Dell EMC iDRAC Service Module 3.5.1

Release Notes

October 2020
Rev. A04

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

Release summary

The Integrated Dell Remote Access Controller (iDRAC) Service Module (iSM) is a lightweight optional software application that can be installed on the yx2x PowerEdge servers or later. This release of iSM supports new operating systems, and existing feature enhancements.

Topics:

Version

iDRAC Service Module version 3.5.1

Release date

May 2020

Priority and recommendations

Recommended: Dell 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 (Firmware, BIOS, drivers, and software).

2

Compatibility

Topics:

License Requirements

For information about license agreements, see *iDRAC Service Module 3.5.1 User's Guide* available at www.dell.com/ismmanuals.com.

Supported Platforms

iDRAC Service Module 3.5.1 supports yx2x to yx5x series PowerEdge servers.

Supported Systems

Table 1. The table lists the platforms that are supported by iDRAC Service Module 3.5.1.

yx5x PowerEdge servers	yx4x PowerEdge servers	yx3x PowerEdge servers	yx2x PowerEdge servers
R6515	XE2420	C4130	FM120
R7515	T140	C6320	M420
R6525	T340	FC430	M520
C6525	R240	FC630	M620
R7525	R340	FC830	M820
	R740xd2	M630 VRTX	R220
	MX740c	M630	R320
	MX840c	M830	R420
	R840	R230	R620
	R940xa	R330	R720
	R7425	R430	R720xd
	R7415	R530	R820
	R6415	R630	R920
	C6420	R730	T320
	FC640	R730xd	T420
	FD332	R830	T620
	M640	R930	
	M640 VRTX	T130	

Table 1. The table lists the platforms that are supported by iDRAC Service Module 3.5.1. (continued)

yx5x PowerEdge servers	yx4x PowerEdge servers	yx3x PowerEdge servers	yx2x PowerEdge servers
	R440	T330	
	R540	T430	
	R640	T630	
	R740		
	R740xd		
	R940		
	T440		
	T640		
	C4140		

Previous versions

- iDRAC Service Module 3.5.0
- 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 managed server operating systems and hypervisors

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.2
- Red Hat Enterprise Linux 8.1
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.7
- SUSE Linux Enterprise Server 15 SP1
- VMware vSphere (ESXi) 7.0 U1 (Supported on yx3x*, yx4x and yx5x PowerEdge servers)
- VMware vSphere (ESXi) 7.0 (Supported on yx3x*, yx4x and yx5x PowerEdge servers)
- VMware vSphere (ESXi) 6.7 U3 (Supported on yx3x, yx4x and yx5x PowerEdge servers)
- VMware vSphere (ESXi) 6.5 U3 (Supported on yx3x, yx4x, and yx5x PowerEdge servers)
- Ubuntu 18.04.3

* - Only few yx3x PowerEdge servers support VMware ESXi 7.0 and ESXi 7.0 U1. To know the list of supported yx3x PowerEdge servers, see VMware vSphere 7.x on Dell EMC PowerEdge Servers Compatibility Matrix.

3

New and enhanced features

- Supports VMware vSphere (ESXi) 7.0 U1
- Supports VMware vSphere (ESXi) 7.0
- Fixes on Microsoft Windows, Linux, and ESXi operating systems:
  - iSM (v3.4.0 or later) communication with iDRAC failure when iDRAC firmware is upgraded to 3.30.30.30 or later
  - iSM (v3.4.0 or later) communication with iDRAC failure when iDRAC firmware is downgraded from any recent version to a version less than 3.30.30.30
- Fixes on Microsoft Windows operating systems only:
  - Ungraceful iSM process termination when S.M.A.R.T Monitoring feature is enabled and when the host has more than 64 drives connected.
  - Updated iSM-supported WMI MOF classes.
- Fixes on VMware ESXi operating systems only:
  - iSM v3.4.0 or later communication failure with iDRAC when VMware ESXi is upgraded from ESXi 6.5 to ESXi 6.7.
  - Security policy updated for the vSwitch created by iSM.

4

Known issues

- **Issue 1:**

  Description:

  When OpenManage Server Administrator (OMSA) is installed on the host operating system, the iDRAC Service Module (iSM) communication with iDRAC will end after every 5 hours 30 minutes. No action is required by the user as the iSM communication with iDRAC is automatically restored.

  Workaround: There is no workaround available.

  Tracking number: 173281

- **Issue 2:**

  Description: When an incorrect SupportAssist proxy details are provided during the registration, a SIGKILL error message is logged by kernel in the operating system event log, while stopping iDRAC Service Module (iSM). There might be a semaphore leak because the iSM process is forcibly stopped by the kernel.

  Workaround: There is no workaround available.

  Tracking number: 161600

- **Issue 2**

Description:

When the customer has set the iDRAC DNS name with 27 characters or multiples of 27 characters, iSM communication with iDRAC is not established and TLS Error is reported. The following message is logged in the operating system event log:

```
The iDRAC Service Module (iSM) is unable to communicate with iDRAC because the client or server certificate is either unavailable or invalid
```

Workaround:

1. Reset iDRAC to factory defaults using the Reset iDRAC to Default Settings option.
2. Modify the iDRAC DNS name with a length of characters other than multiples of 27 characters.
3. Enable the USB NIC.
4. Manually start the iDRAC Service Module (iSM) service on the host operating system. To start the iSM service manually, do the following with respect to the host operating system:
   - On Microsoft Windows operating system, go to the Services menu, and start the iSM service as an Administrator.
   - On Linux operating system, start dcism as a user by using the command `systemctl start dcismeng.service` with the administrator or root privileges.

Tracking number: 165380

- **Issue 4**

Description:

When OSCollector Dup is updated on the iDRAC, the Job Queue page displays the job as "Firmware Update: Diagnostics" instead of OSCollector.

Workaround: There is no workaround available.

Tracking number: 139485, 139088, 141091.

- **Issue 5**

Description:

When Federal Information Processing Standards (FIPS) mode is enabled on the host operating system, communication between iDRAC Service Module and iDRAC is not established.

Workaround: There is no workaround available.

Tracking number: 158514, 158740, 158667, 159019.

- **Issue 6**

Description:

When there is increased workload on the host due to intensive task requests by the CPU, communication between iDRAC Service Module and iDRAC is temporarily interrupted with the warning message, `The iDRAC Service Module communication with iDRAC has ended` in the lifecycle log. The connection automatically resumes and no action is required by the user.

Workaround: There is no workaround available.

Tracking number: 159410

- **Issue 7**

Description:

If a USB NIC is enabled after the motherboard is replaced without restoring the configuration or after the iDRAC is reset to factory settings, the user can observe ISM0003 on operating system logs before starting the communication with an error message, `The iDRAC Service Module is unable to discover iDRAC from the operating system of the server`. No action is required by the user.

Workaround: There is no workaround available.

Tracking number: 161262

Topics:

Known issues on Microsoft Windows operating systems

- **Description:** On Microsoft Windows 2016 server operating system, if you do iDRAC factory reset and when iSM is installed using repair option, sometimes the communication between the iSM and iDRAC is not established.

  Workaround: There is no workaround available.

  Tracking number: 161320

- **Description:** When you run the Windows Management Instrumentation MOF query on **DCIM_View** and **DCIM_EnclosureView** classes using iSM, data will not be populated.

  Workaround: There is no workaround available.

  Tracking number: 157967and 157981

- **Description:** You can configure the Windows Remote Management (WinRM) Listener using a server authenticating certificate. If the server authenticating certificate is not available, iDRAC Service module will force-enable the WinRM listener using a self-signed certificate.

  To configure the Windows Remote Management (WinRM) listener, you can create a self-signed certificate using the PowerShell `cmdlet New-SelfSignedCertificate` from Microsoft Windows Server 2012 or later. In operating systems prior to Microsoft Windows Server 2012, you cannot create a self-signed certificate due to the absence of PowerShell `cmdlet`.

  Workaround: There is no workaround available.

  Tracking number: Not available.

- **Description:** While uninstalling "iDRAC Service Module" a popup is displayed if the Firefox browser is opened. The popup prompts that Firefox browser needs to be closed before continuing the uninstallation. Close the Firefox browser and click the "Retry" option to continue the uninstallation.

  Workaround: There is no workaround available.

  Tracking number: 87075.

- **Description:** When a user performs a Windows Management Instrumentation (WMI) query on the DCIM_Account, DCIM_AccountManagementCapabilities, DCIM_AccountManagementService, and DCIM_ADMProfilesConcreteCollection

classes, using an iDRAC Service Module on iDRAC firmware 4.00.00.00 or later, a MOF query will fail with an error message, `CLASS_NOT_FOUND`. No action is required by the user.

Workaround: No workaround available for this issue.

Tracking number: 159276

- **Description:** While performing a repair or modify operation on a Microsoft Windows 2016 operating system installation, occasionally the communication between the iDRAC Service Module and iDRAC is not established. Retry the operation.

  Workaround: There is no workaround available.

  Tracking number: 161320

Known issues on Linux operating systems

- **Description:** On Linux operating system, when IPv4 address of OS2iDRAC Passthrough interface is deleted on the host, iDRAC Service Module logs the below message before restarting communication with iDRAC using IPv6:

  ```
  The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC
  Pass-through channel.
  ```

  Workaround: There is no workaround available.

  Tracking number: 173559

- **Description:** After performing an iDRAC hard reset operation on certain Linux operating systems, the IPMI driver (ipmi_si) may become unresponsive because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the IPMI driver (ipmi_si).

  Workaround: The issue occurs in Linux kernel version prior to 3.15. An update is available in the following operating systems with Linux kernal version 3.15 or later.

  Steps to reload the IPMI driver:

  - `modprobe -r ipmi_si`: If the removal fails, then all applications (such as iDRAC Service Module and OpenManage Server Administrator) using the `ipmi_si` need to be stopped and retry the operation.
  - `modprobe ipmi_si`: Alternatively, the administrator can also restart the Host OS to resolve the issue.

  IPv6 support on Linux operating systems are not available for the following features:

  - iSM Auto Update
  - ismtechInband iDRAC Access

- **Description:** When an iDRAC Service Module 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.

  Workaround: There is no workaround available.

- **Description:** When an iDRAC Service Module 3.3.0 or later is installed on RHEL 6.10 Operating System with SELinux enabled in either of Permissive or Enforcing modes, AVC denial logs (AVC denial is noticed with iptables) are observed in `/var/log/audit/audit.log` while the following features are enabled or disabled:

  - iDRAC Access via Host OS
  - Host SNMP Alerts

  Workaround: iDRAC Service Module 3.3.0 and later does not support explicit SELinux policies. No action is expected from the user. There is no functionality impact to iSM features due to this. Future releases of iSM shall address the AVC denials.

  Tracking number: 102480

- **Description:** When TLS capable iSM (Example: iSM 3.4.0) is installed on Linux OSs' and the iSM client certificate name is modified and iSM service is restarted, then iSM communication with iDRAC ends.

  Workaround: As a workaround, user has to uninstall and install iSM 3.4.0

  Tracking number: 114656

- **Description:** If the third octet of USBNIC IPv4 address is modified in iDRAC, then the iDRAC Service Module communication with iDRAC will end.

Workaround: There is no workaround available.

Tracking number: 118654

- **Description:** When invoking "iDRAC GUI Launcher" for the first time either using iDRACLauncher.sh or using the program menu shortcut, the following message will be seen in operating system logs.

```
"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")"
```

Workaround: There is no functional impact. No action is required by the user.

Tracking number: 124514

- **Description:** If Support Assist Collection(TSR) is triggered on 13G platforms, it is failing under the following conditions,
  - The maser device which is exposed to OS by iDRAC during the SA collection but it is failing to mount /mnt since it is already mounted by Administrator with read-only file system or no access permission. Once the failure occurs, the Support assist collection will be blocked by iDRAC for 30 mins.

Workaround:

- OS root user or Administrator need to unmount `/mnt`.

(OR)

- Instead of using `/mnt` directly as mount point, OS user/Administrator need to create a separate directory under `/mnt` and use that directory for their activity.

Tracking number: 146515

Known issues on VMware ESXi

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

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

  Tracking number: 176426

- **Description:** When user performs Prepare to Remove operation using the Dell Express Flash NVMe ColdStream P4800x drive on VMware ESXi 7.0 and ESXi 7.0 U1 operating system, the operation fails.

  Workaround: There is no workaround available.

  Tracking number: 169748

- **Description:** Sometimes after updating the iDRAC firmware or BIOS, iSM communication with iDRAC is terminated and the following log message is logged in the operating system.

```
ISM0011 : The server operating system (OS) is unable to start the iDRAC Service
Module, because it is set to "disabled" in iDRAC.
```

  Restarting wbem service using the following commands will establish the iSM communication with iDRAC:

```
*esxcli system wbem set -e 0
```

```
* esxcli system wbem set -e 1
```

  Workaround: There is no workaround available.

  Tracking number: 167495

- **Description:** Upgrading an earlier version of ESXi to ESXi 7.0 is failing with iSM VIB installed. In 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

- **Description:** After performing an iDRAC Hard Reset operation on certain VMware ESXi operating systems, the IPMI driver (ipmi_si_drv on ESXi 6.5U2 and ipmi on ESXi 6.7 U1 Operating Systems) may become unresponsive because of an existing issue in the IPMI driver. If the IPMI driver becomes unresponsive, reload the IPMI driver (ipmi_si_drv on ESXi 6.5U2 and ipmi on ESXi 6.7U1 Operating System).

  Workaround: The issue is observed on iDRAC Service Module v2.3 and later supported ESXi versions.

  To reload the IPMI driver:

  - If the removal fails, then all applications (such as iDRAC Service Module and OpenManage Server Administrator) using the ipmi_si must be stopped and retry the operation.

    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
    esxcli system wbem set -e 1
    ```

    Tracking number: Not available

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

- **Description:** To perform iDRAC Hard Reset operation on VMware ESXi operating system using `winrm` command, iDRAC Service Module should be successfully communicating with iDRAC.

  Workaround: There is no workaround available.

  Tracking number: Not available

5

Limitations

Topics:

Limitations on Microsoft Windows operating systems

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

  Original source path of the file is now found

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

  Tracking number : 115250
- On Windows operating system, 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.
- Communication between iDRAC Service Module and iDRAC over IPv6 will work only on iDRAC firmware 2.70.70.70 or later.

Limitations on Linux operating system

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

  Tracking number: BITS088419
- When iDRAC Hard Reset is disabled in iDRAC and you perform **iDRACHardReset** from the Hypervidor operating systems such as Citrx Xen, the result indicates success although iDRAC is not reset.

  Tracking number: 87572
- When iDRAC Service Module is communicating with iDRAC using IPv6 protocol, enabling the feature "InBand iDRAC Access" indicates a successful message. But this feature is unavailable over IPv6 protocol. No action is required by the user.

  Tracking number: 132983
- Communication between iDRAC Service Module and iDRAC over IPv6 will work only on iDRAC firmware 2.70.70.70 or later.
- On Red Hat Enterprise Linux 8.0 and Red Hat Enterprise Linux 8.1 Operating systems, unable to upload Support Assist Collection report to backend.

  Tracking number: JIT-148281

Limitations on VMware ESXi operating systems

- When the small footprint CIM broker (SFCB) configuration is set to read only mode in VMware ESXi operating system, iSM-Windows remote management (WinRM) commands such as `iDRACHardreset`, and `EnableInBandSNMPTraps` does not function.

  Workaround: User can use `Invoke-iDRACHardReset` utility to perform the iDRAC hard reset operation.

- The iDRAC Access via Host OS feature is not supported on VMware ESXi Operating Systems.
- When Local Racadm set is disabled through iDRAC interfaces:
  - iDRAC Service Module will fail to configure the OS to iDRAC Pass-through in the USB NIC mode.
  - iDRAC Service Module functionality is restored when Local racadm set is enabled.
- EventID for Lifecycle Controller Logs replicated to OS 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 Hard Reset is disabled in iDRAC and user performs iDRACHardReset from the Hypervisor operating systems like VMware ESXi, the result indicates success although iDRAC is not reset.

6

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
```

7

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
  ```

8

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 version of iDRAC Service Module.
- Clicks **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/cmcmanuals	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

9

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/contactdell**.

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.