when iDRAC is configured to support only the TLS 1.3 protocol, and when the remote client (browser) also supports TLS 1.3 protocol.
- Autoupdate—This feature is functional when iDRAC is configured to support only the TLS 1.3 protocol and when the host operating system and the browser in the system support the TLS 1.3 protocol.

Policy settings for OS-BMC Passthrough on VMware ESXi

Following are the commands and the affected parameters of policy settings for OS-BMC Passthrough interface on VMware ESXi:

```
esxcli network vswitch standard portgroup policy security set -u -p "iDRAC Network"
```

Allow Promiscuous: false

Allow MAC Address Change: false

Allow Forged Transmits: false

```
esxcli network vswitch standard policy security set -v vSwitchiDRACvusb -f false -m false
```

Override vSwitch Allow Promiscuous: false

Override vSwitch Allow MAC Address Change: false

Override vSwitch Allow Forged Transmits: false

Authenticate DLLs and shared objects before loading

The secure loading of libraries in iSM prevent the attacks such as DLL hijacking, DLL preloading, and binary planting. To secure iSM from such attacks, this feature will not:

- load dynamic libraries from any arbitrary path.
- load any unsigned library.

This feature will do path verification and Authenticode signature check for DLLs and shared objects. And failure event is triggered in case of DLL and shared objects authentication failure. If the authentication validation do not succeed, the respective library is not loaded and is audited in the operating system log file.

6

Features

Using iSM, you can monitor and manage aspects of server performance including power cycle, security, alerts, also specific device management to optimize and maintain system health and availability.

ⓘ **NOTE:** **FullPowerCycle** and **SupportAssist on the Box** are supported only on PowerEdge yx4x and later servers.

Topics:

S.M.A.R.T monitoring

The S.M.A.R.T monitoring feature supports SATA hard drives enabled with SATA in AHCI mode and RAID mode. It has integrated capability to monitor S.M.A.R.T alerts through iDRAC supported auditing methods for hard drives under SATA chipset controller. Previously alerts were monitored by any open-source utility to monitor the hard drives set in RAID mode.

Table 12. Attribute values and description

Attribute Values	Description
Enabled	The chipset SATA controllers are monitored for S.M.A.R.T events in real time.
Disabled	S.M.A.R.T monitoring is disabled.
NA	Chipset SATA controller is not available.

ⓘ **NOTE:** By default, the S.M.A.R.T attribute is set to **Enabled** or **NA** when the configuration does not support chipset SATA.

S.M.A.R.T monitoring is a feature that is installed through the iSM installer. You can install or modify the iSM installer package to disable the S.M.A.R.T monitoring feature. This feature is available on a Dell EMC on supported SATA disk with S.M.A.R.T capabilities.

If the disk is S.M.A.R.T capable and the feature is enabled, iSM monitors the disks and generates events accordingly. The default monitoring period is 24 hours and cannot be manually configured. Only PDR16 (predictive failure) and PDR22 (temperature threshold exceeded) events are monitored.

If there is an operating system error due to a S.M.A.R.T error of the drive, then the event is not detected by the operating system. If hard drives are part of a storage pool, then iSM does not monitor the drives for S.M.A.R.T failures.

On PowerEdge yx3x servers, S.M.A.R.T monitoring using software RAID is applicable only for the PDR22 event.

ⓘ **NOTE:** S.M.A.R.T also requires iDRAC9 firmware 4.00.00.00 or later to be installed.

Operating system information

OpenManage Server Administrator currently shares operating system information and host name with iDRAC. The iDRAC Service Module (iSM) provides similar information such as host operating system name, server host IP address information, operating system version, and Fully Qualified Domain Name (FQDN) with iDRAC. The network interfaces on the host operating system are also displayed. By default, the monitoring feature is enabled. This feature is available even if OpenManage Server Administrator is installed on the host operating system.

You can also view host operating system network interface details, through the Redfish client plug-in for browsers.

ⓘ **NOTE:** The minimum iDRAC firmware version required to view information using the Redfish client is 3.00.00.00.

ⓘ **NOTE:** iSM is now supporting DHCP clients dhclient, dhcpd, wicked, netplan, and internal with Network Manager. If the network configuration on the host operating system is configured using any other DHCP clients, then iSM will be unable to monitor the network interface's change in states, for instance DHCP configuration of an interface. Hence, you may not be able to view the change of the host operating system network interface details like DHCP status, DHCP server, default gateway, DNS server in the iDRAC interfaces.

Lifecycle Controller log replication into operating system

Lifecycle Controller log replication replicates the Lifecycle Controller (LC) log files to the operating system log files. All events that have the operating system log option as the target in the Alerts page or in the equivalent RACADM or WS-Man interfaces are replicated in the operating system log files. This process is similar to the system event log (SEL) replication performed by OpenManage Server Administrator.

The default set of log files to be included in the operating system log files are the same as the logs configured for SNMP traps or alerts. However, the events logged in the Lifecycle Controller log file after the iSM is installed are replicated to the operating system log file. If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate SEL entries in the operating system log file.

In iSM, you can customize the location to replicate the Lifecycle Controller log files. By default, the Lifecycle Controller log files are replicated in the **System** group of the **Windows logs** folder in the Windows **Event Viewer**. You can replicate the Lifecycle Controller logs to an existing group or create a folder in the **Application and Services Logs** folder in the Windows **Event Viewer**. When iSM is already installed and if the host operating system undergoes a reboot or iSM is restarted, and iDRAC has some Lifecycle Controller log files that are generated during this period of host downtime, then iSM log files these Lifecycle Controller log files as past events in the operating system log file when the service starts.

ⓘ **NOTE:** You can choose the location to replicate the Lifecycle Controller log files only during iSM custom installation or iSM modification.

ⓘ **NOTE:** The source name of the iSM Lifecycle Controller log files has been changed from **iDRAC Service Module** to **Lifecycle Controller Log**.

Automatic system recovery

The automatic system recovery feature is a hardware-based timer, which is used to reset the server in the event of a hardware failure. You can perform automatic system recovery operations such as reboot, power cycle, or power off after a specified time interval. This feature is enabled only when the operating system watchdog timer is disabled. If OpenManage Server Administrator is installed, this monitoring feature is disabled to avoid duplicate watchdog timers.

You can configure three parameters in this feature from iDRAC interfaces:

1. **Watchdog state**: The default state is enabled when OMSA is not present, and when BIOS or operating system watchdog timer is disabled.
2. **Watchdog timeout**: The default value is 480 seconds. The minimum value is 60 seconds, and the maximum value is 720 seconds.
3. **Watchdog timeout Recovery Action or Auto Recovery Action**: The actions can be **Powercycle**, **Power Off**, **Reboot** or **None**.

NOTE: In Windows, when the DLL authentication failure event (SEC0704) is triggered, the Auto System Recovery Action set in the iSM settings page will be performed. iSM must be repaired or reinstalled to restore to the default state.

Windows Management Instrumentation Providers

Windows Management Instrumentation Providers available with iSM exposes hardware data through Windows Management Instrumentation (WMI). WMI is a set of extensions to the Windows Driver Model that provide an operating system interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF) to manage server hardware, operating systems, and applications. WMI Providers help to integrate with Systems Management Consoles such as Microsoft System Center and enable scripting to manage Microsoft Windows servers.

The namespace that is used is `\\root\cimv2\dcim`. The supported queries are **Enumeration** and **Get**. You can use any of the WMI client interfaces such as **winrm**, **Powershell**, **WMIC**, **WBEMTEST** to query the iDRAC supported profiles through the host operating system.

NOTE: When multiple WMI classes are simultaneously enumerated, the iSM might restart communication with the iDRAC. No action that is required.

Prepare to remove a NVMe PCIe SSD device

You can remove a Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) Solid-state device (SSD) without shutting down or rebooting the system. When you are removing a device, all the activities that are associated with the device must be stopped to prevent data loss. Stop any activities manually before performing the prepare to remove task. To prevent the loss of data, use the **Prepare to remove** option, after which you can remove the NVMe PCIe SSD physically. The prepare to remove operation does the validation, and checks if the device is busy with any activity or not. If the device is busy with an activity, the prepare to remove operation will not proceed.

Remote iDRAC hard reset

iDRAC may become unresponsive for various reasons. iSM can fully reset an unresponsive iDRAC8 or iDRAC9 controller by temporarily removing power to the iDRAC controller without affecting operating system production. This feature can only be disabled from the iSM page in iDRAC using the iDRAC interfaces.

To reset iDRAC, use the following Windows PowerShell or Linux shell command:

```
./Invoke-iDRACHardReset
```

NOTE: The shell command is supported only on VMware ESXi 7.x.

In all ESXi operating systems, you can perform the iDRAC reset remotely using the following WinRM remote command:

```
winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cimschema/2/root/cimv2/dcim/
DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:"root-
username" -p:"password" -r:https://"Host-IP":443/wsman -a:basic -encoding:utf-8
-skipCNCheck -skipCACheck -skipRevocationcheck
```

NOTE: The remote iDRAC hard reset feature only works with iDRAC8 on the PowerEdge yx3x or later servers and if logged into the operating system as an administrator.

iDRAC access via Host OS

Using PowerEdge Servers, you can manage the hardware or the firmware of a device through iDRAC by configuring an iDRAC dedicated network. Through the dedicated network port, you can access the iDRAC interfaces such as UI, WS-Man, RACADM, and the Redfish client.

The prerequisite to manage the hardware or the firmware is to have a dedicated connection between a device and the supported iDRAC interface. Using iDRAC access via Host OS, you can connect to an iDRAC interface from an operating system IP or host irrespective of the connection between a device and an iDRAC dedicated network. This feature allows you to monitor the hardware or firmware even if the iDRAC is not connected to the network.

You can select any of the following sub-features to enable the iDRAC access via the Host OS:

- **Access via GUI, WS-Man, Redfish, Remote RACADM**
- **In-Band SNMP Traps**
- **SNMP OMSA Traps**
- **Access via SNMP Get**

If you select **iDRAC access via Host OS**, all the subfeatures are selected by default. If you want to select any of the individual subfeatures, you can select a particular feature and enable it.

For more information, see iDRAC Access via Host operating system.

Accessing iDRAC via GUI, WS-Man, Redfish, and Remote RACADM

The **Access via GUI, WS-Man, Redfish, Remote RACADM** feature enables a host operating system administrator to access iDRAC interfaces remotely through the host operating system. Type the URL `https:// <Host OS IP Address>:<ListenPortNumber>` in the browser of the remote management station to access the iDRAC UI.

NOTE: The ListenPortNumber is the port number that is configured while enabling the iDRACAccessviaHostOS feature in iSM.

In-Band support for iDRAC SNMP alerts

All events that have the **SNMP Trap** option as the target in the Alerts page or in the equivalent RACADM or WS-Man interfaces can be received as the SNMP trap through the operating system using iSM. For iDRAC firmware 3.0.0 or later, this feature does not require the iSM LCL replication feature to be enabled. Only the events logged in the Lifecycle Controller log file after iSM is installed are sent as SNMP traps.

Using iSM, you can receive SNMP alerts from the host operating system similar to the alerts that are generated by iDRAC.

By default this feature is disabled. Though the In-Band SNMP alerting mechanism can co-exist with the iDRAC SNMP alerting mechanism, the recorded logs may have redundant SNMP alerts from both sources. It is recommended to either use the in-band or out-of-band option, instead of using both.

NOTE: You can use the In-Band SNMP feature on PowerEdge yx3x or later servers with a minimum iDRAC firmware version 2.30.30.30.

For more information, see In-Band iDRAC SNMP Alerts.

Mapping iDRAC Lifecycle Logs to OMSA and OMSS SNMP alerts

The ability to map iDRAC Lifecycle logs to OMSA and OMSS SNMP alert is disabled by default and can be enabled only when the existing Host SNMP Alerts feature is enabled. Configure the feature using either the iDRAC RACADM interface or the iSM Installer **Modify** option. When enabled, the feature converts iDRAC Lifecycle logs records selected as SNMP alerts into corresponding OMSA and OMSS SNMP alerts. The resulting OMSA or OMSS alert Object Identifier (OID) corresponds to the OMSA or OMSS product, and the rest of the alert varbinds are those of the iDRAC.

The iSM SNMP subagent forwards the mapped alerts to the SNMP trap destination configured on the host operating system. iSM does not add or modify any trap destination that is configured by the administrator, and does not create any outbound firewall rules to open User Datagram Protocol (UDP) ports corresponding to SNMP traps.

When the Host SNMP OMSA Alerts feature is disabled, the existing feature of forwarding iDRAC LifeCycle Logs as SNMP traps is active. The following table indicates the various feature states:

Table 13. OMSA and OMSS SNMP alert feature states

iDRAC.ServiceModule. HostSNMPAlert	iDRAC.ServiceModule. HostSNMPOMSAAlert	Remarks
Yes	Yes	iDRAC to OMSA SNMP map is trapped and sent to destination.
Yes	No	Only iDRAC alerts are sent to destination (default condition).
No	Yes	NA
No	No	No alert is mapped and sent to any destination.

iSM auto disables this new feature when it detects the OMSA service running on the host operating system to avoid duplicate traps at the trap destination.

Based on the above feature configuration, iSM forwards the received iDRAC alert to the trap destination having any of the following Object Identifiers:

- iDRAC Enterprise Object Identifier (existing feature)
- OMSA/OMSS Enterprise Object Identifier (introduced from iSM 4.1.0.0 onwards)

NOTE: If iSM 4.2.0.0 is installed with iDRAC firmware version 4.40.10 or older, where the OMSA and OMSS alert mapping is not supported by iDRAC interfaces (RACADM, iDRAC UI), this feature can be enabled or disabled only using the iSM installer.

Enable WS-Man remotely

With the WMI information feature, you can connect to the host Microsoft Windows WMI namespace to monitor system hardware. The WMI interface on the host is enabled by default, and you can access it remotely. However, if you want to access the WMI interfaces using WINRM's WMI adapter, you must enable it manually as it is not enabled by default. Using this feature, you can access the WINRM WMI namespaces remotely by enabling it during installation.

This feature can be accessed using PowerShell commands. The commands that are used are as follows:

Table 14. Enable WS-Man remotely

Command	Description
`Enable-iSMWSMANRemote –Status enable –Forcereconfigure yes –Createselfsigncert yes –IPAddress <IP address> –Authmode Basic, Kerberos, Certificate`	Enabling and configuring the remote WS-Man feature
`Enable-iSMWSMANRemote –Status get`	Viewing the status of remote WS-Man feature
`Enable-iSMWSMANRemote –Status disable`	Disable remote WS-Man feature
`Enable-iSMWSMANRemote –Status enable –Forcereconfigure yes –Createselfsigncert yes –IPAddress <IP address>`	Reconfigure the remote WS-Man feature

NOTE: You must have a server authenticating certificate and an https protocol to work with this feature.

Autoupdating iSM

You can autoupdate iSM using the iDRAC autoupdate process.

ⓘ **NOTE:** If iDRAC autoupdate is enabled, iSM LC DUP must be updated to the latest version from Dell.com/support.

ⓘ **NOTE:** You do not have to download the updates from support.dell.com. The updated iSM package is locally available in iDRAC.

ⓘ **NOTE:** iSM LC DUP in iDRAC is removed when the iDRAC LC Wipe option is used. You must download the iSM LC DUP from Dell.com/support.

Table 15. Commands to install and update iSM

Commands to run in the command prompt	Descriptions
`dcism-sync.exe`	To install or update iSM. Complete the steps in the installation wizard.
`--help/-h`	To display the help content.
`--silent/-s`	To do silent install or update.
`--force/-f`	To uninstall the current version and install the update package available in Lifecycle Controller. ⓘ **NOTE:** This option overwrites the previous configuration.
`--get—version/-v`	To get details about the update package version and the installed version of iSM
`--get—update/-g`	To download the iSM update packages to the user specified directory
`dcism-sync.exe —p "feature"`	To install specific features, the same as CLI arguments used with `msiexec.exe`. For example, to install iDRAC access via Host OS iDRAC feature on Windows, type `dcism-sync.exe -p "ADDLOCAL=IBIA"`.

FullPowerCycle

FullPowerCycle is a calling interface function that provides a way to reset the server auxiliary power. An increasing amount of server hardware runs on server auxiliary power. Troubleshooting of some server issues requires you to physically unplug the server power cable to reset the hardware running on auxiliary power.

The FullPowerCycle feature enables the administrator to connect or disconnect auxiliary power remotely without visiting the data center. This feature is supported on PowerEdge yx5x servers.

When a FullPowerCycle **Request** is issued through this interface, system power is not immediately affected. Instead, a flag is set that is queried when the system transitions to S5. For the FullPowerCycle feature to take effect, after issuing the request command you must also issue system shutdown command. If the flag is set on S5 entry, the system is temporarily forced into a lower power state, similar to removing and replacing AC. The flag can be cleared using the **Cancel** function anytime the system is in the S0 state prior to the system entering the S5 state.

You can avail different options of FullPowerCycle on your system. Use the following commands to request, get status, and cancel the FullPowerCycle on your system:

For Windows Operating systems, shortcut menus are available for the FullPowerCycle Activate (request), FullPowerCycle Cancel, and FullPowerCycle get status operations.

Table 16. FullPowerCycle commands for Windows operating system

Commands to run in the power shell console	Descriptions
`Invoke-FullPowerCycle — request`	To request FullPowerCycle on your system.

Table 16. FullPowerCycle commands for Windows operating system (continued)

Commands to run in the power shell console	Descriptions
	ⓘ **NOTE:** A message is displayed that the VirtualAC Power Cycle operation is triggered by the server operating system.
`Invoke-FullPowerCycle - get status`	To get the status of the FullPowerCycle on your system. ⓘ **NOTE:** A message is displayed that the system is going for turn off at the scheduled date and time.
`Invoke-FullPowerCycle - cancel`	To cancel the FullPowerCycle on your system.

For Linux and VMware ESXi operating systems, shortcut menus are available for the FullPowerCycle Activate (request), FullPowerCycle Cancel and FullPowerCycle get status operations.

Table 17. FullPowerCycle commands for Linux and VMware ESXi operating system

Commands to run in the power shell console	Descriptions
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle request`	To request FullPowerCycle on your system.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle cancel`	To cancel the FullPowerCycle on your system.
`/opt/dell/srvadmin/iSM/bin/Invoke-FullPowerCycle get-status`	To get FullPowerCycle status on your system.

The following messages are displayed after each successful FullPowerCycle operation on operating system log files and LCL:

Request message: `"The Full Power Cycle operation is triggered by the server operating system (OS) user <user name> from the OS on date <date>. However, the server components will be AC power cycled when the server is shut down".`

Cancel Message: `"The Full Power Cycle operation is successfully cancelled by the server operating system (OS) user <user name> from the OS on date <date>".`

ⓘ **NOTE:** The FullPowerCycle feature is available for ESXi 7.x operating system, but not for ESXi 6.x operating systems.

ⓘ **NOTE:** The FullPowerCycle feature can be used only with local or domain administrator, or root or sudo users.

SupportAssist on the box

SupportAssist saves time and streamlines technical support cases. A collection based on an event creates an open service request with SupportAssist. Scheduled collections help to monitor and maintain your environment. These collections include hardware information data, RAID controller log files, operating system, and application data. The features that are supported are :

- **SupportAssist Registration**—iSM supports SupportAssist Registration. This is a one time activity. You can enter the required details such as name, email, address, and number to complete the registration.
- **SupportAssist Collection**—The SupportAssist Collection feature in iDRAC collects information about the hardware, operating system, and relevant application data and compresses this information.

SupportAssist also provides:

- Proactive issue identification
- Automated case creation
- Support contact initiated by a Dell technical support agent

ⓘ **NOTE:** You must complete the registration to take advantage of SupportAssist.

You can view the following items in the SupportAssist dashboard.

Service Request Summary

In the Service Request Summary session, you can view the details of the following requests:

- Open
- Closed
- Submitted

Support Assist Overview

You can view the **Service Contract** details such as Contract Type and Expiration Date and the **Automatic Collection** settings details in this session.

On the **Service Requests** tab, you can also view the list of requests that are created and the status, description, source, service request ID, date opened, the date closed, and so on.

If you click the **Collection Log** tab, you can view the collection time, job ID, collection type, data that is collected, collection status, sent time, and so on.

> **NOTE:** When you manually initiate SupportAssist collection from iDRAC, the USB mass storage device is not exposed to the host operating system. The transfer of operating system collector files and the collected log files is handled internally between iDRAC and iSM.

> **NOTE:** The operating system and application data collection on ESXi is supported only by yx4x and later PowerEdge servers.

SupportAssist registration

Before you begin the registration process, ensure that iSM is installed and running in the host operating system, and a working internet connection is available.

1. Log in to iDRAC.
2. From the **Maintenance** drop-down menu, select the **SupportAssist** feature.
   The **SupportAssist Registration** wizard is displayed.
3. On the **Welcome** tab, click **Next**.
4. On the **Contact and Shipping Info** tab, provide your primary contact information such as **First Name**, **Last Name**, **Phone Number**, **Alternate Number**, **Email Address**, **Company Name**, **Address Line 1**, **Address Line 2**, **City**, **State**, **Zip Code**, and **Country**.

   > **NOTE:** You can add the secondary contact information, by clicking the **Add Secondary Contact Information** option.

   > **NOTE:** To continue with the registration, you must fill all the mandatory information required.

5. After filling the contact and shipping information, click **Next**.
6. Read the software license agreement, select **I accept the terms of the license agreement**, and then click **Register**.

   > **NOTE:** It might take few minutes to complete the registration process. After the registration is completed successfully, you will receive a welcome email from SupportAssist at the specified email address.

7. On the **Summary** tab, view the **Registration ID** and **Automatic Features** current setting details.
8. To close the **SupportAssist Registration** wizard, click **Close**.

   In the SupportAssist page, if you navigate to the bottom you can view the contact information.
9. Click the **Edit** option to make any changes in the primary or secondary contact information.
10. Click **Save** to apply the changes.

SupportAssist Collection

The SupportAssist Collection feature in iDRAC collects information about the hardware, operating system, and relevant application data, and compresses the information being collected. Run the operating system Collector tool manually to generate the SupportAssist Collection report. Using iDRAC Service Module, the operating system Collector tool automatically collects relevant operating system and hardware information. Automatic Support Log collection includes operating system and application information collection.

Using iDRAC Service Module, you can reduce the number of manual steps required to collect the Dell Technical Support Report as the collection process is automated.

Data to Collect

SupportAssist automatically creates and sends a collection to Dell Technical Support when there is an event-based trigger or where you have configured a scheduled cadence. You can collect the following type of information:

- **System Information**
- **Storage Logs**
- **OS and Application Data**
- **Debug Logs**

You can also perform the SupportAssist Collection function from an operating system shell to a specified file path using:

```
./ Invoke-SupportAssistCollection [--filepath/-f]
```

ⓘ **NOTE:** This shell command is only supported on iDRAC9 in the PowerEdge yx4x and later servers and if logged into the operating system as an administrator.

ⓘ **NOTE:** On Windows Core operating system, you must go to the absolute path to run the `Invoke-SupportAssistCollection.exe` command.

Collection preferences

You can select or set the collection preferences using the collection preferences feature. You can select any of the following types of collection preferences to save collection reports:

- **Send Now**—You will get a notification that **The job has been successfully added to the job queue** after you click the **Collect** option.
- **Save Locally**
- **Save to Network**—If you select this option, you must provide **Network Settings** details such as **Protocol**, **IP Address**, **Share Name**, **Domain Name**, **User Name**, and **Password**.

You can select any of the collection preferences and click **Collect** to receive the data.

ⓘ **NOTE:** This feature is available by default when you install iDRAC Service Module 2.0 or later versions on systems running supported Microsoft or Linux operating systems. You cannot disable the feature.

ⓘ **NOTE:** The operating system and application data collection on VMware ESXi is supported by PowerEdge yx4x and later servers only.

Anonymous collection of reports

You can perform SupportAssist Collection and upload operations without completing the registration process. Until iDRAC Service Module version 3.0.2, the registration was a prerequisite to perform SupportAssist Collection.

The supported iDRAC firmware for the anonymous collection is iDRAC 3.15.15.15 in PowerEdge yx4x and yx5x servers, and 2.60.60.60 in PowerEdge yx3x servers.

ⓘ **NOTE:** You can perform Anonymous SupportAssist Collection upload using a blank username or password in a proxy environment on PowerEdge yx3x servers.

Correlation of software events to hardware failures for Microsoft SDS

The event log files for hardware storage pool alerts or events are monitored by iSM with the server storage correlation feature. The server storage subsystem is monitored when Dell EMC storage controllers are used in RAID mode. But in Storage Spaces (SS) or Storage Space Direct (S2D), the server storage subsystem is monitored in a passthrough mode, or the SATA chipset is used to create the storage pool. With this feature, hardware-defined alerts that are covered by the Lifecycle Controller (LC) log and software-defined alerts that are covered by operating system log files are merged, and the alerts are registered in the iDRAC Lifecycle log files.

This feature is installed with the iSM package and will be enabled by default. You can change the preferences in the iDRAC settings. As part of the monitoring, iSM will audit the log files for potential failures and warnings. iSM will embed the SS correlation events on the host to an equivalent Lifecycle Controller event. The SSLCMAP should only reach the Lifecycle log files and SupportAssist alert. You cannot configure the SSLCMAP to any other alert destination in iDRAC .

The following are the prerequisites for S2D log collection:

- The SS event correlation feature must be enabled in the service module page in the iDRAC UI.
- The PII filter must be disabled in the service module page in the iDRAC UI.

Table 18. Windows Event Message mapped under LC logs monitored under S2D event correlation

Windows event source—SourceID	Windows event message	Mapped on iDRAC LC log
StorageSpaces—drivers—100	Physical drive %1 failed to read the configuration or returned corrupt data for storage pool %2. As a result the in-memory configuration might not be the most recent copy of configuration. Return code: %3	**MessageID** : SDS0001
StorageSpaces—drivers—102	Most of the physical drives of storage pool %1 failed a configuration update, which caused the pool to go into a failed state. Return code: %2	**MessageID** : SDS0002
StorageSpaces—drivers—103	The capacity consumption of the storage pool %1 has exceeded the threshold limit set on the pool. Return code: %2	**MessageID** : SDS0003
StorageSpaces—drivers—200	Windows was unable to read the drive header for physical drive %1. If you know that the drive is still usable, then resetting the drive health by using command line or UI may clear this failure condition and enable you to reassign the drive to its storage pool. Return code: %2	**MessageID** : SDS0004
StorageSpaces—drivers—203	An I/O failure has occurred on physical drive %1. Return code: %2	**MessageID** : SDS0005
StorageSpaces—drivers—300	Physical drive %1 failed to read the configuration or returned corrupt data for storage space %2. As a result the in-memory configuration may not be the most recent copy of configuration. Return code: %3	**MessageID** : SDS0006
StorageSpaces—drivers—301	All pool drives failed to read the configuration or returned corrupt data for storage space %1. As a result the storage space will not attach. Return code: %2	**MessageID** : SDS0007
StorageSpaces—drivers—302	Most of the pool drives hosting space metadata for storage space %1 failed a space metadata update, which caused the storage pool to go to failed state. Return code: %2	**MessageID** : SDS0008
StorageSpaces—drivers—303	Drives hosting data for storage space have failed or are missing. As a result, no copy of data is available. Return code: %2	**MessageID** : SDS0009
StorageSpaces—drivers—304	One or more drives hosting data for storage space %1 have failed or are missing. As a result, at least one copy of data is not available. However, at least one copy of data is still available. Return code: %2	**MessageID** : SDS0010

Table 18. Windows Event Message mapped under LC logs monitored under S2D event correlation (continued)

Windows event source—SourceID	Windows event message	Mapped on iDRAC LC log
StorageSpaces—drivers—306	The attempt to map, or to allocate more storage for, the storage space %1 has failed. This is because there was a write failure that is involved in the updating the storage space metadata. Return code: %2	**MessageID** : SDS0011
StorageSpaces—drivers—307	The attempt to unmap or trim the storage space %1 has failed. Return code: %2	**MessageID** : SDS0012

NOTE: The *Event and Error Message Reference Guide* provides information about the event and error information that is generated by firmware and other agents that monitor system components.

NOTE: PPID field is not recorded for alerts corresponding to a storage pool. iSM will replicate these alerts into the Lifecycle Controller log files in iDRAC with PPID as "NA".

Storage Spaces Direct log files collection with SupportAssist Collection

SupportAssist Collection (SAC) request will collect and package Storage Spaces Direct (S2D) log files. This feature is available only on Microsoft Windows operating system. The SDS Event Correlation feature must be enabled for SAC to include this log collection report.

S.M.A.R.T log files for disks and chipset into SupportAssist Collection report

iDRAC Service Module (iSM) collects the S.M.A.R.T log data from the SATA chipset driver when the SupportAssist Collection (SAC) is requested in real time.

This feature requires the **S.M.A.R.T monitoring** feature to be enabled in iSM, and **Storage Logs** under SupportAssist Collection preferences is enabled in iDRAC.

Historic S.M.A.R.T log

Historic S.M.A.R.T log files are collected from a SATA controller driver chipset or a Windows software RAID controller device every 24 hours, if this feature is enabled. The historic S.M.A.R.T log files are collected in a scheduled interval in iSM and sent to iDRAC. iDRAC bundles these historic S.M.A.R.T log files as part of the SupportAssist Collection you configure. Historic S.M.A.R.T log files are enabled or disabled by using the iSM installer or dcismcfg CLI.

NOTE: This feature requires iDRAC9 firmware 4.40.00.00 and later.

In SupportAssist Collection, these log files are available at `\tsr\storagelog\Smartlogs-nightly.zip`.

The filenames of earlier S.M.A.R.T. log files that are provided by iDRAC Service Module consists of the hostname as a prefix followed by an alphanumeric value. For example, HostRD20200414.json.

iDRAC Service Module CLI tool—dcismcfg

The dcismcfg utility is used to enable or disable the Historic S.M.A.R.T log collection feature. This utility is supported on all operating systems. Once the utility is used to enable or disable the Historic S.M.A.R.T log collection feature, the next polling cycle of S.M.A.R.T Monitoring fulfills the request.

Run the following commands to enable or disable the Historic S.M.A.R.T log collection:

For Windows run either one of the following commands:

-
  ```
  <iSM install path>/shared/bin/dcismcfg.exe --collectperiodicsmartlog true/false
  ```

-
  ```
  <iSM install path>/shared/bin/dcismcfg.exe -c true/false
  ```

For Linux run either one of the following commands:

-
  ```
  <iSM install path>/bin/dcismcfg --collectperiodicsmartlog true/false
  ```

-
  ```
  <iSM install path>/bin/dcismcfg -c true/false
  ```

dcismcfg utility must run as an administrator or root user and is supported for iDRAC firmware version 4.40.00.00 and later.

> **NOTE:** Historic S.M.A.R.T log collection is a subfeature of S.M.A.R.T Monitoring feature. However, while enabling Historic S.M.A.R.T log collection, if S.M.A.R.T Monitoring feature is not enabled, you are prompted to enable S.M.A.R.T Monitoring in order to enable Historic log collection.

SupportAssist Collection settings

To open the SupportAssist Collection Settings page, go to the SupportAssist dashboard in iDRAC and select **Settings** from the drop-down menu.

iSM 3.4.0 or later supports filter and nonfilter **OSApp Collection** (operating system and Application Data collection) on ESXi. This selection can be made from **Collection Preferences**.

A nonfiltered selected Collection contains **vmsupport** log files for **Logs**, **Network**, **Storage**, **Configuration**, **Installer**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines**, and **hostProfiles**.

A filtered selected Collection contains **vmsupport** log files for **Storage**, **Configuration**, **Installer**, **HungVM**, **PerformanceSnapshot**, **VirtualMachines**, and **hostProfiles**.

Set Archive directory

You can store the copies of collections that are performed by SupportAssist into a directory. Click the **Set Archive Directory** button to set the location.

Identification information

You can include the identification information in the data that is sent by clicking the drop-down menu and selecting **No** or **Yes**.

Email notifications

You can set email notification preferences when a new support case is opened or a new SupportAssist collection is uploaded. From the **Receive Email Notifications** drop-down menu, select **No** or **Yes**.

You can also select the language preference. The available languages are:

- **English**
- **German**
- **French**
- **Japanese**
- **Spanish**
- **Simplified Chinese**

Automatic collection

By default, the automatic collection feature is enabled. To disable this feature, use the drop-down menu to select either **Enable** or **Disable**.

You can also specify the time for scheduled collection by selecting any of the following options from the **Schedule automatic collections** drop-down menu:

- **Weekly**

- **Monthly**
- **Quarterly**
- **Never**

You can also set the automatic collection as recurring.

To view the ProSupport Plus Recommendations report, select **Yes** from the **Send ProSupport Plus Recommendations Report** drop-down menu.

After selecting your preferences, click **Apply** to save the changes.

iDRAC Service Module SupportAssist disk Auto Dispatch

If the server encounters a **PDR16 and PDR63**, Dell EMC support emails you notice of the predictive failure or a bad disk block on an SSD subject to the prevailing licensing terms and conditions. Once you receive the email, you must follow up and provide the service address to Dell EMC support for the delivery of the dispatched parts.

Configuring the In-Band SNMP Get feature—Linux

Install and configure **net-snmp** package to accept SNMP requests from remote systems. This feature is disabled by default.

To install the In-Band SNMP get feature through setup.sh installer, complete the following tasks:

1. To start the iSM installation, execute `./setup.sh` at the command line.
2. Read and accept the license agreement to proceed with the installation.
   A list of feature is displayed.
3. To select the **Access via SNMP Get** sub-option under the **iDRAC access via Host OS** feature, enter **4.c** , and press **Enter**.
4. After the feature is enabled, enter **I** and press **Enter**, to start the installation process of the selected features.
5. After the installation is completed, start the iDRAC Service Module process.

   If the SNMP Agent service is not enabled on iDRAC, iSM configures and enables the SNMP Agent.
6. To view the SNMP Agent properties, go to **Settings** on the iDRAC GUI.
7. Click **iDRAC Service Module Setup**.
8. Under **Monitoring** session, verify that **SNMP Get via Host OS** option is enabled.
9. Open a new '**PuTTY Configuration**' window, provide your Host Name IP address and click **Open**.
10. Click **Yes**, to enable the **PuTTY Security Alert**.
11. Log in to iDRAC using the proper credentials.
12. Type `racadm get iDRAC.ServiceModule.HostSNMPGet` and enter.
    Verify that **HostSNMPGet** is enabled.

    If the In-Band SNMP Get feature is not enabled during iDRAC Service Module installation, you can enable it using the following iDRAC UI or the RACADM commands:

    - Through the iDRAC UI—**iDRAC Settings->Settings->iDRAC Service Module Setup->Enable SNMP Get via Host OS->Enable or Disable**
    - Through the RACADM—**racadm set idrac.servicemodule.HostSnmpGet "Enabled" or "Disabled"**

    NOTE: iDRAC UI or RACADM commands for the In-Band SNMP Get feature are applicable only for PowerEdge yx4x and yx5x servers. On PowerEdge yx3x servers, you must use the iSM installer for enabling and disabling this feature.

    When the SNMP Get feature is enabled, it creates an iDRAC account **iSMSnmpUse**r for SNMPv3 support internally. If the account already exists, iSM logs the following error message and the feature is disabled.

    ```
    Unable to create the user \"iSMSnmpUser"\ on iDRAC because the username already
    exists. The SnmpGet via Host OS feature will be disabled.
    ```

    In such cases, you must remove the "iSMSnmpUser" in iDRAC and disable and enable the **Enable SNMP Get via Host OS** feature on iDRAC UI once again. The iSMSnmpUser account created by iSM is deleted when the feature is disabled or iSM is uninstalled. The SNMP Get feature will not work when there are maximum number of iDRAC accounts created (16) and there are no further slots.

Configuring the In-Band SNMP Get feature—Windows

The In-Band SNMP Get feature allows you to query the system management data over the SNMP service on the host operating system. The host SNMP services must be enabled and configured as a prerequisite for this feature.

The SNMP service on the iDRAC must be enabled. If it is not enabled, then iDRAC Service Module will enable and configure the SNMP service on the iDRAC. This feature can be enabled or disabled using any of the iDRAC interfaces or the installer.

This feature supports SNMP v1 and v2 on Microsoft Windows operating systems and SNMP v1, v2, and v3 on Linux operating systems.

NOTE: iDRAC UI or RACADM commands for In-Band SNMP Get feature is applicable only for yx4x and later PowerEdge servers.

NOTE: iDRAC Service Module supports only the iDRAC SNMP OID 1.3. 6.1. 4.1.674.10892.5.

iDRAC GUI Launcher

Using iDRAC Service Module 3.1 or later, you can launch iDRAC UI from your local system. Double-click the **iDRAC GUI Launcher** icon. The iDRAC UI log in page opens in the default browser. Use your iDRAC credentials to log in to the iDRAC home page. This is supported only on the Microsoft Windows operating systems. The shortcut is available on the start menu after the successful installation of iSM 3.1 or later.

NOTE: When the iSM is disabled, the iDRAC GUI Launcher icon is also disabled.

NOTE: If the default browser proxy is set to use the system proxy, then you will see a failure to launch the iDRAC UI. You must copy the IP address from the address bar and enter it in the exceptions list of 'proxy settings'.

Single sign-on to iDRAC UI from host operating system administrators desktop

Overview

Host administrators can launch iDRAC from within the host operating system using IPv6. iDRAC SSO launcher requires a desktop environment like GNOME or K Desktop Environment(KDE) on the host operating system.

.

NOTE: Nonadministrators cannot access this feature on the host operating system.

The single sign-on (SSO) feature enables an authenticated operating system administrator to directly access the iDRAC web interface without requiring log in using separate iDRAC administrator credentials. After installing this feature, a **Program Menu** shortcut called **Invoke-iDRACLauncher** on Microsoft Windows operating systems is created. On the Linux operating system, iSM creates a shortcut under **Applications** which you can double-click to launch the iDRAC dashboard. iSM provides a command-line interface that is called **Invoke-iDRACLauncher** on Microsoft Windows operating systems and **Invoke-iDRACLauncher.sh** on Linux operating systems.

You can configure the iDRAC Service Module using the IPv6 address. By default, communication is established through IPv4. Upon failure, the communication is reattempted over IPv6. An error message is audited when the communication fails.

You can update the IPv6 address using **RACADM-passthru** commands. The SSO feature over IPv6 is valid only when IPv6 is configured with a valid Unique Local Address (ULA). For example:

```
fde1:53ba:e9a0:de12::/64
fde1:53ba:e9a0:de13::/64
fde1:53ba:e9a0:de14::/64
fde1:53ba:e9a0:de15::/64
fde1:53ba:e9a0:de16::/64
```

You can choose from two types of privileges to log in to iDRAC.

- **Read-Only** account: An express or basic install of iSM installs **iDRAC SSO launcher**, enabling the administrator to log in to iDRAC as a **Read-Only** account. In addition to the ability to view component health status, logs, and inventory, a few more **SupportAssist** operations that are required by the service personnel are enabled.
- **Administrative** account: Installing this feature by selecting the **Administrator** privilege enables the host operating system administrator to log in to iDRAC as an operator user. Using this account, you can perform all the operations that an iDRAC root user can perform, except configuring or deleting iDRAC users or clearing the Lifecycle Log.

ⓘ **NOTE:** Host operating system accounts without administration rights cannot initiate the iDRAC GUI Launcher if the iDRAC firmware version is 4.00.00.00 or later and the communication between iDRAC and iSM is not through IPv4.

ⓘ **NOTE:** See *iDRAC 9 User's Guide* for specific privileges that are granted to a *Read-only* or *Operator* accounts.

Disable SSO to iDRAC from host operating system: You can also opt to **Disable** this feature completely. When iSM is installed by disabling this feature, launching the **iDRAC GUI launcher** launches the iDRAC log in page with the default browser.

Invoke-iDRACLauncher is independent of the iSM service and can be invoked even if iSM service is stopped.

When browsers are not installed on the host operating system or **Invoke-iDRACLauncher** is not able to launch iDRAC due to a browser issue, a session is still created in iDRAC. Using an iDRAC administrator account, you can login to iDRAC and delete the sessions.

The iDRAC GUI Launcher behaves differently depending on the state of the **OS to iDRAC Pass-through** setting.

- When the **OS to iDRAC Pass-through** setting in iDRAC is disabled, **Invoke-iDRACLauncher** prompts you to enable OS to iDRAC Pass-through in USBNIC mode.
- When the **OS to iDRAC Pass-through** setting is already configured in LOM mode, the iDRAC GUI Launcher does not launch the iDRAC UI.
- When the **OS to iDRAC Pass-through** setting is disabled in iDRAC and **Disable iDRAC Local Configuration using Settings** is also disabled or Lockdown mode is enabled in iDRAC, the iDRAC UI is not launched.

  ⓘ **NOTE:** When **Local Configuration using Settings** or **Local Configuration using RACADM** is disabled in iDRAC, the iDRAC login screen is displayed.

When an iDRAC SSO session is active on the host operating system, closing the related terminal closes the browser with SSO session as well.

ⓘ **NOTE:** Ensure that you invoke the **iDRAC GUI Launcher** from a UI-supported and UI-capable interface. SSO over IPv4 does not work when you modify the third octet in the USB-NIC IP address. Using this feature with IPv6 requires iDRAC9 firmware 4.00.00.00 or later.

Prerequisites

Linux packages:

1. Browser such as Mozilla firefox
2. Sudo
3. PowerEdge yx4x and later servers
4. iDRAC firmware versions 3.30.30.30 and later

   ⓘ **NOTE:** Single sign-on over IPv6 is supported on iDRAC firmware version 4.00.00.00 and later.

Limitations for Linux operating systems

The limitations of the **iDRAC SSO Launcher** on Linux operating systems that does not support:

1. Desktop utilities other than GNOME
2. Browsers other than Mozilla Firefox

ⓘ **NOTE:** When local configuration over KC or RACADM is disabled in iDRAC, then the iDRAC login screen is displayed.

IPv6 communication between iSM and iDRAC over OS to iDRAC Pass-through

The iSM supports both IPv4 and IPv6 modes of communication. After you install iSM, the iSM service attempts to connect to iDRAC using an IPv4 link-local address. If there is no IP address on the host USB NIC interface, iSM tries to configure IPv4 address on the host side. This USB NIC interface configuration on the host operating system from iSM is done only once. iSM remains disconnected from iDRAC if there is any subsequent change in USB NIC configuration that can break the communication between iSM and iDRAC. If the connection fails even after configuring IPv4 address, iSM tries to connect to iDRAC using IPv6.

NOTE: This feature is supported only on Linux operating systems.

NOTE: If the IPv6 network stack is disabled on the host operating system, then iSM tries again to communicate with iDRAC using IPv4.

If either of the protocols is disabled, then iSM will not try to connect to iDRAC using the disabled protocol.

NOTE: If the iDRAC firmware version does not support IPv6 on USB NIC, the connection between iSM and iDRAC is established using IPv4.

Respective audit messages are logged by iSM indicating the protocol version using which iSM connected with iDRAC.

NOTE: When iDRAC USB NIC is already configured with only IPv6 address on the host operating system and then iSM is installed on the host, then iSM communication with iDRAC will start using IPv4 protocol.

Unsupported features with IPv6 protocol

The features that are not supported when iSM is configured with IPv6 protocol and IPv4 configuration is not available on the USB NIC interface are:

- In-Band iDRAC Access
- In-Band SNMP Get
- idrac.local and drac.local
- Autoupdate of iSM

Isolation of OS to iDRAC Pass-through Independent feature

When iSM is unable to establish communication with iDRAC over the OS to iDRAC Pass-through interface, the iSM runs in the **Limited Functionality** mode and the core service remains functional. When iSM is running in the **Limited Functionality** mode, the following message with informational severity is logged on the host operating system:

```
ISM0056: The iDRAC Service Module is running with Limited Functionality Mode, hence
some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting
in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP
address.
```

On disabling the **OS to iDRAC Pass-through** interface from the iDRAC, iSM continues to run in the **Limited Functionality** mode. When iSM runs in the **Limited Functionality** mode, the iSM status in the iDRAC interface is displayed as **Not running**. If the **OS to iDRAC Pass-through** interface is enabled again, all feature states are updated according to the iSM configuration. During iDRAC reset, reboot, and racresetcfg, iSM switches to the **Limited Functionality** mode temporarily and restores back after the communication is reestablished. The feature is compatible with all operating systems supported on iSM 4.2.0.0 and later version.

Table 19. iSM features available on Limited Functionality mode

Feature	iSM support
OS Information (name, version and hostname)	Yes

Table 19. iSM features available on Limited Functionality mode (continued)

Feature	iSM support
Auto System Recovery (ASR)	Yes
iDRACHardReset	Yes
FullPowerCycle (VAC)	Yes

Table 20. Tools and the console messages on Limited Functionality mode

Tool	Console messages
dcismcfg	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP address.` The message is displayed while running the following commands: ● `[--collectperiodicsmartlog/-c] {TRUE,FALSE} Use TRUE/FALSE to Enable/Disable Periodic SMART log collection feature` ● `[--getismstatus/-g] iDRAC service Module status`
Invoke-SupportAssistCollection	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP address.`
Invoke-iDRACLauncher	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP address.`
Enable-iDRACSNMPTrap.sh (Linux)	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP address.`
dcism-sync	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on the host OS does not have a configured IP address.`
Enable-iDRACAccessHostRoute (Linux)	`The iDRAC Service Module is running with Limited Functionality Mode hence some features are unavailable. Possible reasons are: 1) OS-to-BMC Passthrough setting in iDRAC is disabled 2) USBNIC interface on`

Table 20. Tools and the console messages on Limited Functionality mode (continued)

Tool	Console messages
	`the host OS does not have a configured IP address.`
Enable-iDRACAccessHostRoute (Window)	Global handler is not available for iSM. Ensure that iSM service is running and OS to iDRAC Pass-through communication channel is enabled.
ESXi operating system running status in limited mode	`iSM is active (running limited functionality)`
EnableInBandSNMPTraps (Windows)	`winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/dcim_ismservice? instanceid="ismexportedfunctions" @{state="1"}` EnableInBandSNMPTraps_OUTPUT ReturnValue = **34**

Software RAID

Some of the Dell EMC PowerEdge servers have an embedded Software RAID controller, which facilitates enumeration, configuration and monitoring of the controllers, physical disks, and virtual disks which are attached to the server. Software RAID solution provides small to medium business owners the ability to use RAID technology at no additional costs, on Microsoft Windows operating systems.

Software RAID Enumeration

Starting from iSM 4.2.0.0, the Software RAID feature on iDRAC Service Module enables enumeration of PowerEdge RAID Controller (PERC) S130 and later series of controllers, through out-of-band interfaces. Enumeration identifies all Software RAID controller supported devices that are attached to the system, and lists information about controller, physical disk, and virtual disk. The disks enumerate with three nexus structure, similar to **Controller: Bay ID: Slot Number (X:Y:Z)**.

The operating system admin user can run the `dcismcfg.exe` command on the host operating system to collect the latest inventory of the controllers, physical disks, and virtual disks. You must have administrator privileges to run the `dcismcfg.exe` command and enable the feature.

Table 21. Software RAID enumeration supported commands

iSM utility name	CLI options	Description
`dcismcfg.exe -swraid`	`-getctrl`	Displays controller information and enumerates controller properties.
`dcismcfg.exe -swraid`	`-getpd`	Displays the Physical Disk properties.
`dcismcfg.exe -swraid`	`-getvd`	Displays the Virtual Disk properties.
`dcismcfg.exe -swraid`	`-ctrlID=0/1 -getpd/-getvd`	Displays the Physical or Virtual Disk properties managed by the controller 0/1.
`dcismcfg.exe -swraid`	`-getSWRAIDfeatureState`	Displays the current Software RAID feature status.

iSM supports the Software RAID feature on Microsoft Windows operating system with the type Volume, RAID 1, RAID 0, RAID 5, and RAID 10. iSM Software RAID functionality of enumeration is supported on PowerEdge yx3x and later servers using only the iSM command-line interface.

Table 22. Software RAID enumeration feature support matrix for OMSA/OMSS and iSM

Features	OMSA and OMSS	iSM
Controller information	Yes	Yes

Table 22. Software RAID enumeration feature support matrix for OMSA/OMSS and iSM (continued)

Features	OMSA and OMSS	iSM
Virtual Disk information	Yes	Yes
Physical Disk information	Yes	Yes
Backplane information	Yes	No
Create Virtual Disk	Yes	No
Delete Virtual Disk	Yes	No
Import Foreign Virtual Disk	Yes	No
Clear Foreign Virtual Disk	Yes	No
Modify the existing Virtual Disk	Yes	No
Creation on partial Virtual Disk	Yes	No
Setting cache policy for Virtual Disk	Yes	No
Assign or unassign DHS	Yes	No
Assign or unassign GHS	Yes	No
NVMe Cryptographic Erase	Yes	No
Blink	Yes	No
Unblink	Yes	No

7

Frequently asked questions

This section lists some frequently asked questions about the iDRAC Service Module (iSM).

iSM communication with iDRAC switches from IPv4 protocol to IPv6 protocol

iSM communication with iDRAC switches from IPv4 to IPv6 protocol, when you run `ifconfig iDRAC down`, when iSM is communicating with iDRAC through IPv4.

Table 23. The change in protocol when you run the command

Feature/Protocol	IPv4 on Linux	IPv4 on Windows	IPv6 on Linux	IPv6 on Windows
OS information	Yes	Yes	Yes	Yes
WMI	N/A	Yes	N/A	Yes
SupportAssist	Yes	Yes	Yes	Yes
Invoke-iDRACLauncher	Yes	Yes	Yes	Yes
Invoke-iDRACHardReset	Yes	Yes	Yes	Yes
Invoke-VirtualPowerCycle	Yes	Yes	Yes	Yes
Host SNMP Get	Yes	Yes	No	No
In-Band SNMP Traps	Yes	Yes	Yes	Yes
In-Band OMSA SNMP Traps	Yes	Yes	Yes	Yes
iDRAC SSO Launcher	Yes	Yes	Yes(ULA)	Yes(ULA)
Auto System Recovery	Yes	Yes	Yes	Yes
iDRAC In-Band Access	Yes	Yes	No	No
iSM Auto Update	Yes	Yes	No	No
NVMe Prepare to Remove	Yes	Yes	Yes	Yes
Server Storage Correlation	Yes	Yes	Yes	Yes
S.M.A.R.T logs on AHCI	Yes	Yes	Yes	Yes
Software RAID	N/A	Yes	N/A	Yes
Isolation of OS to iDRAC Pass-through Independent feature	Yes	Yes	Yes	Yes

Multiple iDRAC SSO sessions are active over both IPv4 and ULA address

When user changes the IPv4 or ULA address in the iSM, multiple sessions are created. The old IP address is eventually deleted.

Workaround: Manually delete the old IP address.

Must I uninstall OpenManage Server Administrator before installing or running iSM?

No. Before you install or run the iSM, however, ensure that you have stopped the features of OpenManage Server Administrator that the iSM provides.

ⓘ **NOTE:** Uninstalling the OpenManage Server Administrator is not required.

The iDRAC GUI launcher fails and 400-Bad Request error is displayed while accessing via OS2iDRAC.

When the **HostHeaderCheck** property is enabled on iDRAC, the following iSM features are not functional:

- iDRAC access via Host Route
- WSMAN and Redfish via Host Route
- Remote Racadm via Host Route

To enable the feature, use the command, `racadm set iDRAC.WebServer.HostHeaderCheck Disabled`

To check the status of web server property, use the command, `racadm get iDRAC.WebServer.HostHeaderCheck`

For more information about this property, see, DSA-2021-041: Dell iDRAC8 Security Update for a host header injection vulnerability.

How do I know that the iSM is running on my system?

To verify that the iSM is installed on your system,

- On Microsoft Windows operating system, run the command `service.msc`. Check the list of services for the service named **DSM iDRAC Service Module**.
- On Linux operating system, run the command `/etc/init.d/dcismeng status`. If iSM is installed and running, the status is displayed as **running**.
- On VMware ESXi operating system, run the command `/etc/init.d/dcism-netmon-watchdog status`. If iSM is installed and running, the status is displayed as **running**.

ⓘ **NOTE:** Use the `systemctl status dcismeng.service` command instead of the `init.d` command to check if the iSM is installed on Red Hat Enterprise Linux or SUSE Linux operating systems.

How do I know which version of the iSM I have on my system?

To check the version of the iSM installed on the system, click **Start** > **Control Panel** > **Programs and Features**. The version of the installed iSM is listed in the **Version** tab. You can also check the version by go to **My Computer** > **Uninstall or change a program**.

On the Linux operating system, run the following command:

```
rpm -qa | grep dcism
```

On the VMware ESXi operating system, run the following command:

```
esxcli software vib get --vibname=dcism
```

What is the minimum permission level required to install iSM?

To install iSM, you must have operating system administrator level privileges.

I see the message "The iSM is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel" in the operating system log files, even when the OS to iDRAC Pass-through over USBNIC is configured properly. Why do I get this message?

iSM uses the OS to iDRAC Pass-through over USBNIC to establish communication with iDRAC. Sometimes, the communication is not established though the USBNIC interface is configured with correct IP endpoints. This may happen when the host operating system routing table has multiple entries for the same destination mask and the USBNIC destination is not listed as the first one in routing order.

Table 24. Routing order details

Destination	Gateway	Genmask	Flags	Metric	Ref	Use Iface
default	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

In the example **enp0s20u12u3** is the USBNIC interface. The link-local destination mask is repeated, and the USBNIC is not the first one listed. This results in the connectivity issue between iSM and iDRAC over the OS to iDRAC Pass-through. To troubleshoot the connectivity issue, ensure that the iDRAC USBNIC IPv4 address—by default it is 169.254.1.1—is reachable from the host operating system. If it is not reachable from the host operating system do one of the following:

- Change the iDRAC USBNIC address on a unique destination mask.
- Delete the unwanted entries from the routing table to ensure that USBNIC is chosen by route when the host wants to reach the iDRAC USBNIC IPv4 address.

Whenever I try to install iSM, the following error message is displayed: This operating system is not supported.

iSM can be installed only on supported operating systems. For information about operating systems that are supported, see Supported operating systems.

I used the remote iDRAC hard reset feature to reset the iDRAC. However, the IPMI is unresponsive and I am not able to troubleshoot.

If you try to use the remote iDRAC hard reset feature on **VMware ESXi operating system** the IPMI drivers becomes unresponsive, and because of this the iSM communication is stopped. You may have to reboot the server and load the IPMI driver again to resolve the issue.

Where do I find the Replicated LifeCycle log on my operating system?

To view the replicated Lifecycle log files:

Table 25. Operating system and location

Operating System	**Location**
Microsoft Windows	**Event viewer** > **Windows Logs** > ***<Existing group or Custom folder>***. All the iSM Lifecycle log files are replicated under the source name **iDRAC Service Module**.
Red Hat Enterprise Linux, and SUSE Linux	**/var/log/messages**
VMware ESXi	**/var/log/syslog.log**
Ubuntu	**/var/log/syslog**

What is the default SNMP protocol configured in iSM to send alerts in Linux operating systems?

By default, the SNMP multiplexing protocol (SMUX) is configured in iSM to send alerts.

SMUX is not supported on my system. Which protocol should I configure to send alerts?

If SMUX is not supported on your system, Agent-x is used as a default protocol.

How do I configure iSM to use the Agent-x protocol to send alerts by default?

You can configure Agent-x as the default protocol using `./Enable-iDRACSNMPTrap.sh 1/agentx –force` command. If `–force` is not specified, ensure that the net-SNMP is configured and restarts the snmpd service.

What are the Linux-dependent packages or executables I should install while completing the Linux installation?

To view the list of Linux-dependent packages, see Linux dependencies.

I created a custom folder in Windows Event Viewer, but the Lifecycle log files are not replicated in my custom folder. What do I have to do now to replicate the Lifecycle log files?

Ensure that you close the Windows **Event Viewer** after creating the custom folder. Open the Windows **Event Viewer** again to view the replicated Lifecycle log files.

I chose the custom install option from the Graphical User Interface during iSM installation and disabled a feature, but I am not able to enable the feature using any of the other interfaces. How do I enable the feature again?

On systems running Microsoft Windows, a feature that is enabled using the installer and disabled using any interface other than the installer can only be enabled using the same interface or the installer in Graphical User Interface mode.

For example, you may not be able to enable a feature that was disabled from the Graphical User Interface during iSM installation using the RACADM CLI commands.

I am not able to access the iDRAC page through the host operating system as an Active Directory user over LDAP. I am trying to access the iDRAC page through the host operating system, but I get an error saying that the site cannot be reached. How do I troubleshoot the issue?

When you are trying to access the iDRAC page through the host operating system, you may get an error saying that the site cannot be reached. Ensure that the iDRAC network is configured for authentication as an LDAP user. You can also log in as a local user or a guest.

I am not able to access the iDRAC page through the host operating system after performing an iDRAC factory reset operation such as `racadm racresetcfg`. How do I troubleshoot the issue?

Ensure that the **OS to iDRAC Pass-through** channel is enabled. By default, it is disabled in factory mode. To enable the **OS to iDRAC Pass-through** channel on iDRAC, use the following command: `racadm set idrac.os-bmc.adminstate 1`.

I am seeing 169.254.0.2 as the source IP address in the iDRAC SNMP trap received through iSM. How do I troubleshoot the issue?

On the Linux operating system, the iDRAC SNMP traps received through the host operating system displays the hostname or source IP address as 169.254.0.2 instead of the actual host operating system name or IP address. This is determined by the operating system to populate the entry before rendering the trap to the user.

I have configured my OS to iDRAC Pass-through to LOM and when I try to run dcism-sync, the update operation fails. What can be done?

OS to iDRAC Pass-through must be configured to use USB-NIC mode. This is a pre-requisite for iSM installation and update.

I can enable or disable the WMIInfo feature of iSM on Linux and VMware ESXi using RACADM and WS-Man commands. Does this impact my iSM configuration on the host operating system?

The WMIInfo feature of iSM is applicable only to Microsoft Windows operating systems. However, enabling or disabling this feature from any of the iDRAC interfaces on any operating system other than Microsoft Windows does not impact the iSM configuration on the host operating system.

If I delete the IP address of the USBNIC interface on the host operating system, then iSM is unable to communicate with iDRAC.

The iSM configures the host operating system USBNIC interface only once. Later, if you bring down the USBNIC interface on the host operating system by deleting the IP address, making the interface link down or disabling the IPV4 or IPV6 address on this interface, then iSM will retain the user configuration and does not override the interface settings. To restore the communication between iSM and iDRAC, restart the iSM service on the host operating system.

After installing iSM using the batch file ISM_Win.BAT from the iDRAC exposed logical partition "SMINST" on Microsoft Windows operating system, I see a console message saying "The system cannot find the file specified."

After iSM is installed successfully, the logical partition **SMINST** is unmounted from the host operating system. This message appears if the BAT script is invoked from the **SMINST** partition itself. The installation is successful. No action is required by the user.

If dependent packages for iSM are not present on Ubuntu operating system, then installation through operating system DUP installs iSM in install+unpacked state.

You can verify this using the below command:

```
#dpkg -s dcism
Package: dcism
Status: install ok unpacked
```

To fix this issue, run the command `apt-get install -f`. This installs dependent packages.

When I install iSM 3.4.0 or later on Linux operating systems such as Red Hat Enterprise Linux, I see some messages in operating system logs such as G_IS_SIMPLE_ACTION (simple)' failed: failed to rescan: Failed to parse /usr/share/applications/iDRACGUILauncher.desktop file: cannot process file of type application/x-desktop.

The messages are related to the GNOME desktop manager. Various operating system groups have Bugzilla items to address this scenario. For example, https://bugzilla.redhat.com/show_bug.cgi?id=1594177. No action is required by the user.

I see a blank terminal on Red Hat Enterprise Linux operating system when I click iDRAC GUI Launcher shortcut from Menu > Accessories.

The visibility of text on the terminal depends on the GNOME version running on the resident operating system. An alternative is to run the launcher from a UI-capable shell. For example, `bash#> sh /opt/dell/srvadmin/iSM/bin/iDRACLauncher.sh` as a sudo user.

In case, the **OS to iDRAC Pass-through** is disabled in iDRAC, you see a blank terminal when the iDRAC UI is launched from the Linux operating system such as Red Hat Enterprise Linux 7.x and 8.x. Select **y** or **Y**, and press **Enter** to indicate configuration of USBNIC interface on the host operating system.

Alternatively, you can enable the **OS to iDRAC Pass-through** in iDRAC in USBNIC mode and rerun the iDRAC launcher from the host operating system.

When I try to launch Single Sign-on feature in a pure IPv6 environment, the iDRAC UI session does not launch and a blank screen is displayed.

By default, the USB_NIC device has IPv4 (link-local) and IPv6 (link-local) addresses along with a ULA address. Ensure that all the three IP addresses are present in the USB_NIC device. If the ULA address is not present, verify that the device IPv6 protocol setting is set to Disable or Link local state. It must be in automatic mode for the Single Sign-on feature to work.

iSM Host SNMP OMSA alert is enabled even when the parent iSM Host SNMP alert is disabled.

To disable the iSM Host SNMP OMSA alert feature, you must first enable the parent iSM Host SNMP alert and then disable the child iSM Host SNMP OMSA alert feature.

The iSM Host SNMP OMSA alert feature can be disabled using one of the following options:

- RACADM interface
- iSM installer for operating system, where it is supported.

iDRAC to OMSA SNMP alert mapping gets enabled when OMSA is running.

To disable iSM Host SNMP OMSA alert, restart the iDRAC Service Module.

"Signature not okay" (GPG key) error message is displayed during the installation of iSM on Linux operating system.

Install the Gnu Privacy Guard (GPG) key to verify the Linux DUP digital signature on your system. To install the GPG key, complete the following steps:

1. To download the GPG key, run the following command:

   ```
   wget https://linux.dell.com//repo/pgp_pubkeys/0x1285491434D8786F.asc -O RPM-GPG-KEY
   ```

2. To import the public key to the **gpg** trust database, run the following command:

   ```
   rpm --import RPM-GPG-KEY
   ```

3. Retry the installation.

How does iSM communicate with iDRAC?

iSM communicates with iDRAC using Secure Socket Layer (SSL) over Transmission Connect Protocol (TCP) in a client-server model. The communication is a point-to-point connection using link-local IP address. The interface supports both IPv4 and IPv6 addresses. Both the iDRAC and host USBNIC interface addresses must be within the same subnet.

For example, if iDRAC USBNIC interface is configured as 169.254.1.1 with subnet 255.255.255.0, then the USBNIC interface on the host must be configured as 169.254.1.2 with subnet 255.255.255.0. Ensure that there are no IP address conflicts between any two interfaces on the host operating system.

8

Linux and Ubuntu installer packages

The installer packages for supported Linux and Ubuntu operating system are as follows:

Table 26. Linux installer packages

Supported Linux operating system	Installer package
Red Hat Enterprise Linux 7	`SYSMGMT\iSM\linux\RHEL7\x86_64\dcism-4.2.0.0-<bldno>.el7.x86_64.rpm`
Red Hat Enterprise Linux 8	`SYSMGMT\iSM\linux\RHEL8\x86_64\dcism-4.2.0.0-<bldno>.el8.x86_64.rpm`
Ubuntu 20	`SYSMGMT\iSM\linux\Ubuntu20\x86_64\dcism-4.2.0.0-<bldno>.ubuntu20.deb`
SUSE Linux Enterprise Server 15	`SYSMGMT\iSM\linux\SLES15\x86_64\dcism-4.2.0.0-<bldno>.sles15.x86_64.rpm`

9

Resources and support

For more information about the features of this release, see the iDRAC Service Module 4.2.0.0 documentation.

Latest Released Documents

To access the latest version of iDRAC Service Module documents:

1. Go to https://www.dell.com/idracmanuals.
2. Click **iDRAC Service Module**, and then click to open the required version of iDRAC Service Module.
3. Click **Documentation**.

Accessing documents using direct links

Table 27. Direct links for documents

URL	Product
https://www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
https://www.dell.com/cmcmanuals	Chassis Management Controller (CMC)
https://www.dell.com/esmmanuals	Enterprise System Management
https://www.dell.com/serviceabilitytools	Serviceability Tools
https://www.dell.com/omconnectionsclient	Client System Management

Accessing documents using the product search

1. Go to https://www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. A list of matching products are displayed.
3. Select your product and click the search icon or press enter.
4. Click **Documentation**.

Accessing documents using the product selector

You can also access documents by selecting your product.

1. Go to https://www.dell.com/support.
2. Click **Browse all products**.
3. Click the required product category, such as Servers, Software, Storage.
4. Click the required product and then click the required version if applicable.

   ⓘ **NOTE:** For some products, you may need to navigate through the subcategories.
5. Click **Documentation**.

Topics:

- Identifying the series of your Dell EMC PowerEdge servers

Identifying the series of your Dell EMC PowerEdge servers

The PowerEdge series of servers from Dell EMC are divided into different categories based on their configuration. They are referred as YX2X, YX3X, YX4X, YX4XX, or YX5XX series of servers. The structure of the naming convention is described below:

The letter Y denotes the character in the server model number. The character denotes the form factor of the server. The form factors are listed below:

- C — Cloud
- F — Flexible
- M or MX — Modular
- R — Rack
- T — Tower
- XR — Industrial-grade server for extreme environment

The letter X denotes the numbers in the server model number. The number denotes multiple characteristics about the server. They are listed as follows:

- The first digit (X) denotes the value stream or class of the server.
  - 1-5 — iDRAC basic
  - 6-9 — iDRAC Express
- The second digit denotes the series of the server. It is retained in the server naming convention and does not replace the letter X.
  - 0 — series 10
  - 1 — series 11
  - 2 — series 12
  - 3 — series 13
  - 4 — series 14
  - 5 — series 15
- The last digit (X) always denotes the make of the processor as described below:
  - 0 — Intel
  - 5 — AMD

NOTE: For servers that use an AMD processor, the model number is made up of four digits instead of three. The third digit (X) denotes the number of processor sockets that the series of server supports.

- 1–one socket server
- 2–two socket server

Table 28. PowerEdge servers naming convention and examples

YX3X systems	YX4X systems	YX4XX systems	YX5XX systems
PowerEdge M630	PowerEdge M640	PowerEdge R6415	PowerEdge R6515
PowerEdge M830	PowerEdge R440	PowerEdge R7415	PowerEdge R7515
PowerEdge T130	PowerEdge R540	PowerEdge R7425	PowerEdge R6525

10

Contacting Dell EMC

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues, see www.dell.com/contact.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.