

Dell EMC iDRAC Service Module 3.6

Release Notes

Notes, cautions, and warnings

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

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

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

Chapter 1: Release summary	5
Version.....	5
Release date.....	5
Priority and recommendations.....	5
Chapter 2: Compatibility	6
License requirements.....	6
Supported platforms.....	6
Previous versions.....	7
Supported operating systems and hypervisors.....	7
Chapter 3: New in this release	8
Chapter 4: Known issues	9
Common issues.....	9
A warning message indicating the iSM communication restart is observed in both iDRAC Lifecycle log files and operating system log files.....	9
Job Queue page displays the job as Firmware Update instead of OSCollector.....	9
Increased workload on the host interrupts the communication between iSM and iDRAC	9
ISM0003 event message after replacing the system board	10
Registering SupportAssist Enterprise.....	10
Enabling operating system information.....	10
iDRAC GUI launcher fails with OS2iDRAC	10
Known issues on Microsoft Windows operating systems.....	11
Invoke-iDRACHardReset and Invoke-FullPowerCycle are not functional.....	11
Alert message is displayed when OMSA is installed and TSR is requested.....	11
An internal error occurred when running the DCIM_View class.....	11
A popup is displayed when uninstalling iSM.....	12
Running WMI MOF query on DCIM results with no data.....	12
iSM communication with iDRAC switches from IPv6 to IPv4.....	12
During the repair or modify operation on Microsoft Windows 2016 operating system installation, communication between the iSM and iDRAC is not established.....	12
Known issues on Linux operating systems.....	13
iSM communication with iDRAC is dropped, when Enable-iDRACAccessHostRoute feature is enabled and firewall service is disabled.....	13
ipmi_si IPMI_driver does not respond after iDRAC hard reset	13
InBand iDRAC Access feature is unavailable in IPv6 protocol.....	13
AVC denial with iptables.....	13
A message is displayed when invoking iDRAC GUI Launcher for the first time.....	14
Known issues on VMware ESXi operating systems.....	14
iDRAC Service Module communication with iDRAC is interrupted in ESXi 7.0 U1.....	14
Communication is not restarting after performing Restart Management Agents.....	14
IPMI driver becomes unresponsive on VMware ESXi.....	14
Performing iDRAC hard reset operation on VMware ESXi	15

Chapter 5: Limitations.....	16
Limitations on Linux operating system.....	16
Limitations on Microsoft Windows operating systems.....	16
Limitations on VMware ESXi operating systems.....	17
Chapter 6: User notes.....	18
User notes for supported Microsoft Windows operating systems.....	18
User notes for supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server.....	18
Chapter 7: Resources and support.....	19
Identifying the series of your Dell EMC PowerEdge servers.....	20
Chapter 8: Contacting Dell EMC	21

Release summary

iDRAC Service Module (iSM) is a lightweight software application that can be installed on yx2x or later PowerEdge servers. This release of iSM supports new operating systems, additional features, and existing feature enhancements.

Topics:

- [Version](#)
- [Release date](#)
- [Priority and recommendations](#)

Version

iDRAC Service Module version 3.6

Release date

December 2020

Priority and recommendations

Dell Technology recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that help keep your system software current and compatible with other system modules, including firmware, BIOS, drivers, and software.

Compatibility

Topics:

- [License requirements](#)
- [Supported platforms](#)
- [Previous versions](#)
- [Supported operating systems and hypervisors](#)

License requirements

For information regarding license agreements, see *iDRAC Service Module 3.6 User's Guide* available at www.dell.com/ismmanuals.

Supported platforms

iDRAC Service Module 3.6 supports yx2x to yx5x generation of PowerEdge servers. See *Identifying the series of your Dell EMC PowerEdge servers* for more information.

Supported systems

Table 1. The table lists platforms that are supported by iDRAC Service Module 3.6.

yx5x PowerEdge servers	yx4x PowerEdge servers	yx3x PowerEdge servers	yx2x PowerEdge servers
R6515	XE7440	C4130	FM120
R7515	XE7420	C6320	M420
R6525	R240	FC 430	M520
C6525	R340	FC 630	M620
R7525	T140	FC 830	M820
	T340	M630	R220
	R740xd2	M630-VRTX	R320
	R840	M830	R420
	R940 xa	R230	R620
	MX740c	R330	R720
	MX840c	R430	R720XD
	R7425	R530	R820
	R7415	R630	R920
	R6415	R730	T320
	C6420	R730xd	T420
	FC 640	R830	T620
	M640	R930	

Table 1. The table lists platforms that are supported by iDRAC Service Module 3.6. (continued)

yx5x PowerEdge servers	yx4x PowerEdge servers	yx3x PowerEdge servers	yx2x PowerEdge servers
	M640-VRTX	T130	
	FD332	T330	
	R440	T430	
	R540	T630	
	R640		
	R740		
	R740xd		
	R940		
	T440		
	T640		

Previous versions

- iDRAC Service Module 3.5.1
- iDRAC Service Module 3.5
- iDRAC Service Module 3.4.1
- iDRAC Service Module 3.4
- iDRAC Service Module 3.3.1
- iDRAC Service Module 3.3
- iDRAC Service Module 3.2
- iDRAC Service Module 3.1
- iDRAC Service Module 3.0.2
- iDRAC Service Module 3.0.1
- iDRAC Service Module 2.5.1
- iDRAC Service Module 2.5
- iDRAC Service Module 2.4
- iDRAC Service Module 2.3
- iDRAC Service Module 2.2
- iDRAC Service Module 2.1
- iDRAC Service Module 2.0
- iDRAC Service Module 1.0

Supported operating systems and hypervisors

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP2
- Ubuntu 20.04 LTS
- VMware vSphere (ESXi) 7.0 U1 (supports yx3x, yx4x, and yx5x PowerEdge servers)
- VMware vSphere (ESXi) 7.0 U2 (supports yx3x, yx4x, and yx5x PowerEdge servers)
- VMware vSphere (ESXi) 6.7 U3 (supports yx3x, yx4x, and yx5x PowerEdge servers)

New in this release

New supported operating systems

iDRAC Service Module 3.6 supports the following operating systems:

- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 7.9
- SUSE Linux Enterprise Server 15 SP2
- Ubuntu server 20.04 LTS
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

New and enhanced features

The following are the new and enhanced features of iDRAC Service Module 3.6:

- Secure loading of libraries to prevent preloading on Linux and VMware ESXi.
- Monitoring of S.M.A.R.T attributes of chipset SATA devices under software RAID controller.
- Inclusion of Chipset SATA device's historic S.M.A.R.T log files into SupportAssist Collection.
- SupportAssist Auto Dispatch for disks for two events for VMware ESXi:
 - Predictive failure reported for physical disk.
 - A bad disk block on <device> cannot be reassigned during a write operation.
- Enhanced NVMe Prepare to Remove feature in Linux operating system—NVMe prepare to remove operation is not allowed when a NVMe drive is in use or raw read and write operation is in progress on the NVMe drive.
- Enhanced iDRACHardReset and FullPowerCycle features—The iDRACHardReset and FullPowerCycle operations are supported when secure boot option is enabled in the BIOS. The minimum BIOS version required is 1.5.3 for yx5x AMD server.

Known issues

Topics:

- [Common issues](#)
- [Known issues on Microsoft Windows operating systems](#)
- [Known issues on Linux operating systems](#)
- [Known issues on VMware ESXi operating systems](#)

Common issues

The issues that are mentioned in this section are common for all the operating systems.

A warning message indicating the iSM communication restart is observed in both iDRAC Lifecycle log files and operating system log files

Description: When both iDRAC Service Module (iSM) and OpenManage Server Administrator (OMSA) services are running on the host operating system, iSM communication with iDRAC might stop and start every 5 hours 30 minutes automatically. A warning message indicating the iSM communication restart is observed in both iDRAC Lifecycle log files and operating system log files. No action is required as iSM communication is restored automatically within 1 to 2 minutes.

```
Log Message: ISM0007 The iDRAC Service Module communication with iDRAC has ended.
```

Cause: Not available.

Workaround: Not available.

Tracking number: 180859

Job Queue page displays the job as Firmware Update instead of OSCollector

Description: When OSCollector Dell Update Package (DUP) is updated in iDRAC, the Job Queue page displays the job as `Firmware Update: Diagnostics` instead of OSCollector.

Cause: Not available.

Workaround: There is no workaround available.

Tracking number: 139485, 139088, 141091

Increased workload on the host interrupts the communication between iSM and iDRAC

Description: When there is increased workload on the host due to intensive task requests by the processor, communication between iSM and iDRAC is temporarily interrupted with the following warning message in

the Lifecycle log file: The iDRAC Service Module communication with iDRAC has ended. The connection automatically resumes and no action is required.

Cause: Not available.

Workaround: There is no workaround available.

Tracking number: 159410

ISM0003 event message after replacing the system board

Description: If a USB NIC is enabled after the system board is replaced without restoring the configuration or after the iDRAC is reset to factory settings, you can observe the following ISM0003 event message on operating system log files before starting the communication: The iDRAC Service Module is unable to discover iDRAC from the operating system of the server. No action is required.

Cause: Not available.

Workaround: There is no workaround available.

Tracking number: 161262

Registering SupportAssist Enterprise

Description: SupportAssist registration fails on Dell Original Equipment Manufacturer (OEM) servers with iSM 3.5.0 or later.

Cause: Not available.

Workaround: Not available.

Tracking number: 193977

Enabling operating system information

Description: On enabling operating system information when iSM is installed, IPv6 default gateway address and DNS server fields are not rendered in the iDRAC interfaces.

Cause: Not available.

Workaround: Not available.

Tracking number: 193255

iDRAC GUI launcher fails with OS2iDRAC

Description: iDRAC GUI launcher fails with OS2iDRAC, and **400-Bad Request** error is received while using an ErrorDocument to handle the request.

Cause: When **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

Workaround: To enable the feature, use the following command:

```
racadm set iDRAC.WebServer.HostHeaderCheck Disabled
```

To check the status of web server property, use the following 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](#).

Tracking number: 212613

Known issues on Microsoft Windows operating systems

Invoke-iDRACHardReset and Invoke-FullPowerCycle are not functional

Description: The Invoke-iDRACHardReset and Invoke-FullPowerCycle features are not functional and a console message is displayed: *This feature is not supported on this platform*. The message is displayed in the following scenarios:

- When iDRAC Service Module (iSM) and Open Manage Server Administrator (OMSA) both are installed and running on the host operating system, and OMSA is uninstalled from the operating system.
- When iSM is installed and Dell Update Package (DUP) such as iDRAC firmware update package is invoked from the host operating system.

Cause: Not available.

Workaround: Reinstalling iSM enables the Invoke-iDRACHardReset and Invoke-FullPowerCycle features.

Tracking number: 186472

Alert message is displayed when OMSA is installed and TSR is requested

Description: When OpenManage Server Administrator (OMSA) is installed on yx3x PowerEdge servers and Tech Support Report (TSR) is requested from any of the iDRAC interfaces, then a critical alert that is related to ChipsetDriver.exe is observed in the operating system log files.

Cause: Not available.

Workaround: The alert can be ignored and no action is required.

Tracking number: 185544

An internal error occurred when running the DCIM_View class

Description: When DCIM_View class is enumerated with any WSMAN client through the iSM's **WMI Info** feature on yx5x PowerEdge servers and iDRAC firmware 4.00.00.00 or later, the response is partial and fails with the following error code 5:

```
The specified class does not exist in the given namespace
```

Cause: The failure is because the DCIM_VFlashView class is deprecated starting with the iDRAC firmware version 4.00.00.00.

Workaround: Enumerate the explicit classes such as DCIM_CPUView, DCIM_FANView, and so on.

Tracking number: 157981

A popup is displayed when uninstalling iSM

- Description:** If the Firefox browser is opened when uninstalling the iSM, a popup is displayed. The popup notifies you that the Firefox browser must be closed before continuing the uninstallation procedure. Close the Firefox browser, and click the **Retry** option to continue the uninstallation procedure.
- Cause:** Not available.
- Workaround:** There is no workaround available.
- Tracking number:** 87075

Running WMI MOF query on DCIM results with no data

- Description:** When a Windows management instrumentation (WMI) MOF query is run on DCIM_View classes using iSM, no data is populated.
- Cause:** Not available.
- Workaround:** There is no workaround and no action is required.
- Tracking number:** 157981

iSM communication with iDRAC switches from IPv6 to IPv4

- Description:** When iDRAC Service Module (iSM) is communicating with iDRAC over IPv6 protocol on a Microsoft Windows operating system, and if you perform an iDRAC Hard Reset operation or iDRAC firmware upgrade or downgrade, then the communication switches back to IPv4.
- Cause:** Not available.
- Workaround:** There is no workaround and no action is required.
- Tracking number:** 138538, 146421

During the repair or modify operation on Microsoft Windows 2016 operating system installation, communication between the iSM and iDRAC is not established

- Description:** While performing a repair or modify operation during Microsoft Windows 2016 operating system installation, communication between the iSM and iDRAC might not be established. Retry the operation.
- Cause:** Not available.
- Workaround:** There is no workaround available.
- Tracking number:** 161320

Known issues on Linux operating systems

iSM communication with iDRAC is dropped, when Enable-iDRACAccessHostRoute feature is enabled and firewall service is disabled

- Description:** iSM communication with iDRAC is dropped, when Enable-iDRACAccessHostRoute feature is enabled and firewall service is disabled in SUSE Linux Enterprise 12 SP2 operating system.
- Cause:** Not available.
- Workaround:** Not available.
- Tracking number:** 173354

ipmi_si IPMI_driver does not respond after iDRAC hard reset

- Description:** After performing an iDRAC hard reset operation on certain Linux operating systems, the ipmi_si, IPMI driver may not respond because of an existing issue in the IPMI driver. If the IPMI driver stops responding, reload the ipmi_si IPMI driver.
- Cause:** Not available.
- Workaround:** The issue occurs in Linux kernel version earlier to 3.15. An update is available in the following operating systems with Linux kernel version 3.15 or later.
- Steps to reload the IPMI driver:
- `modprobe -r ipmi_si`: If the removal fails, then applications such as iDRAC Service Module and OpenManage Server Administrator must be stopped using the command: `ipmi_si`, and then you can retry the operation.
 - `modprobe ipmi_si`: Alternatively, the administrator can also restart the host operating system to resolve the issue.
- Tracking number:** Not available

InBand iDRAC Access feature is unavailable in IPv6 protocol

- Description:** When the iSM is communicating with iDRAC using IPv6 protocol, enabling the feature **InBand iDRAC Access** indicates a successful message. But this feature is unavailable in IPv6 protocol.
- Cause:** Not available.
- Workaround:** There is no workaround available.
- Tracking number:** Not available.

AVC denial with iptables

- Description:** When iDRAC Service Module (iSM) is installed on Red Hat Enterprise Linux operating system with SELinux enabled in the either of Permissive or Enforcing modes, AVC denial with iptables in the AVC denial log files are observed in the `/var/log/audit/audit.log` path, when the following features are either enabled or disabled:
- iDRAC Access via Host operating system
 - Host SNMP Alerts
- Cause:** Not available.
- Workaround:** iSM does not support explicit SELinux policies. There is no functionality impact to iSM features.

Tracking number: 102480

A message is displayed when invoking iDRAC GUI Launcher for the first time

Description: When invoking **iDRAC GUI Launcher** for the first time either using iDRACLauncher.sh or the program menu shortcut, the following message is displayed in operating system log files:

```
"localhost dbus-daemon[2369]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.18176' (uid=0 pid=126684 comm="sudo -l /opt/dell/srvadmin/ism/bin/InvokeiDRACLau" label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023") "
```

Cause: Not available.

Workaround: There is no functional impact. No action is required.

Tracking number: 124514

Known issues on VMware ESXi operating systems

iDRAC Service Module communication with iDRAC is interrupted in ESXi 7.0 U1

Description: In VMware ESXi 7.0 U1, iDRAC Service Module (iSM) communication with iDRAC is dropped. No action is required as the communication is restored automatically within 1 to 2 minutes.

Cause: Not available.

Workaround: Not available.

Tracking number: 172915

Communication is not restarting after performing Restart Management Agents

Description: iDRAC Service Module is not restarting the communication with iDRAC after performing **Restart Management Agents** on VMWare ESXi.

Cause: Not available.

Workaround: You must try performing **Restart Management Agents** again immediately after the first attempt.

Tracking number: 176426

IPMI driver becomes unresponsive on VMware ESXi

Description: After performing an iDRAC hard reset operation on certain VMware ESXi, the ipmi_si_drv IPMI driver on ESXi 6.5 U2 and ipmi IPMI drive on ESXi 6.7 U1 do not respond because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the ipmi_si_drv IPMI driver on ESXi 6.5 U2 and ipmi IPMI drive on ESXi 6.7 U1.

Cause: Not available.

Workaround: The issue is observed in iDRAC Service Module 2.3 and later supported ESXi versions.

To reload the IPMI driver, run the following commands:

```
esxcli system wbem set -e 0
esxcfg-module -u ipmi_si_drv/ipmi => unload ipmi_si_drv/ipmi
esxcfg-module ipmi_si_drv/ipmi => load ipmi_si_drv/ipmi
esxcfg-module ipmi_si_drv/ipmi => load ipmi_si_drv/ipmi
esxcli system wbem set -e 1
```

If the removal fails, then applications such as iDRAC Service Module and OpenManage Server Administrator must be stopped using the `ipmi_si` command, and then you can retry the operation.

Alternatively, the administrator can also restart the host operating system to resolve the issue.

Tracking number: Not available.

Performing iDRAC hard reset operation on VMware ESXi

Description: To perform iDRAC hard reset operation on VMware ESXi operating system using the `winrm` command, the iSM must be communicating with iDRAC.

Cause: Not available.

Workaround: There is no workaround available.

Tracking number: Not available.

Limitations

Common limitations

The following limitations are applicable to all the operating systems.

- When Federal Information Processing Standards (FIPS) mode is enabled either on the host operating system or iDRAC, communication between iSM and iDRAC is not established.
- When there is an increased workload on the host due to intensive task request by the processor, the communication between iDRAC Service Module and iDRAC is interrupted for a moment and restored automatically.

Tracking number: 158514, 158740, 158667, 159019

Topics:

- [Limitations on Linux operating system](#)
- [Limitations on Microsoft Windows operating systems](#)
- [Limitations on VMware ESXi operating systems](#)

Limitations on Linux operating system

- The NVMe prepare to remove operation on disk with storage capacity more than 5 TB takes more time to shutdown than expected. As a result, the prepare to remove job status fails on iDRAC. However, the disk is removed from the operating system, and the correct status of the prepare to remove operation is reflected in the iSM operating system log.

Tracking number: 202946

- Feature Lifecycle Log Replication on operating system log file shows a one-hour difference in the **EventTimeStamp** displayed in the operating system log when daylight saving is applied.

Tracking number: 088419

- IPv6 support on Linux operating systems are not available for the following features:
 - iSM Auto Update
 - ismtech
 - Inband iDRAC Access
 - SNMP Get via Host operating system
- When iSM is communicating with iDRAC using IPv6 protocol, enabling the InBand iDRAC Access feature indicates a successful message, but this feature is unavailable over IPv6 protocol. No action is required.

Tracking number: 132983

- Communication between iSM and iDRAC over IPv6 will work only on iDRAC firmware 2.70.70.70 or later.

Limitations on Microsoft Windows operating systems

- Do not specify user profile folders such as C:\Users\administrator\Desktop as custom installation paths for installing iSM. This is because services running on the system account cannot access such folders.
- You cannot view Lifecycle Controller log files in the new folder in the Event Viewer, 169898, if you have recently changed the folder name of the Lifecycle Controller log files in the Event Viewer. Microsoft recommends that you reboot the operating system to view the Lifecycle Controller log files under the new view name.
- When iSM is installed on Microsoft Windows operating systems using an operating system DUP, then the iSM **Modify and Repair** operation from the **Add/Remove** option displays the following error message:

Original source path of the file is now found.

You can extract the iSM DUP, double-click the MSI, and run repair.

Tracking number : 115250

- Communication between iSM and iDRAC over IPv6 will work only on iDRAC firmware 2.70.70.70 or later.
- On Windows operating systems, 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 GUI mode.
- IPv6 support on Linux operating systems are not available for the following features:
 - iSM Auto Update
 - ismtech
 - Inband iDRAC Access
 - SNMP Get via Host operating system

Limitations on VMware ESXi operating systems

- Upgrading an earlier version of ESXi to ESXi 7.x is failing with iSM VIB installed. In VMware vSphere 7.0, 32-bit userworld support is deprecated. For more information, see the *Deprecation of 32-bit Userworld Support* section in [VMware vSphere 7.0 Release Notes](#) and *Known issues* section in [VMware vSphere 7.x on Dell EMC PowerEdge Servers Release Notes](#).

Workaround: Before upgrading an earlier version of ESXi to ESXi 7.0, uninstall the 32-bit iSM VIB corresponding to iSM v3.5.0 or earlier on the hypervisor.

Tracking number: 148591

- When the small footprint CIM broker (SFCB) configuration is set to read-only mode in the VMware ESXi operating system, iSM-Windows remote management (WinRM) commands such as `iDRACHardreset`, `EnableInBandSNMPTraps` do not function. As a workaround, use the `Invoke-iDRACHardReset` command line utility to perform the iDRAC Hardreset operation.
- The iDRAC Access via Host operating system feature is not supported on VMware ESXi operating systems.
- When Local Racadm set is disabled through iDRAC interfaces:
 - iSM fails to configure the operating system to iDRAC passthru in the USB NIC mode.
 - iSM functionality is restored when Local Racadm set is enabled.
- EventID for Lifecycle Controller logs replicated to operating system log will be 0 for some of the past events.
- TrapID for In-band SNMP Traps will be 0 for some of the past traps.
- When iDRAC Hardreset is disabled in iDRAC and you perform an iDRAC Hardreset operation from the hypervisor operating systems like VMware ESXi, the result indicates success although iDRAC is not reset.

User notes

Topics:

- User notes for supported Microsoft Windows operating systems
- User notes for supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server

User notes for supported Microsoft Windows operating systems

To enable WSMAN silently, use the following CLI command:

```
Msiexec.exe/i iDRACSvcMod.msi ADDLOCAL="WSMAN_Enablement" CP_SELF_SIGN_CERT="2"  
CP_WSMAN_PORT="1234" CP_CERTIFICATE="1" CP_NEGOTIATE="1"/qn
```

User notes for supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server

- To perform an **Express Install** on Red Hat Linux Server and SUSE Linux Enterprise Server operating systems, run the following command from the **SYSMGMT/iSM/linux** directory:

```
dcism-setup.sh -x
```

For more information on the installation instructions, refer to the iDRAC Service Module User's Guide.

- By default, you do not have permission to run the script directly on the disk partition. Run the following command to run the script directly and initiate iDRAC Service Module installation:

```
sh ISM_Lx.sh or .ISM_Lx.sh
```

Resources and support

For more information about the features of this release, see the iDRAC Service Module 3.5.1 documentation.

Latest Released Documents

To access the latest version of iDRAC Service Module documents:

- Go to www.dell.com/ismmanuals.com.
- Click the desired version of iDRAC Service Module.
- Click **Manuals & Documents**.

Accessing documents using direct links

Table 2. Direct links for documents

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


Accessing documents using the product search

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, PowerEdge or iDRAC. A list of matching products is displayed.
3. Select your product and click the search icon or press enter.
4. Click **Manuals & documents**.

Accessing documents using the product selector

You can also access documents by selecting your product.

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

 **NOTE:** For some products, you may need to navigate through the subcategories.
5. Click **Manuals & documents**.

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

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 3. PowerEdge servers naming convention and examples

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

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.