April 2019

Dell EMC OpenManage Integration for Microsoft System Center Version 7.1.1 for System Center Configuration Manager and System Center Virtual Machine Manager Release Notes

OpenManage Integration Version 7.1.1 for Microsoft System Center Release Notes

Topics:

This document describes the features, known issues, and resolutions in OpenManage Integration Version 7.1.1 for Microsoft System Center (OMIMSSC).

Release type and definition

OpenManage Integration Version 7.1.1 for Microsoft System Center

OpenManage Integration for Microsoft System Center (OMIMSSC) provides 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), and of Modular Systems (Dell EMC PowerEdge MX7000) by using OpenManage Enterprise Modular Edition.

OMIMSSC offers operating system deployment, Storage Spaces Direct cluster creation, hardware patching, firmware update, and device maintenance. Integrate OMIMSSC with Microsoft System Center Configuration Manager (SCCM) for managing devices in traditional data center, or integrate OMIMSSC with Microsoft System Center Virtual Machine Manager (SCVMM) for managing devices in virtual and cloud environments.

Version

7.1.1 Rev.A00

Release date

April 2019

Previous versions

OMIMSSC v7.1

Importance

RECOMMENDED: Dell EMC recommends the customer to review specifics about the software update to determine if it applies to your system. The update contains changes that impact certain configurations, or provides new features that may/may not apply to your environment.

NOTE: This patch is only applicable to OpenManage Integration for Microsoft System Center version (OMIMSSC) 7.1.1 for System Center Configuration Manager (SCCM) and System Center Virtual Machine Manager (SCVMM) platforms. Not applicable for Microsoft System Center Operations Manager (SCOM) platform.

Platform(s) Supported

- Rack, tower, and modular Dell EMC PowerEdge servers--11G, 12G, 13G, and 14G.
- Dell EMC PowerEdge MX7000 (OpenManage Enterprise) Modular Systems.

What's new?

- Update sources--Supports Hyper Text Transfer Protocol Secure (HTTPS) type of update source.

  The default update source catalog is available at https://www.downloads.dell.com.

Fixes

- OMIMSSC infrastructure security has been enhanced.
- Static iDRAC IPv4 and IPv6 address values on multiple servers can be applied in a single configuration task through Operational Templates.

Installation prerequisites

- Ensure OMIMSSC for SCCM and SCVMM version 7.1 is deployed before upgrading to OMIMSSC for SCCM and SCVMM version 7.1.1.
- Ensure that no jobs are running. If running, wait till the jobs are completed.
- Back up the OMIMSSC appliance data.

NOTE: For information about the backup procedure, see the Back up OMIMSSC Appliance topic in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

Upgrade instructions

To upgrade from an earlier version of OMIMSSC, back up the data of your current version, and then update by using a service pack.

1. In the OMIMSSC Admin Portal, click **Settings** > **Service Pack Updates**.
2. In the **Repository URL** box, enter the URL of the location of the service pack repository using one of the following update methods:
   a. To update using the offline package, in the **Repository URL** box, provide the URL information of the location where the service pack is saved in the format http://<hostname or IP address>/OMIMSSC_v7.1.1_SP/RPM_Repository.
   b. To update using the linux.dell.com, in the **Repository URL** box, provide the URL information in the format http://linux.dell.com/repo/omimssc-sccm-scvmm/<Service Pack Version> and if required, provide proxy server details and credentials to access the server, and then click **Save**.

NOTE: If necessary, enter the proxy server information and login credentials to access the proxy server.

3. Select **Check for Updates** check box. The current version of OMIMSSC and service pack are displayed.
4. Click **Apply**, and then click **OK**.
5. Navigate to **Settings** > **Logs** > in the upgradelogs directory, to view or download the log files for the service pack upgrade, select the <service pack version number> directory, for example 7.1.1.2035 directory to view or download the log files for the service pack upgrade.
6. Log in to the **Admin Portal**, and then delete the browser cache history.
7. After the service pack update is complete, reboot the appliance manually.

NOTE: If you have already enrolled to OMIMSSC version 7.1 for System Center Configuration Manager or System Center Virtual Machine Manager console, do not upgrade the OMIMSSC version 7.1.1 console extension.

For more information about creating service pack update repositories, see the **About service packs updates** topic in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide.*

Known issues and resolutions

- **Issue 1**

  Description:

  If the test connection or enrollment fails, then you get an error message.

  Workaround:

  As a workaround, perform the following steps:

  - Ping from OMIMSSC Appliance to enrolled SCCM or SCVMM server FQDN by logging in to OMIMSSC Appliance VM as a read-only user. If there is a response, then wait for some time and then continue with the enrollment.

    To launch the OMIMSSC Appliance VM as a read-only user, enter user name as `readonly` with the same password used to log into the OMIMSSC Appliance VM.
  - Ensure that the SCCM or SCVMM server is running.
  - The Microsoft account used to enroll the console should be a delegated admin or an administrator in System Center, and a local administrator for the System Center server.
  - Specific for SCVMM users:
    - Ensure that the SCVMM server is not registered with any other OMIMSSC Appliance. If you want to register the same SCVMM server with the OMIMSSC Appliance, then delete the **OMIMSSC Registration Profile** application profile from the SCVMM server.
    - If you have applied SCVMM roll up update, then check the Indigo TCP port number of SCVMM console in registry `(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings)`. Use the same port number that was used to register SCVMM console. By default it is 8100.
- **Issue 2**

  Description:

  After enrolling and installing OMIMSSC console extension in SCVMM environment, when you try to launch OMIMSSC, the following error is displayed: `Connection to server failed`.

  Workaround:

  As a workaround, perform the following steps:

  1. Add the OMIMSSC Appliance IP and FQDN into local intranet in SCVMM console, when you are launching OMIMSSC.
  2. Add the OMIMSSC Appliance IP and FQDN in **Forward Lookup Zones** and **Reverse Lookup Zones** in DNS.
  3. For further details, check if there are any error messages in `C:\ProgramData\VMMLogs\AdminConsole` file.
- **Issue 3**

  Description:

  After applying Update Rollup for SC2012 R2 VMM, 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 System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

- **Issue 4**

  Description:

  After creating and starting the OMIMSSC Appliance VM, the OMIMSSC Appliance IP address is not assigned or displayed.

  Workaround:

  As a workaround, check if the virtual switch is mapped to a physical switch, if the switch is configured correctly, and then connect to OMIMSSC Appliance.

- **Issue 5**

  Description:

  SC2016 VMM RTM build 4.0.1662.0 Administrator console may crash when importing OMIMSSC console extension.

  Workaround:

  As a workaround, upgrade SCVMM using the 4094925 KB article available at `support.microsoft.com/kb/4094925`, and then import the OMIMSSC console extension.

- **Issue 6**

  Description:

  After logging in to OMIMSSC console extensions with different credentials used to login to Microsoft console, the login activity fails with following error message: `Username or Password is incorrect`

  Workaround:

  As a workaround, login and launch Microsoft console with the credentials used to login to OMIMSSC console extension. This is a one-time activity.

- **Issue 7**

  Description:

  After upgrading to SC2012 VMM SP1, when importing OMIMSSC console extension to SC2012 VMM UR5 or later, the SCVMM console may crash.

  Workaround:

  For information about this issue and resolving the issue, see issue 5 in the knowledge base URL: `support.microsoft.com/kb/2785682`.

- **Issue 8**

  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 9**

  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`

- **Issue 10**

  Description:

When the OMIMSSC admin portal is launched on a Windows 2016 default IE browser, the admin portal is not displayed with the Dell EMC logo.

Workaround:

As a workaround, do one of the following:

- Upgrade IE browser to the latest version.
- Delete the browsing history, and then add the OMIMSSC admin portal URL to browser's favorite list.

- **Issue 11**

  Description:

  If you provide incorrect credential details during discovery, then based on the iDRAC version, the following resolutions are available:

  Workaround:

  - While discovering a 12th generation PowerEdge server with iDRAC version 2.10.10.10 and later, if incorrect details are provided in the credential profile, the server discovery fails, with the following behavior:
    - For first attempt, server IP address is not blocked.
    - For second attempt, server IP address is blocked for 30 seconds.
    - For third and subsequent attempts, server IP address is blocked for 60 seconds.

    You can reattempt server discovery with correct credential profile details after the IP address is unblocked.
  - While discovering an 11th or 12th generation PowerEdge server with iDRAC versions prior to 2.10.10.10, if server discovery attempts fail due to incorrect credential profile details, then rediscover the server with the correct credential profile details.
  - For iDRAC versions prior to 2.10.10.10, blocking of IP addresses is configurable. For more information, see iDRAC documentation at **Dell.com/idracmanuals**. Based on your requirement, you can also disable blocking of IP addresses. And you can also check if the `iDRAC.IPBlocking.BlockEnable` feature is enabled in iDRAC.
  - If the default iDRAC credential profile is changed after a server is discovered and added in the Appliance, then no activity can be performed on the server. To work with the server, rediscover the server with the new credential profile.

- **Issue 12**

  Description:

  When modular servers that were previously in another chassis are added to a VRTX chassis and discovered in OMIMSSC, the modular servers carry previous chassis service tag information. Hence, a VRTX chassis group with old chassis information is created in the Appliance instead of the latest chassis information.

  Workaround:

  As a workaround, do the following:

  1. Enable CSIOR, and reset iDRAC on the newly added modular server.
  2. Manually delete all the servers in the VRTX chassis group, and then rediscover the servers.

- **Issue 13**

  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 14**

  Description:

  The modular servers are not able to access the CIFS share using the host name for performing any job in OMIMSSC.

  Workaround:

  As a workaround, specify the IP address of the server having the CIFS share instead of the host name.

- **Issue 15**

  Description:

  The **Jobs and Logs Center** page is not displayed in OMIMSSC console extensions.

  Workaround:

  As a workaround, re-enroll the console and then launch the **Jobs and Logs** page.

- **Issue 16**

Description:

When the Domain Name System (DNS) network configuration of the Appliance is changed, creation of HTTP or FTP type of update source fails.

Workaround:

As a workaround, restart the Appliance, and then create the update source of type HTTP or FTP.

- **Issue 17**

  Description:

  After setting up and configuring, upgrading, or migrating OMIMSSC when you try to access the FTP site using the default update source **Dell Online Catalog** it may fail if proxy credentials are required.

  Workaround:

  As a workaround, to access the FTP site using **Dell Online Catalog** as an update source, edit the update source to add the proxy credentials.

- **Issue 18**

  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 **dlciappliance_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_TIMEOUTwhere EnableSMB1Protocol = false.`*

  Workaround:

  As a workaround, see to the following KB article: *support.microsoft.com/en-us/help/4034314*

- **Issue 19**

  Description:

  Creation of a repository may fail during a firmware update because of incorrect credentials provided while creating an update source, or update source is not reachable by OMIMSSC Appliance.

  Workaround:

  As a workaround, ensure that the update source is reachable from where the OMIMSSC Appliance is hosted, and provide the correct credentials while creating an update source.

- **Issue 20**

  Description:

  After upgrading to the latest version of OMIMSSC, if the connection to `ftp.dell.com` or `downloads.dell.com` fails, the default Dell online FTP, or Dell HTTP update source cannot download the catalog file. Hence, the comparison report is not available.

  Workaround:

  As a workaround, to view a comparison report for the default update source, edit the default Dell online FTP, or Dell HTTP update source, create proxy credentials, and then select the update source from **Select Update Source** drop-down menu. For more information about editing an update source, see *Modifying update source* section from *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

- **Issue 21**

  Description:

  After a job is submitted in OMIMSSC to update firmware of clusters, the clusters are not updated due to certain reasons displaying the following error messages in **Activity Logs**.

  ```
  Cluster Aware Update failed for cluster group <cluster group name>.
  ```

  ```
  Failed to perform Cluster Aware Update for cluster group <cluster group name>.
  ```

  Workaround:

  Reasons of failure of firmware update on clusters with the following workaround:

  - If the required DUPs and catalog files are not present in the selected local update source.

As a workaround is to ensure that all the required DUPs and catalog files are available in the repository, and then update the firmware of clusters.

- Cluster group becomes unresponsive or firmware update job was canceled in CAU due to an in-progress job, then the DUPs are downloaded and placed in each server cluster node belonging to the cluster group.

  As a workaround, delete all the files in Dell folder, and then update the firmware of clusters.

- If Lifecycle Controller (LC) is busy with other operations, then firmware update task on a cluster node fails. To check if the update failed because of LC being busy, check for the following error message in each node of the cluster at the following path: `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then reboot the system.
  ```

  As a workaround, shut down the server, remove the power cables, and then restart the server. After reboot, update the firmware on clusters.

- **Issue 22**

  Description:

  Firmware update job submitted from OMIMSSC to iDRAC fails, and the OMIMSSC main log displays the following error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

  Workaround:

  As a workaround, manually delete the completed jobs in iDRAC, and retry the firmware update job. For more information about deleting jobs in iDRAC, see iDRAC documentation at **dell.com/support/home**.

- **Issue 23**

  Description:

  Firmware update job may fail if you are using DRM update source with insufficient access to the share folders. If the Windows credential profile provided while creating DRM update source is not a part of domain administrator group or the local administrator group, the following error message is displayed: `Local cache creation failure`.

  Workaround:

  As a workaround, perform the following:

  1. After creating the repository from DRM, right-click on the folder, click **Security** tab, and then click **Advanced**.
  2. Click **Enable inheritance** and select the **Replace all child object permission entries with inheritable permission entries from this object** option, and then share the folder with **Everyone** with read-write permission.

- **Issue 24**

  Description:

  The same components on identical servers get updated during a firmware update irrespective of the selection of components made on these individual servers. This behavior is observed for 12th and 13th generation of PowerEdge servers with Enterprise license of iDRAC.

  Workaround:

  As a workaround, do one of the following:

  - First apply updates for common components on identical servers, and then apply updates for specific components on individual servers.
  - Perform staged updates with planned outage time to accommodate the firmware update.

- **Issue 25**

  Description:

  After successfully updating the firmware versions on 11th generation PowerEdge servers, the latest inventory information is not displayed.

  In OMIMSSC, refreshing the inventory is an activity performed immediately after a firmware update job is complete. Firmware update is completed even before the PowerEdge server's CSIOR activity is complete, due to which the earlier firmware inventory information is displayed.

  Workaround:

  As a workaround, check if the CSIOR activity is complete in the PowerEdge server, and then refresh the firmware inventory in OMIMSSC. Also, ensure to restart the server after applying agent-free staged update. For more information about refreshing the inventory, see *Viewing and refreshing firmware inventory* section in *OpenManage Integration for Microsoft System Center Configuration Manager and Virtual Machine Manager User's Guide*.

For more information about CSIOR, see the Troubleshooting section in the latest version of *Dell Lifecycle Controller GUI User's Guide* available at **dell.com/support/home**.

- **Issue 26**

  Description:

  After scheduling any job on a server belonging to a custom update group, if the server is deleted from Microsoft console and you synchronize registered Microsoft console with OMIMSSC, the server is removed from the custom update group and the server is moved to a predefined update group. You cannot delete such custom update group, because it is associated with a scheduled job.

  Workaround:

  As a workaround, delete the scheduled job from **Jobs and Logs** page, and then delete the custom update group.

- **Issue 27**

  Description:

  When you try to update the WinPE image, update job may fail with the following error message: `Remote connection to console failed.`

  Workaround:

  As a workaround, run the **DISM** command to clean up all previously mounted images in Microsoft console, and then retry to update the WinPE image.

- **Issue 28**

  Description:

  Firmware updates applied on 11th generation of PowerEdge servers may fail due to incompatible versions of iDRAC and LC with the following error: `WSMan command failed to execute on server with iDRAC IP <IP address>`.

  Workaround:

  As a workaround, upgrade the iDRAC and LC to the latest versions, and then apply the firmware updates. The table lists out the latest versions of LC and iDRAC.

- **Issue 29**

  Description:

  After proving the details of a local update source, the test connection may fail as the required files may be not accessible.

  Workaround:

  As a workaround, ensure that `catalog.gz` file is present in the following folder structure.

  - For local HTTP update source: `http:\\IP address\catalog\catalog.gz`
  - For local FTP update source: `ftp:\\IP address\catalog\catalog.gz`
  - For local DRM update source: `\\IP address\\catalog\<catalogfile>.gz`

- **Issue 30**

  Description:

  After deploying the Operational Template on the selected servers, the attributes or attribute values are not appropriate for the selected .CSV file, or the iDRAC IP or iDRAC credentials are changed due to the configurations in the template. The job in iDRAC is successful, however the status of this job in OMIMSSC is shown as unsuccessful or failure due to invalid .CSV file, or the job cannot be tracked due to the iDRAC changes on the target server.

  Workaround:

  As a workaround, ensure the selected .CSV file has all the proper attributes and attribute values, and the iDRAC IP or credentials do not change due to the configurations in the template.

- **Issue 31**

  Description:

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

  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 32**

  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 SCCM.

Workaround:

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

- **Issue 33**

  Description:

  Hypervisor deployment fails displaying the following error message in activity log: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

  Workaround:

  This error may occur due to one of these reasons:

  - Dell Lifecycle Controller's state is bad.

    As resolution, log in to iDRAC user interface and reset Lifecycle Controller.

    After resetting Lifecycle Controller, if you still face the problem try the following alternative:
  - The antivirus or firewall may restrict the successful run of the `WINRM` command.

    See the following KB article for workaround: `support.microsoft.com/kb/961804`

- **Issue 34**

  Description:

  Hypervisor deployment fails displaying the following error message in activity log:

  - **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
  - **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
  - **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

  These errors may occur due to exception output by the VMM command-let `GET-SCJOB status` and driver files are retained in the library share. Before you retry or do another hypervisor deployment you must remove these files from the library share.

  Workaround:

  To remove files from library share:

  1. From SCVMM console, select **Library** > **Library Servers** and then select the IG server that was added as the library server.
  2. In the library server, select and delete the library share.
  3. After the library share is deleted, connect to the IG share using `\\<Integration Gateway server>\LCDriver\`.
  4. Delete the folder that contains the driver files.

  After this, you can deploy the hypervisors.

- **Issue 35**

  Description:

  While adding servers to Active Directory, SCVMM error 21119 is displayed. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

  Workaround:

  As a workaround, do the following:

  1. Wait for some time to see if the server is added to the Active Directory.
  2. If the server is not added to the Active Directory, then manually add the servers to the Active Directory.
  3. Add the server in to SCVMM.
  4. After the server is added in to SCVMM, rediscover the server in OMIMSSC.

     The server will now be listed under the **Host** tab.

- **Issue 36**

  Description:

  Hypervisor deployment fails on the 11th generation PowerEdge blade servers when using the Active Directory user credentials. The 11th generation PowerEdge blade servers use the Intelligent Platform Management Interface (IPMI) protocol for communication. However, the IPMI standard is not supported for using credentials from the Active Directory setup.

Workaround:

As a workaround to deploy operating systems on these servers, use supported credential profiles.

- **Issue 37**

  Description:

  When deploying OS and injecting LC drivers using SC2012 VMM, the OS is deployed successfully but, the LC drivers are not injected.

  Workaround:

  To resolve the issue, apply the latest rollup for SCVMM.

- **Issue 38**

  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`.

- **Issue 39**

  Description:

  After submitting the import server profile job in OMIMSSC, the job gets timed out after two hours.

  Workaround:

  As a workaround, perform the following steps:

  1. Start the server, press F2, and then enter **BIOS Settings**.
  2. Click **System Setup**, and select **Miscellaneous Settings**.
  3. Disable **F1/F2 Prompt on Error**.

  After performing the following steps, export the server profile again, and use the same server profile to import on that server.

- **Issue 40**

  Description:

  When you try to download the LC log files to .CSV format, the download operation fails.

  Workaround:

  As a workaround, add the OMIMSSC Appliance FQDN in the browser under local intranet site. For information about adding the OMIMSSC Appliance in local intranet, see *Viewing LC logs* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

- **Issue 41**

  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`.

- **Issue 42**

  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 43**

  Description:

All the features of OMIMSSC does not perform as expected on the managed systems due to a Transport Layer Security (TLS) version.

Workaround:

If you are using iDRAC firmware version 2.40.40.40 or later, Transport Layer Security (TLS) versions 1.1 or later is enabled by default. Before installing the console extension, install the update to enable TLS 1.1 and later as mentioned in the following KB article: `Support.microsoft.com/en-us/kb/3140245`. It is recommended that you enable support for TLS 1.1 or later on your SCVMM server and SCVMM console to ensure that OMIMSSC operates as expected. And for more information about iDRAC, see Dell.com/idracmanuals.

- **Issue 44**

  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 45**

  Description:

  If you are accessing local FTP using proxy credentials created by CCProxy server, then the local FTP site is not accessible.

- **Issue 46**

  Description:

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

- **Issue 47**

  Description:

  The action in comparison report for operating system collector component is displayed as downgrade even if it an upgrade action.

- **Issue 48**

  Description:

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

- **Issue 49**

  Description:

  After discovering the servers in OMIMSSC for SCCM 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 SCCM and the server is added to this group.

- **Issue 50**

  Description:

  When you create a Storage Spaces Direct 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 Storage Spaces Direct cluster. For more information on clearing the storage pool, see *Troubleshoot Storage Spaces Direct health and operational states* section from Microsoft documentation.

- **Issue 51**

  Description:

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

  Workaround:

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

- **Issue 52**

  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 53**

  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 54**

  Description:

  When you are creating an Operational Template, if you select and clear a dependent attribute's check box having pool value, you are not able to save the Operational Template with the following error message:

  ```
  Select atleast one attribte, under the selected components, before creating the
  Operational Template.
  ```

  Workaround:

  As a workaround, perform any one of the following:

  - Select any other dependent attribute having pool value or the same dependent attribute and save the Operational Template.
  - Create a new Operational Template.

- **Issue 55**

  Description:

  If a managed server is not discovered in OMIMSSC, and you change the frequency of polling and notification option, the bell color changes to yellow after sometime, even if there are no changes in the catalog.

  Workaround:

  As a workaround, discover managed servers and then change the frequency of polling and notification option.

- **Issue 56**

  Description: If you delete a large number of credential profiles, the SCVMM and OMIMSSC consoles may be unresponsive till the profiles are deleted.

- **Issue 57**

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

- **Issue 58**

  Description: The notification icon in the **Maintenance Center**, changes its color to yellow irrespective of polling frequency being set to once a week/once a month.

  Workaround:

  As a workaround, manually refresh the **Maintenance Center** at every 10 minutes interval to view the latest catalog.

- **Issue 59**

  Description: Filter on **Maintenance Center** is not available for MX7000 Modular Systems.

- **Issue 60**

  Description: In **Modular Systems** view, the **Firmware Version** of PowerEdge MX7000 displays up to two decimal values only.

  Workaround:

  As a work around, in **Maintenance Center** page, expand the **Chassis Update Group** tab and select **Management Module** to view the firmware version.

- **Issue 61**

  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 used while updating the firmware. Go to **Maintenance Center** to view the correct number of updates.

- **Issue 62**

  Description: In **Maintenance Center** page, the **Firmware compliance** report for 14th generations of servers with iDRAC firmware of 3.30.30.30 and above, for Perc H330 adapter/NIC/BOSS, the update shows as **NOT AVAILABLE** for both online and DRM catalogs.

Download instructions

You can download an evaluation version of OMIMSSC from www.dell.com. However, to download a production version, contact your local Dell EMC Sales representative, purchase the appliance license, and then import to the required file location.

For more information about importing the OMIMSSC appliance license file, see the OpenManage Integration for Microsoft System Center User's Guide.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell 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 for sales, technical support, or customer service issues:

1. Go to **Dell.com/support.**
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

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.