Rev. A04
December 2021

Dell EMC iDRAC Service Module 4.1.0.0 Release Notes

Current Release Version: 4.1.0.0
Previous Release Version: 4.0.1

Topics:

Revision History

Table 1. Document revision history

Document revision	Date	Description
A00	July 2021	Initial release
A01	September 2021	Added Microsoft Windows Server 2022 Added JIT-205713 to known issues
A02	October 2021	Added R250, R350, T150, and T350 platform support Added VMware vSphere ESXi 7.0 U3 operating system support Added JIT-202946 to limitations
A03	October 2021	Added T550 platform support
A04	December 2021	Added Red Hat Enterprise Linux 8.5 operating system support Added new client operating system for Dell EMC Precision R7920 Added JIT-212613 and JIT-211318 to known issues

Product Description

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

Version

iDRAC Service Module 4.1.0.0

Release date

July 2021

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.

New in this release

New supported operating systems

iDRAC Service Module 4.1.0.0 supports the following operating systems:

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8.5
- Red Hat Enterprise Linux 8.4
- SUSE Linux Enterprise Server 15 SP3
- Ubuntu Server 20.04.2 LTS
- VMware vSphere ESXi 7.0 U3

iDRAC Service Module 4.1.0.0 supports the following new client operating systems on Dell EMC Precision R7920:

- Red Hat Enterprise Linux 8
- Microsoft Windows 10
- Microsoft Windows 11 Pro
- Ubuntu Desktop 20.04 LTS

New and enhanced features

The following are the new and enhanced features of iDRAC Service Module 4.1.0.0:

- OMSA SNMP alerts mapping — iSM can now send SNMP traps from the host operating system in OMSA format when this feature is enabled.
- Yellowdog Updater, Modified (YUM) — System administrators can deploy iSM using the YUM tool for Red Hat Enterprise Linux operating systems. The Dell YUM repository is updated with new artifacts when a new version is released.
- Enhanced iDRAC Service Module firewall rules update on Linux operating systems — Additional firewall rules relevant to iSM has been added to facilitate uninterrupted iSM communication with iDRAC.
- Enhanced iDRACHardReset on VMWare ESXi operating systems —The iDRACHardReset operation is supported when secure boot option is enabled in the BIOS.
- Enhanced support for normal lockdown mode on VMWare ESXi 7.x operating systems with administrative privileges.

  For more information, see VMWare ESXi lockdown mode.
- Performance improvement for establishing iSM communication with iDRAC on VMWare ESXi operating systems.

Compatibility

License requirements

For information regarding license agreements, see *iDRAC Service Module 4.1.0.0 User's Guide* available at www.dell.com/ismmanuals.

Supported platforms

iDRAC Service Module 4.1.0.0 supports PowerEdge yx2x to yx5x generation of servers. See Identifying the series of your Dell EMC PowerEdge servers for more information.

Table 2. iDRAC Service Module 4.1.0.0 supported platforms.

Supported Dell EMC PowerEdge servers			
PowerEdge yx5x servers	**PowerEdge yx4x servers**	**PowerEdge yx3x servers**	**PowerEdge yx2x servers**
PowerEdge C6520	PowerEdge C6420	PowerEdge C4130	PowerEdge FM120
PowerEdge C6525	PowerEdge FC640	PowerEdge C6320	PowerEdge M420
PowerEdge MX750c	PowerEdge FD332	PowerEdge FC430	PowerEdge M520
PowerEdge R250	PowerEdge M640	PowerEdge FC630	PowerEdge M620
PowerEdge R350	PowerEdge M640-VRTX	PowerEdge FC830	PowerEdge M820
PowerEdge R450	PowerEdge MX740c	PowerEdge M630	PowerEdge R220
PowerEdge R550	PowerEdge MX840c	PowerEdge M630-VRTX	PowerEdge R320
PowerEdge R650	PowerEdge R240	PowerEdge M830	PowerEdge R420
PowerEdge R650XS	PowerEdge R340	PowerEdge R230	PowerEdge R620
PowerEdge R6515	PowerEdge R440	PowerEdge R330	PowerEdge R720
PowerEdge R6525	PowerEdge R540	PowerEdge R430	PowerEdge R720XD
PowerEdge R750	PowerEdge R640	PowerEdge R530	PowerEdge R820
PowerEdge R750xa	PowerEdge R6415	PowerEdge R630	PowerEdge R920
PowerEdge R750XS	PowerEdge R740	PowerEdge R730	PowerEdge T320
PowerEdge R7515	PowerEdge R740xd	PowerEdge R730xd	PowerEdge T420
PowerEdge R7525	PowerEdge R740xd2	PowerEdge R830	PowerEdge T620
PowerEdge T150	PowerEdge R7415	PowerEdge R930	
PowerEdge T350	PowerEdge R7425	PowerEdge T130	
PowerEdge T550	PowerEdge R840	PowerEdge T330	
PowerEdge XR11	PowerEdge R940	PowerEdge T430	
PowerEdge XR12	PowerEdge R940xa	PowerEdge T630	
PowerEdge XE8545	PowerEdge T140		
	PowerEdge T340		
	PowerEdge T440		
	PowerEdge T640		
	PowerEdge XE7420		
	PowerEdge XE7440		

Supported operating systems and hypervisors

iDRAC Service Module 4.1.0.0 support is available on 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 20.04.02 LTS
- VMware vSphere (ESXi) 7.0 U3 supported on PowerEdge yx3x, yx4x, and yx5x servers.
- VMware vSphere (ESXi) 7.0 U2 supported on PowerEdge yx3x, yx4x, and yx5x servers.
- VMware vSphere (ESXi) 6.7 U3 supported on PowerEdge yx3x, yx4x, and yx5x servers.

For more information on the supported operating system and platform matrix, see the *Dell EMC iDRAC Service Module User's Guide* available at www.dell.com/idracmanuals

Fixed issues

The following are the fixed issues in iDRAC Service Module 4.1.0.0 :

- iSM ungraceful exit when network interface is configured with WireGuard VPN on Linux operating systems.
- Recommended file privileges are updated for iSM configuration files.
- iSM communication with iDRAC ends when hostd service on VMWare ESXi is stopped or restarted.
- When iDRAC Service Module creates the virtual switch, NIC teaming failover order status for vusb0 interface is set to 'standby' by default.

Known issues

Common Issues

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

Table 3. Common issues

Issue ID	Functional area	Description	Workaround
180859	iSM communication restart is observed in both iDRAC Lifecycle Log files and operating system log files	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. `Log Message: ISM0007 The iDRAC Service Module communication with iDRAC has ended.`	No action is required as iSM communication is restored automatically within 1–2 minutes.
159410	Increased workload on the host interrupts communication between iSM and iDRAC	When the workload on the host increases 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`	The connection automatically resumes and no action is required.

Table 3. Common issues (continued)

Issue ID	Functional area	Description	Workaround
		`Service Module communication with iDRAC has ended.`	
161262	ISM0003 event message after replacing the system board	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.
193255	Enabling operating system information	On enabling operating system information when iSM is installed, IPv6 default gateway address and DNS server fields are not rendered in the iDRAC interfaces.	Not available.
212613	iDRAC GUI launcher fails with OS2iDRAC	iDRAC GUI launcher fails with OS2iDRAC, and **400-Bad Request** error is received while using an ErrorDocument to handle the request.	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 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.

Known issues on Microsoft Windows operating system

Table 4. Known issues on Microsoft Windows operating system

Issue ID	Functional area	Description	Workaround
157981	An internal error occurred when running the DCIM_View class	When DCIM_View class is enumerated with any WSMAN client through the iSM **WMI Info** feature on PowerEdge yx5x 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` The failure is because the DCIM_VFlashView class is deprecated	Enumerate the explicit classes such as DCIM_CPUView, DCIM_FANView, and so on

Table 4. Known issues on Microsoft Windows operating system (continued)

Issue ID	Functional area	Description	Workaround
		starting with the iDRAC firmware version 4.00.00.00.	
87075	A popup is displayed when uninstalling iSM	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.
157981	Running WMI MOF query on DCIM results with no data	When a Windows management instrumentation (WMI) MOF query is run on DCIM_View classes using iSM, no data is populated.	No action is required
138538 146421	iSM communication with iDRAC switches from IPv6 to IPv4	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.	No action is required
193621	Warning message in the Application Logs section	When iDRAC Service Module is installed on Microsoft Windows operating system, the following warning message is observed in the Application Logs section of Windows Event Viewer. `A provider, ismserviceprovider, has been registered in the Windows Management Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.`	No action is required
185544	Critical alert related to ChipsetDriver.exe displayed in operating system logs	When OpenManage Server Administrator is installed on yx3x servers and Tech Support Report (TSR) is requested from any of iDRAC interfaces, then a critical alert that is related to ChipsetDriver.exe is displayed in the operating system logs.	The alert can be ignored and no action is required.
211318	OSC data on SupportAssist collection report	On Microsoft Windows 11 Pro operating system, the SupportAssist collection report does not contain OSC data when collected using invoke script.	Not available

Known issues on Linux operating system

Table 5. Known issues on Linux operating system

Issue ID	Functional area	Description	Workaround
Not available	ipmi_si IPMI_driver does not respond after iDRAC hard reset.	After performing an iDRAC hard reset operation on certain Linux operating systems, the ipmi_si, IPMI driver may not	The issue occurs in Linux kernel version earlier to 3.15. An update is available in the following operating

Table 5. Known issues on Linux operating system (continued)

Issue ID	Functional area	Description	Workaround
		respond because of an existing issue in the IPMI driver. If the IPMI driver stops responding, reload the ipmi_si IPMI driver.	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
102480	AVC denial with iptables	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	iSM does not support explicit SELinux policies. There is no functionality impact to iSM features.
124514	A message is displayed when invoking iDRAC GUI Launcher for the first time.	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")"`	There is no functional impact. No action is required.

Known issues on VMware ESXi operating system

Table 6. Known issues on VMware ESXi operating system

Issue ID	Functional area	Description	Workaround
172915	iSM communication with iDRAC is interrupted.	In VMware ESXi 7.x, iDRAC Service Module (iSM) communication with iDRAC is dropped.	No action is required as the communication is restored automatically within 1–2 minutes.

Table 6. Known issues on VMware ESXi operating system (continued)

Issue ID	Functional area	Description	Workaround
176426	Communication is not restarting after performing Restart Management Agents.	iDRAC Service Module is not restarting the communication with iDRAC after performing **Restart Management Agents** on VMWare ESXi 7.x.	Perform the **Restart Management Agents** again immediately after the first attempt.
Not available.	IPMI driver becomes unresponsive on VMware ESXi.	After performing an iDRAC hard reset operation on certain VMware ESXi, the ipmi_si_drv IPMI driver on ESXi 6.x and ipmi IPMI drive on ESXi 6.x/7.x 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.x and ipmi IPMI drive on ESXi 6.x/7.x.	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.
188568	Invoke-FullPowerCycle	The iSM feature "Invoke-FullPowerCycle" is not supported when the "SMM Security Mitigation" is enabled from the BIOS on VMware ESXi 7.x operating systems.	Not available.
205713	Installing iSM using vSphere Lifecycle Manager (vLCM) image-based method in vSphere Client (VC).	On VMware ESXi 7.0 U2, when installing iSM using vSphere Lifecycle Manager (vLCM) image-based method in vSphere Client (VC), during remediation process, the following noncompliant error message is displayed: `A failure occurred when starting a host compliance check operation on host: Error: com.vmware.vapi.std.errors.internal_server_error Messages: com.vmware.esx.task.exec.error <Failed to start the task. Please ensure the system has enough resources and retry.>` However, iSM is installed successfully on ESXi host.	Reboot ESXi host and run the **Check Compliance** option in vSphere Client (VC) to resolve the issue.

Limitations

Common limitations

The following limitations are applicable to all the operating systems.

Table 7. Common limitations

Issue ID	Functional area	Description	Workaround
158667 159019 158514 158740	Interruption in communication between iDRAC and iSM.	When the workload on the host increases due to intensive task requests by the processor, the communication between iDRAC Service Module and iDRAC is interrupted for a moment and restored automatically.	Not applicable
Not available	Communication between iSM and iDRAC is not established.	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.	Not applicable
Not available	iSM Host SNMP OMSA alert	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, first you must 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.
Not available	iDRAC to OMSA SNMP alert mapping	iDRAC to OMSA SNMP alert mapping is enabled when OMSA is running.	To disable iSM Host SNMP OMSA alert, restart the iDRAC Service Module.

Limitations on Microsoft Windows operating system

Table 8. Limitations on Microsoft Windows operating system

Issue ID	Functional area	Description
115250	Installing iSM on Microsoft Windows operating systems.	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.
169898	Lifecycle Controller log files not listed in the Event Viewer .	You cannot view Lifecycle Controller log files in the new folder in the Event Viewer, 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

Table 8. Limitations on Microsoft Windows operating system (continued)

Issue ID	Functional area	Description
		to view the Lifecycle Controller log files under the new view name.
Not available	Custom installation paths for installing iSM.	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.
Not available	Enabling and disabling feature.	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.
Not available	IPv6 support	IPv6 support is not available for the following features: ● iSM Auto Update ● Inband iDRAC Access ● SNMP Get via Host OS

Limitations on Linux operating system

Table 9. Limitations on Linux operating system

Issue ID	Functional area	Description
202946	NVMe prepare to remove operation.	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.
132983	Enabling the InBand iDRAC Access feature.	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.
088419	Lifecycle Log Replication feature.	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.
Not available	IPv6 support on Linux operating systems.	IPv6 support on Linux operating systems is not available for the following features: ● iSM Auto Update ● Inband iDRAC Access ● SNMP Get via Host OS

Limitations on VMware ESXi operating system

Table 10. Limitations on VMware ESXi operating system

Issue ID	Functional area	Description	Workaround
148591	Upgrading an earlier version of ESXi to ESXi 7.x.	Upgrading an earlier version of ESXi to ESXi 7.x fails 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	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.

Table 10. Limitations on VMware ESXi operating system (continued)

Issue ID	Functional area	Description	Workaround
		7.x on Dell EMC PowerEdge Servers Release Notes.	
Not available	Non-functional iSM-Windows remote management commands.	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.	Use the `Invoke-iDRACHardReset` command line utility to perform the iDRAC Hardreset operation.
Not available	iDRAC Access via Host OS.	The iDRAC Access via Host OS feature is not supported on VMware ESXi operating systems.	Not applicable
Not available	Local Racadm.	When Local Racadm set is disabled through iDRAC interfaces: ● iSM fails to configure the operating system to iDRAC pass-through in the USB NIC mode. ● iSM functionality is restored when Local Racadm set is enabled.	Not applicable
Not available	Lifecycle Controller logs.	EventID for Lifecycle Controller logs replicated to operating system log will be 0 for some of the past events.	Not applicable
Not available	In-band SNMP Trap	TrapID for In-band SNMP Traps will be 0 for some of the past traps.	Not applicable
87572	iDRAC Hardreset	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.	Not applicable
Not available	iDRAC Hardreset operation on VMware ESXi.	To perform iDRAC hard reset operation on VMware ESXi operating system using the `winrm` command, the iSM must be communicating with iDRAC.	Not applicable
160283	iSM command-line utility	When any iSM command-line utility running on the VMware ESXi operating system is interrupted, you can not remove the iSM VIB using the same terminal.	Use another terminal to remove the iSM VIB.
Not available	NVMe Prepare to remove operation	The NVMe Prepare to remove operation is not supported on the VMware ESXi operating system when the NVMe device is configured as a pass-through device.	Not applicable

User notes

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 Linux operating systems

- To perform an **Express Install** on Linux 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 4.1.0.0 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 11. 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. 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 https://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**.

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 12. 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

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.

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.**