

# **Dell EMC iDRAC Service Module 3.5**

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.

© 2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

# Contents

<b>1 Release Summary.....</b>	<b>4</b>
Version.....	4
Release Date.....	4
Priority and recommendations.....	4
<b>2 Compatibility.....</b>	<b>5</b>
License Requirements.....	5
Supported Platforms.....	5
Previous Versions.....	6
Supported managed server operating systems and hypervisors.....	6
<b>3 New and enhanced features.....</b>	<b>7</b>
<b>4 Known Issues.....</b>	<b>8</b>
Known issues on Microsoft Windows operating system.....	8
Known issues on Linux operating systems .....	8
Known issues on VMware ESXi operating systems.....	9
<b>5 Limitations.....</b>	<b>11</b>
Limitations on Microsoft Windows operating systems.....	11
Limitations on Linux operating system.....	11
Limitations on VMware ESXi operating systems.....	11
<b>6 User notes for supported Microsoft Windows operating systems.....</b>	<b>12</b>
<b>7 User notes for supported Red Hat Enterprise Linux and SUSE Linux Enterprise Server.....</b>	<b>13</b>
<b>8 Resources and support.....</b>	<b>14</b>
<b>9 Contacting Dell EMC .....</b>	<b>15</b>

# 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 generation of PowerEdge servers or later. This release of iDRAC Service Module adds support for Red Hat Enterprise Linux 8.1, Red Hat Enterprise Linux 8.0, Red Hat Enterprise Linux 7.7 and additional security features.

## Topics:

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

## Version

iDRAC Service Module version 3.5

Version : A01

## Release Date

February 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).

# Compatibility

## License Requirements

For information regarding license agreements, go to iDRAC Service Module 3.5 User's Guide available at [www.dell.com/ismmanuals](http://www.dell.com/ismmanuals)

## Supported Platforms

iDRAC Service Module 3.5 supports yx2x to yx5x generation of PowerEdge servers.

## Supported Systems

The table lists the platforms that are supported by iDRAC Service Module 3.5.

<b>yx5x servers</b>	<b>yx4x servers</b>	<b>yx3x servers</b>	<b>yx2x servers</b>
R6515	T140	C4130	FM120
R7515	T340	C6320	M420
R6525	R240	FC430	M520
C6525	R340	FC630	M620
R7525	R740xd2	FC830	M820
	MX740c	M630 VRTX	R220
	MX840c	M630	R320
	R840	M830	R420
	R940xa	R230	R620
	R7425	R330	R720
	R7415	R430	R720 XD
	R6415	R530	R820
	C6420	R630	R920
	FC640	R730	T320
	FD332	R730xd	T420
	M640	R830	T620
	M640-VRTX	R930	
	R440	T130	
	R540	T330	
	R640	T430	
	R740	T630	
	R740xd		
	R940		
	T440		
	T640		

## Previous Versions

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

## Supported managed server operating systems and hypervisors

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 8.1 operating system
- Red Hat Enterprise Linux 8.0 operating system
- Red Hat Enterprise Linux 7.7 operating system
- SUSE Linux Enterprise Server 15 SP1
- VMware vSphere (ESXi) 6.5 U3 (Support for yx3x, yx4x and yx5x servers)
- VMware vSphere (ESXi) 6.7 U3 (Support for yx3x, yx4x and yx5x servers)
- Ubuntu 18.04.3

## New and enhanced features

- Support for yx5x server R7525
- Support for Red Hat Enterprise Linux 7.7 operating system (64-bit)
- Support for Red Hat Enterprise Linux 8.0 operating system (64-bit)
- Support for Ubuntu Server 18.04.03 LTS (64-bit)
- Support for VMware ESXi 6.7U3
- Support for VMware ESXi 6.5U3
- Support for Microsoft Windows 10 RS5 Client Operating System.
- Support for IPv6 communication between iDRAC Service Module and iDRAC over OS-BMC Passthru on Microsoft Windows Operating Systems.
- Secure loading of libraries to prevent DLL pre-loading attacks on Windows Operating Systems.
- Monitoring of S.M.A.R.T attributes of Chip-set SATA controller devices under AHCI mode.
- Inclusion of Chip-set SATA device's S.M.A.R.T logs into SupportAssist Collection.
- Support for Correlation of Software Events to Hardware failures for Microsoft Storage Spaces Direct(S2D).
- Inclusion of Storage Spaces Direct(S2D) logs into SupportAssist Collection.
- Single sign-on(SSO) to iDRAC GUI from Host OS over IPv6 ULA (iDRAC Firmware 4.00.00.00 or later) on administrator's desktop.
- SupportAssist Auto Dispatch for Disks (for below two events) for Linux Operating systems
  - Predictive failure reported for physical disk.
  - A bad disk block on <device> cannot be reassigned during a write operation.

## Known Issues

- **Description:**

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

**Workaround:** NA

**Tracking ID:** JIT-139485,JIT-139088,JIT-141091.

- **Description:** When iDRAC firmware is downgraded from 3.30.30.30 to a lower version, the communication between iDRAC and iDRAC Service module ends.

**Workaround:** User has to install iDRAC Service Module that is supported by the downgraded version of iDRAC installed.

### Topics:

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

## Known issues on Microsoft Windows operating system

- 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.

**Tracking ID:** NA.

- 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.

**Tracking ID:** 87075.

## Known issues on Linux operating systems

- **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 is seen on Linux kernel version prior 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 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 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.

**Workaround:** There is no workaround available.

- **Description:** When 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:** JIT-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:** JIT-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:** NA.

**Tracking number:** JIT-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:** JIT-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:** JIT-146515

## Known issues on VMware ESXi operating systems

- **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 6.7U1 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 need to 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
```

- Alternatively, the administrator can also restart the Host OS to resolve the issue .
- **Description:** To perform iDRAC Hard Reset operation on VMware ESXi operating system using `wiorm` command, iDRAC Service Module should be successfully communicating with iDRAC.

## Limitations

### 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 an 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 Hypervisor operating systems such as Citrix 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 IPv4 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

- 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.

# 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 documentation for iDRAC Service Module 3.5.

### Latest Released Documents

To access the latest version of iDRAC Service Module documents:

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

### Accessing documents using direct links

You can directly access the documents using the following links:


URL	Product
<a href="http://www.dell.com/idracmanuals">www.dell.com/idracmanuals</a>	iDRAC and Lifecycle Controller
<a href="http://www.dell.com/cmmanuals">www.dell.com/cmmanuals</a>	Chassis Management Controller (CMC)
<a href="http://www.dell.com/esmanuals">www.dell.com/esmanuals</a>	Enterprise System Management
<a href="http://www.dell.com/serviceabilitytools">www.dell.com/serviceabilitytools</a>	Serviceability Tools
<a href="http://www.dell.com/omconnectionsclient">www.dell.com/omconnectionsclient</a>	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**.

## 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](http://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.