

# **OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager**

## 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.

# Contents

<b>Chapter 1: Release type and definition</b> .....	<b>4</b>
Priority and recommendations.....	4
<b>Chapter 2: Compatibility</b> .....	<b>5</b>
Supported devices and platforms.....	5
<b>Chapter 3: What's new?</b> .....	<b>6</b>
<b>Chapter 4: Fixes</b> .....	<b>7</b>
<b>Chapter 5: Importance</b> .....	<b>8</b>
<b>Chapter 6: Known issues and resolutions</b> .....	<b>9</b>
<b>Chapter 7: Limitations</b> .....	<b>14</b>
<b>Chapter 8: Instructions for installing</b> .....	<b>16</b>
Installation prerequisites.....	16
Installation process.....	16
Upgrade instructions.....	16
<b>Chapter 9: Contacting Dell EMC</b> .....	<b>17</b>

# Release type and definition

## OpenManage Integration Version 7.3 for Microsoft System Center

OpenManage Integration for Microsoft System Center (OMIMSSC) is an appliance-based integration into System Center suite of products. OMIMSSC enables full lifecycle management of Dell EMC PowerEdge servers by using integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC).

OMIMSSC offers operating system deployment, Dell EMC HCI Solutions for Microsoft Windows server creation, hardware patching, firmware update, and maintenance of servers and modular systems. Integrate OMIMSSC with Microsoft Endpoint Configuration Manager (MECM) previously known as Microsoft System Center Configuration Manager (SCCM) for managing the Dell PowerEdge servers in traditional data center, integrate OMIMSSC with Microsoft System Center Virtual Machine Manager (SCVMM) for managing The Dell PowerEdge servers in virtual and cloud environments.

This release is the immediate successor of OMIMSSC version 7.2.1 for SCCM and SCVMM.

For information about MECM, SCVMM, and SCCM brand name change see, the Microsoft documentation.

### Version

7.3 Rev.A00

### Release date

May 2021

### Previous versions

OMIMSSC v7.2.1

## Priority and recommendations


Recommended: Dell EMC 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

## Supported devices and platforms

For more information about supported devices and platforms, see the **Support Matrix** section in the *OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Unified User's Guide*.

## What's new?

- Support for Microsoft Endpoint Configuration Manager (MECM) version 2103.
- Support for Microsoft Endpoint Configuration Manager (MECM) version 2010.
- Support for Microsoft Endpoint Configuration Manager (MECM) version 2006.
- Support for System Center Virtual Machine Manager (SCVMM) 2019 UR3.
- Support for System Center Virtual Machine Manager (SCVMM) 2019 UR2.
- Support for System Center Virtual Machine Manager (SCVMM) 2016 UR10.
- Support for custom SSL certificate management.
- Cluster-Aware Updates for HCI and Failover clusters now includes the capability to perform driver updates combined with BIOS and Firmware for Windows Server based clusters.
- Support for new Intel based iDRAC 9 based PowerEdge servers.
  - R450
  - R550
  - R650
  - R650xs
  - R750
  - R750xs
  - R750xa
  - C6520
  - XR11
  - XR12
  - MX750c
  - XE2420
- Support for creation of Windows Server based HCI clusters, management and Cluster Aware Update of AX nodes and S2D ready node.
  - AX6515
  - AX740xd
  - AX640
  - R440
- Support for WinPE driver injection using Dell EMC OpenManage server driver pack.
  -  **NOTE:** DTK is End of Life product from Dell EMC. Use Dell EMC OpenManage server driver pack for WinPE drivers.
- Support for ESXi operating system deployment versions 7.0 U2, 7.0 U1, and 6.7 U3.
- Support for RHEL operating system deployment versions 7.9, 8.0, 8.3, and 8.4.
- Restructured user document. (Installation guide, User's guide, and Troubleshooting information consolidated in a single unified document).
- Support for deploying the Dell EMC OMIMSSC appliance for OpenManage Integration for Microsoft Endpoint Configuration Manager (MECM) and System Center Virtual Machine Manager (SCVMM) version 7.3 on the following VMware ESXi versions using .ova file:
  - Version 6.5
  - Version 6.7
  - Version 7.0

along with the existing support for deploying Dell EMC OMIMSSC appliance for MECM and SCVMM on Hyper-V using .vhd file.

## Fixes

- During firmware update, the components that are selected for two identical servers get updated individually as per the selection that is made by the user.
- While creating HCI Solutions for Microsoft Windows server cluster, the Quality of Service policy for the Mellanox/Qlogic card on each cluster node allocates 50% to the SMB traffic as per recommendation.
- Windows operating system deployment from MECM console on Dell servers with PERC H730, H330 Adapter, H730 mini, H330 mini controller in BIOS boot mode is supported.
- In HCI Solutions for Microsoft Windows server operational template, the compliance comparison report with predefined operational template displays as **Compliant**.
- Filter on **Maintenance Center** is available for MX7000 Modular Systems.

## Importance

**URGENT:** Dell EMC recommends applying this update as soon as possible. The update contains changes to improve the reliability and availability of your Dell system.



# Known issues and resolutions

- **Issue 1**

**Description:**

System Center Administrator console will crash while importing OMIMSSC console extension in certain System Center versions. System Center versions where the issue may be seen : SC2016 VMM RTM build 4.0.1662.0, SC2012 VMM UR5 or later.

**Workaround:**

As a workaround for SC2016 VMM RTM build 4.0.1662.0 version, upgrade SCVMM using the 4094925 KB article available at [support.microsoft.com/kb/4094925](http://support.microsoft.com/kb/4094925), and then import the OMIMSSC console extension. For information about this issue in SC2012 VMM UR5 or later and resolving the issue, see issue 5 in the knowledge base URL: [support.microsoft.com/kb/2785682](http://support.microsoft.com/kb/2785682).

- **Issue 2**

**Description:**

After logging in to OMIMSSC Console extension for MECM with different credentials used to login to Microsoft console, the login activity fails with following error message: Failed to login. Ensure to use correct credentials or check if account is locked in Active Directory.

**Workaround:** As a workaround, ensure to use correct credentials or check if account is locked in Active Directory. For more information on Active Directory account lockout policies see, Microsoft Documentation.

- **Issue 3**

**Description:**

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2`. When you try to enroll with the above domain user account, the test connection fails.

**Workaround:**

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

- **Issue 4**

**Description:**

When accessing the OMIMSSC admin portal by using Mozilla Firefox browser, you get the following warning message: "Secure Connection Failed".

**Workaround:**

As a workaround, delete the certificate created from a previous entry of the admin portal in the browser. For information about deleting certificate from Mozilla Firefox browser, see [support.mozilla.org](http://support.mozilla.org)

- **Issue 7**

**Description:**

When a cluster is discovered in OMIMSSC, a cluster update group gets created in the **Maintenance Center** with all the servers listed in the cluster update group. Later, if all the servers are removed from this cluster through SCVMM, and an autodiscovery or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Maintenance Center**.

**Workaround:**

As a workaround, to delete the empty server group, rediscover the servers.

- **Issue 8**

**Description:**

Creating DRM update source on management server running on Windows 10 Operating System (OS) may fail, displaying the following error message: Failed to reach location of update source. Please try again with correct location and/or credentials.

Refer the **omimsscappliance\_main** log in OMIMSSC Admin portal, if the error message displayed is: `Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUT` where `EnableSMB1Protocol = false`.

- **Issue 9**

**Description:**

The **Deploy** option is not displayed in an existing task sequence after uninstalling and reinstalling OMIMSSC console extension for MECM.

**Workaround:**

As a workaround, open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option is displayed again.

- **Issue 10**

**Description:**

If the DHCP lookup fails while operating system deployment, then the server times out and the server is not moved into Managed Lifecycle Controller Lifecycle Controller (ESXi) collection in MECM.

**Workaround:**

As a workaround, install the MECM client server, and then perform a synchronization to add the servers in Managed Lifecycle Controller Lifecycle Controller (ESXi) collection.

- **Issue 13**

**Description:**

After scheduling an export server profile job, the server profile is not exported, and the following error message is displayed: `The selectors for the resource are not valid.`

**Workaround:**

As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see iDRAC documentation available at [dell.com/support](http://dell.com/support).

- **Issue 15**

**Description:**

After collecting the LC logs, when you try to view the LC log file for a server, the following error message is displayed: `"Failed to perform the requested action. For more information see the activity log"`.

**Workaround:**

As a workaround, reset iDRAC, and then collect and view the LC logs. For information about resetting iDRAC, see iDRAC documentation available at [dell.com/support](http://dell.com/support).

- **Issue 16**

**Description:**

After discovering the servers in OMIMSSC for MECM console extension, the server may not get added into **All Dell Lifecycle Controller Servers** collection.

**Workaround:**

As a workaround, delete the **All Dell Lifecycle Controller Servers** collection and then discover the server. The collection is automatically created in MECM and the server is added to this group.

- **Issue 17**

**Description:**

When you create a Windows server HCI cluster on nodes that were part of an existing cluster, then the storage pool and the disk configurations have the configurations of the existing cluster. Hence, the cluster storage pool might not be created and if the cluster storage pool is created the health status may be displayed as unknown.

**Workaround:**

As a workaround, clear the storage pool and disk configuration having existing cluster details and then create the Windows server HCI cluster. For more information on clearing the storage pool, see *Troubleshoot Windows server HCI health and operational states* section from Microsoft documentation.

- **Issue 18**

**Description:**

When multiple Microsoft consoles are enrolled to an OMIMSSC Appliance, and you try to discover a server, if even one of the MECM consoles are not reachable, then the server discovery job will fail.

**Workaround:**

As a workaround, de-enroll the MECM console that is not reachable, or fix the errors and ensure that the MECM console is reachable from OMIMSSC Appliance.

- **Issue 19**

**Description:**

When using Windows 2012 R2 operating system, the context sensitive online help content is launched displaying an error message.

**Workaround:**

As a solution, update the operating system using the latest KB articles, and then view the online help content.

- **Issue 20**

**Description:**

When you delete a server or all the servers in an update group from OMIMSSC, and rediscover them you cannot perform any other operations on these servers like updating firmware, exporting and importing LC logs, exporting and importing server profiles.

**Workaround:**

As a workaround, after rediscovering the deleted server or servers, perform firmware updates using the **Deploy Operational Template** feature in **Server View** and for other maintenance scenarios use iDRAC.

- **Issue 22**

**Description:**

After the firmware update of PowerEdge MX7000 components, the comparison report under **Available Updates** in the **Maintenance Center** page, displays incorrect number of updates even if the firmware update is successful.

**Workaround:**

As a work-around, go to **Maintenance Settings** and click **Test Connection** of update source that is used while updating the firmware. Go to **Maintenance Center** to view the correct number of updates.

- **Issue 23**

**Description:**

After de-enrolling SCVMM from the appliance, OMIMSSC page can still be opened through SCVMM console.

**Workaround:**

As a work-around, ensure to uninstall SCVMM console plug-in after de-enrolling SCVMM from the appliance.

- **Issue 24**

**Description:**

If the update source does not contain update for the selected device, the firmware update for complete MX chassis group does not complete.

**Workaround:**

Ensure to select devices for which updates are available in the selected update source.

Or

Select only the devices that have applicable updates which are based on the selected update source for firmware update job to complete.

- **Issue 25**

**Description:**

The Dell EMC Repository Manager (DRM) stops when repository of complete MX7000 chassis group is created using its inventory.xml file.

**Workaround:**

Select only MX7000 chassis and servers. Ensure that the inventory does not contain IOMs and storage sleds.

● **Issue 26**

**Description:**

While discovering servers using **IP Address Range** and specifying the IP addresses to exclude, if you change any IP value specified in the **IP Address Range** after specifying the IP address to exclude, the following error is displayed, The IP address range that you want to exclude is not within the specified IP address range.

**Workaround:**

As a workaround, do not change the **IP Address Range** values after you have specified the exclude IP address range to discover the servers.

● **Issue 27**

**Description:**

In the **Modular System View** page, the **Firmware Version** is not displayed after restoring the MX7000 modular system which is discovered in the previous version of OMIMSSC.

**Workaround:**

As a workaround, rediscover the MX7000 modular system to view the firmware version.

● **Issue 28**

**Description:**

In the **Maintenance Center** page, if disk attached to AHCI controller is attempted for an update through cluster aware method, the updated **Post Successful Update Version** of the disk component will not be reflected.

**Workaround:**

As a workaround, after the CAU job is completed, restart the cluster node or nodes where AHCI controller is an applicable update and refresh the inventory.

● **Issue 29**

**Description:**

In the **Maintenance Center** page, while performing **Run Update** using **Cluster Aware Update** method, user cannot update the firmware version of operating system driver pack.

**Workaround:**

As a workaround, you can update the operating system driver pack from iDRAC console, or can directly run the DUP on the node operating system.

● **Issue 30**

**Description:**

In **Modular Systems** view, Operational Template **Compliance Summary** displays noncompliant with zero noncompliant attributes for MX7000.

**Cause:**

If MX7000 discovered in OMIMSSC is at 1.10.00 firmware version, attributes present under following specified groups cannot be configured using modular system type Operational Template and these attributes should be modified outside of OMIMSSC

- LocalAccessConfiguration
- TimeConfig
- Power
- SessionConfiguration

**Workaround:**

Recapture the Operational Template and rerun the compliance.

● **Issue 31**

**Description:**

In the **Maintenance Center** page, on performing import device profile, using vFlash as a **Protection Vault**, imported firmware version of few components may not reflect .

**Workaround:**

As a workaround, perform a refresh inventory after successful import of device profile.

● **Issue 32**

**Description:**

Operating system deployment in SCVMM fails with an error message: `Invalid data manager state found for host` . Reason being, managed node does not boot to installed operating system since the WinPE image is not disconnected.

**Workaround:**

On completion of operating system installation in SCVMM, before the manage node boots to installed operating system, disconnect the attached WinPE image.

To disconnect run the following WinRM command: `winrm i DetachISOImage http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_OSDeploymentService?CreationClassName=DCIM_OSDeploymentService+Name=DCIM:OSDeploymentService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:<username> -p:<password>-r:https://<ip address> -SkipCACheck -SkipCNCheck -encoding:utf-8 -a:basic`

● **Issue 33**

**Description:**

After applying Update Rollup for SC2012 R2 VMM, SC2016 UR9, and SC2019 UR1, if you try to open the already installed OMIMSSC console, SCVMM displays an error message for security reasons, and you cannot access the OMIMSSC console.

**Workaround:**

As a workaround, do the following:

1. Delete the folder at default path: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Restart SCVMM.
3. Remove the console extension, and then import the console extension as mentioned in *Importing OMIMSSC console extension for SCVMM section of Dell EMC OpenManage Integration for Microsoft System Center for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

● **Issue 34**

**Description:**

Console Integration workflow triggered from DRM to connect to OMIMSSC appliance fails with password that includes special characters such as, `<, >, ' , " , &`

**Workaround:**

As a work around, change the appliance password from OMIMSSC black console to ensure the above mentioned special characters are not part of the password.

● **Issue 35**

**Description:**

In the **Maintenance Center** page, even after updating Intel(R) Ethernet Converged Network Adapter X710 component the current version will not be displayed as compliant with baseline version.

**Workaround:**

As a work around, login to iDRAC life cycle controller logs page to confirm if the Intel(R) Ethernet Converged Network Adapter X710 component has been updated with the appropriate baseline version.

● **Issue 36**

**Description:**

Removing SCVMM 2019 UR2, SCVMM2019 UR3, or SCVMM 2016 UR10 console plugins causes SCVMM UI to freeze and close.

**Workaround:**

As a work around, re-open the SCVMM Management console and remove the OMIMSSC console add-in again

# Limitations

- **Issue 1**

**Description:**

Operational Template compliance is not displayed for Active Directory attribute, since the attribute value is present in managed device and not in Operational Template.

- **Issue 2**

**Description:**

In **BIOS Settings**, the snoop mode attribute does not support **ClusterOnDie** option.

- **Issue 3**

**Description:**

While creating a logical switch or a hypervisor profile and selecting host groups in OMIMSSC, the groups are not listed in nested form as present in SCVMM.

- **Issue 4**

**Description:**

If you delete multiple credential profiles, the SCVMM and OMIMSSC consoles may be unresponsive until the profiles are deleted.

- **Issue 5**

**Description:**

Synchronizing OMIMSSC with enrolled Microsoft console takes sometime depending on the number of servers discovered.

- **Issue 6**


**Description:**

In **Server View** page, under **Hosts** tab, the **Select Console Hosts** drop-down menu lists all the host groups present in MECM with an internal group name. If you select the internal group name, all the hosts that are discovered and managed in MECM and OMIMSSC are displayed.

- **Issue 7**

**Description:**

Modified date of a credential profile on creation is set to created date.

 **NOTE:** On consequent edits, modified dates are updated appropriately.

- **Issue 8**

**Description:**

While deploying Operational Template, if **RAID** is selected as **Device Component**, the attributes of hardware and software components do not get updated in the target server.

- **Issue 9**

**Description:**

In **Credential Profile** page, the device credential profile can be edited and reused but cannot be deleted. If you choose to delete, the following error message is displayed: One or more Credential Profile cannot be deleted. One or more Credential Profile are locked and could not be deleted.

- **Issue 10**

**Description:**

If user copies the already logged in Admin Portal page URL in to a new browser window, the browser does not redirect the user to the login page.

- **Issue 11**

**Description:**

Cluster Aware Update fails for "Intel(R) Ethernet Converged Network Adapter X710" firmware intermittently.

- **Issue 12**

**Description:**

In **Maintenance center**, after the CAU job completed successfully, the OMIMSSC inventory displays QLogic BCM 57xx and 57xxx Driver Family component as non-compliant for Windows 2012R2 Hyper-V clusters.

# Instructions for installing

## Installation prerequisites

To install the Dell EMC OMIMSSC 7.3, deploy the Dell EMC OMIMSSC 7.3 available as .vhd or .ova and enroll the Management Server in Appliance Web Console.

For detailed installation, pre-requisites, configuration, upgrade, and uninstallation instructions, see the Dell EMC OpenManage Integration for Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Unified User's Guide at [Dell.com/openmanagemanuals](http://Dell.com/openmanagemanuals).

## Installation process

For more information about installation process, see the **Deploy OMIMSSC** chapter in the OpenManage Integration Microsoft System Center Version 7.3 for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Unified User's Guide.

## Upgrade instructions

Service Pack upgrade from previous versions of OMIMSSC to OMIMSSC version 7.3 is not available.

1. You can upgrade to OMIMSSC version 7.3 from previous versions by using backup and restore appliance capability of OMIMSSC.
2. Ensure OMIMSSC for MECM (SCCM) and SCVMM version 7.2 or 7.2.1 is deployed before restoring to OMIMSSC for MECM and SCVMM version 7.3
3. Ensure that no jobs are running. If running, wait till the jobs are completed.
4. Backup the OMIMSSC appliance data of previous release from the appliance black console.
5. Restore the data into OMIMSSC version 7.3 from Admin Portal.

**i** **NOTE:** For more information about the backup and restore procedure in previous versions, see the **Backup OMIMSSC Appliance** and **Restore OMIMSSC Appliance** sections in *Dell EMC OpenManage Integration for Microsoft System Center for Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager Unified User's Guide*.



## 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 <https://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.