

OpenManage Integration for Microsoft System Center Version 7.1.1 for System Center Configuration Manager and System Center Virtual Machine Manager

User's Guide

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 Introduction to OMIMSSC.....	7
What's new ?.....	7
2 Use cases of OMIMSSC	8
Use cases for deployment scenarios.....	8
Deploying Windows OS using OMIMSSC console extension for SCCM.....	10
Deploying hypervisor using OMIMSSC console extension for SCVMM.....	10
Redeploying Windows OS using OMIMSSC.....	11
Deploying non-windows OS using OMIMSSC console extensions.....	11
Creating Storage Spaces Direct clusters by using predefined Operational Templates.....	12
Use cases for maintaining devices.....	13
Updating the firmware of servers and MX7000 devices.....	14
Configuring replaced components.....	15
Exporting and importing server profiles.....	15
3 Views in OMIMSSC.....	16
Launching Server View.....	16
Launching Modular Systems view.....	17
Launching OpenManage Enterprise Modular console.....	18
Input/Output Modules.....	18
Launching Cluster View.....	18
Launching iDRAC console.....	19
Launching Maintenance Center.....	19
Launching Jobs and Logs Center.....	20
4 Managing profiles.....	21
About credential profile.....	21
Predefined credential profile.....	21
Creating credential profile.....	21
Modifying credential profile.....	22
Deleting credential profile.....	22
About hypervisor profile (for SCVMM users).....	23
Creating hypervisor profile.....	23
Modifying hypervisor profile.....	24
Deleting hypervisor profile.....	24
5 Discovering devices and synchronizing servers with MSSC console.....	25
About reference server configuration.....	25
About reference Modular System configuration.....	25
Discovering devices in OMIMSSC.....	25
Device discovery in OMIMSSC console extension for SCCM.....	26
Device discovery in OMIMSSC console extension for SCVMM.....	26

System requirements for managed systems.....	26
Discovering servers using auto discovery.....	26
Discovering servers using manual discovery.....	27
Discovering MX7000 by using manual discovery.....	28
Synchronization of OMIMSSC console extension with enrolled SCCM.....	28
Synchronization of OMIMSSC console extension with enrolled SCVMM.....	29
Synchronizing with enrolled Microsoft console.....	29
Resolving synchronization errors.....	29
Viewing System Lockdown Mode.....	29
Deleting servers from OMIMSSC.....	30
Deleting Modular Systems from OMIMSSC.....	30
6 Preparing for operating system deployment.....	31
About WinPE image	31
Providing WIM file for SCCM.....	31
Providing WIM file for SCVMM.....	31
Extracting DTK drivers.....	31
Updating WinPE image.....	32
Preparing for operating system deployment on SCCM console.....	32
Task sequence-SCCM.....	32
Setting a default share location for the Lifecycle Controller boot media.....	34
Creating a task sequence media bootable ISO.....	34
Preparing for non-Windows operating system deployment.....	35
7 Managing Operational Templates.....	36
Predefined Operational Templates.....	37
Creating Operational Template from reference servers.....	37
Windows OS component for OMIMSSC console extension for SCCM.....	39
Windows component for OMIMSSC console extension for SCVMM.....	39
Non-Windows component for OMIMSSC console extensions.....	39
Creating Operational Template from reference Modular Systems.....	40
Viewing Operational Template.....	41
Modifying Operational Template.....	41
Deleting Operational Template.....	42
Assigning Operational Template and running Operational Template compliance for servers.....	42
Deploying Operational Template on servers	42
Assigning Operational Template for Modular Systems.....	43
Deploying Operational Template for Modular System.....	44
Unassigning Operational Template.....	44
8 Firmware update in OMIMSSC.....	45
About update groups.....	45
Predefined update groups.....	45
Custom update groups.....	46
Viewing update groups.....	46
Creating custom update groups.....	46

Modifying custom update groups.....	46
Deleting custom update groups.....	47
About update sources.....	47
Predefined and default update source.....	48
Predefined and default update sources for Storage Spaces Direct clusters.....	48
Predefined and default update sources for Modular Systems.....	48
Validating data using test connection.....	48
Setting up local FTP.....	48
Setting up local HTTP.....	49
Setting up local HTTPS.....	49
Viewing update source.....	49
Creating update source.....	49
Modifying update source.....	50
Deleting update source.....	50
Integration with Dell EMC Repository Manager(DRM).....	51
Integrating DRM with OMIMSSC	51
Setting polling frequency.....	51
Viewing and refreshing device inventory.....	52
Applying filters.....	53
Removing filters.....	53
Upgrading and downgrading firmware versions using run update method.....	53
Updates using CAU.....	54
9 Creating clusters using Operational Template.....	56
Creating logical switch for Storage Spaces Direct clusters.....	56
Creating Storage Spaces Direct clusters.....	56
10 Managing devices in OMIMSSC.....	58
Server recovery.....	58
Protection vault.....	58
Exporting server profiles.....	59
Importing server profile.....	60
Applying firmware and configuration settings on replaced component.....	60
Collecting LC logs for servers.....	61
Viewing LC logs.....	62
File description.....	62
Exporting inventory.....	63
Cancelling scheduled jobs.....	63
11 Configuration and deployment.....	64
Use cases.....	64
Creating Operational Templates.....	65
Installer folders.....	66
Assign Operational Templates.....	66
Deploy Operational Templates.....	67
Windows OS component for the OMIMSSC console extension for SCCM.....	68

Windows component for the OMIMSSC console extension for SCVMM.....	68
Non-Windows component for the OMIMSSC console extension for SCCM/SCVMM.....	68
Discovery in enrolled MSSC.....	69
Importing server profile.....	69
Export server profile.....	69
Viewing LC logs.....	69
Collect LC logs.....	69
Part replacement.....	69
Polling and notification.....	70
Launch iDRAC.....	70
Launch Input Output Module.....	70
Resolving synchronization errors.....	70
Synchronizing OMIMSSC with enrolled Microsoft console.....	70
Assign and deploy.....	71
Run update.....	71
12 Appendix.....	72
13 Accessing documents from the Dell EMC support site.....	76
Contacting Dell.....	76

Introduction to OMIMSSC

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.

For information about SCCM and SCVMM, see the Microsoft documentation.

What's new ?

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

Use cases of OMIMSSC

This chapter covers high-level details for discovering, deploying operating system, creating clusters, and maintaining Dell EMC devices using OMIMSSC.

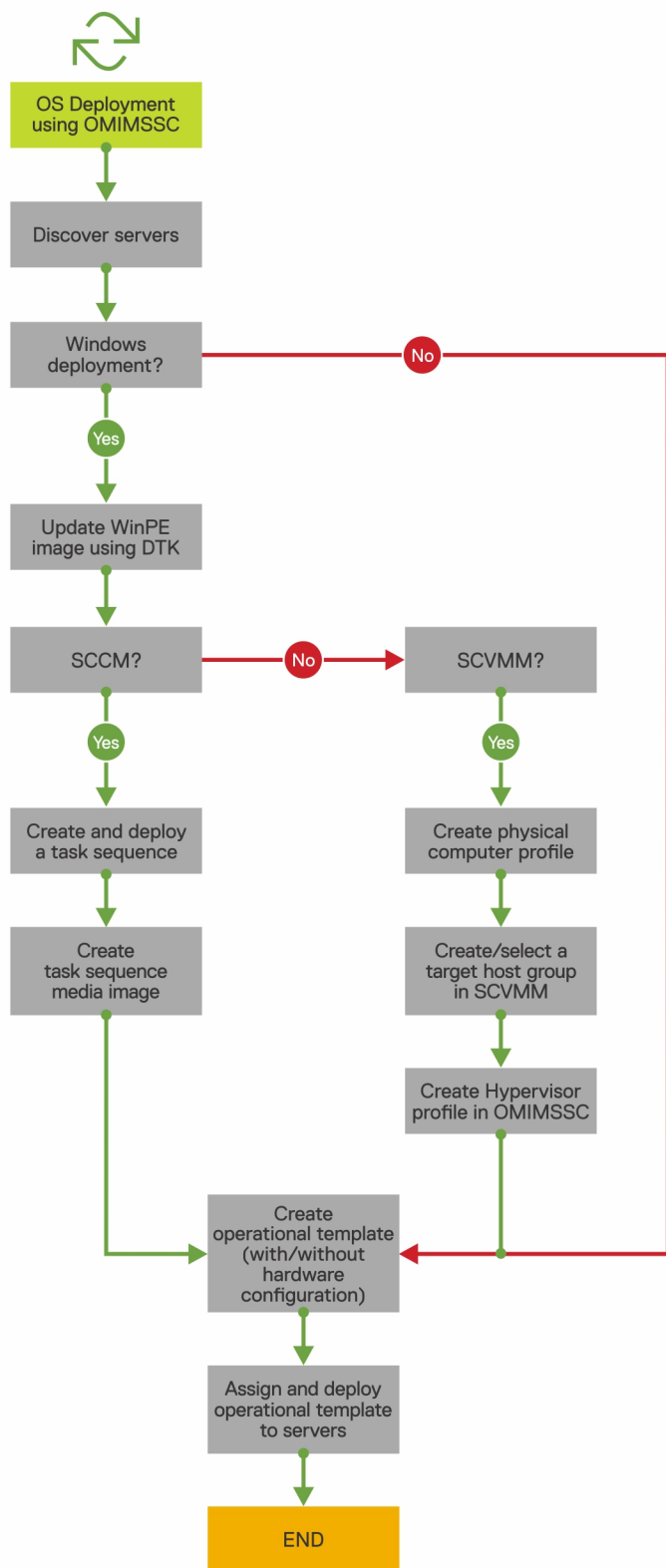
Use cases for deployment scenarios

Use OMIMSSC to deploy Windows and non-Windows operating system in SCCM or SCVMM environments using Operational Templates.

NOTE: Ensure that you upgrade the device firmware versions to the latest versions available at <ftp.dell.com> or <downloads.dell.com> before deploying the operating system.

NOTE: Non-windows operating system deployment is not supported on 11th generation of servers.

Here is a pictorial representation of the operating system deployment use cases in OMIMSSC.



Deploying Windows OS using OMIMSSC console extension for SCCM

About this task

To deploy Windows OS through SCCM console using OMIMSSC, perform the following steps:

NOTE: Before deploying OS on a host server, ensure that in SCCM, the Client status of the server is No.

Steps

- 1 Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot WIM image. For more information, see the [WinPE update](#).
- 2 Import this .WIN image into the SCCM console, and create a boot image in SCCM. For more information, see the *Microsoft documentation*.
- 3 Create a task sequence in SCCM. For more information, see [Creating task sequence](#).
- 4 Create a task sequence media image in SCCM. For more information, see the *Microsoft documentation*.

NOTE: To enable unattended OS deployment when creating task sequence media, in **Select the type of media**, select **Allow unattended operating system deployment check-box**.

- 5 Discover the reference server by using the **Discovery** page. For more information, see the [Discovering servers using manual discovery](#).
- 6 Create an Operational Template, by capturing all the details of the discovered server. For more information, see [Creating Operational Template from reference servers](#).
- 7 Assign an Operational Template on managed device, and check for the template compliance. For more information, see [Assigning Operational Template and running Operational Template compliance](#).
- 8 Deploy an Operational Template to make the device template compliant. For more information, see [Deploying Operational Template](#).
- 9 View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see [Launching Jobs and Logs Center](#).

Deploying hypervisor using OMIMSSC console extension for SCVMM

About this task

The different scenarios for hypervisor deployment are as follows:

Table 1. Hypervisor deployment scenarios

Condition	Action
If you require the latest factory drivers.	While creating a hypervisor profile, enable Lifecycle Controller (LC) driver injection.
If you want to retain the existing hardware configuration.	While creating the Operational Template, clear the check box for all the components that do not require any changes.

To deploy hypervisor through SCVMM console using OMIMSSC, perform the following steps:

Steps

- 1 Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot ISO image. For more information, see the [WinPE update](#).
- 2 Create a physical computer profile, and a host group in SCVMM. For more information, see the SCVMM documentation.
- 3 Create a hypervisor profile in the OMIMSSC console extension for SCVMM. For more information, see [Creating a hypervisor profile](#).
- 4 Discover the reference server by using the **Discovery** page. For more information, see the [Discovering servers using manual discovery](#).

- 5 Create an Operational Template, by capturing all the details of the discovered server. For more information, see [Creating Operational Template from reference servers](#).
- 6 Assign an Operational Template on managed device, and check for the template compliance. For more information, see [Assigning Operational Template and running Operational Template compliance](#).
- 7 Deploy an Operational Template to make the device template compliant. For more information, see [Deploying Operational Template](#).
- 8 View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see [Launching Jobs and Logs Center](#).

Redeploying Windows OS using OMIMSSC

About this task

To redeploy Windows OS on a server by using OMIMSSC console extension for SCCM or OMIMSSC console extension on SCVMM, perform the following steps:

Steps

- 1 Delete the server from the Microsoft console. For more information, see Microsoft documentation.
- 2 Rediscover the server or synchronize OMIMSSC with the registered Microsoft console. The server is added as an unassigned server in OMIMSSC. For more information about discovery, see [Discovering servers using manual discovery](#). For more information about synchronization, see [Synchronizing with enrolled Microsoft console](#).
- 3 Create an Operational Template, by capturing all the details of the discovered server. For more information, see [Creating Operational Template from reference servers](#).
- 4 Assign an Operational Template on managed device, and check for the template compliance. For more information, see [Assigning Operational Template and running Operational Template compliance](#).
- 5 Deploy an Operational Template to make the device template compliant. For more information, see [Deploying Operational Template](#).
- 6 View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see [Launching Jobs and Logs Center](#).

Deploying non-windows OS using OMIMSSC console extensions

About this task

To deploy non-windows OS using OMIMSSC, perform the following steps:

NOTE: Steps to deploy non-windows OS through OMIMSSC is common in both the Microsoft consoles.

Steps

- 1 Discover the reference server by using the **Discovery** page. For more information, see the [Discovering servers using manual discovery](#).
- 2 Create an Operational Template, by capturing all the details of the discovered server. For more information, see [Creating Operational Template from reference servers](#).
- 3 Assign an Operational Template on managed device, and check for the template compliance. For more information, see [Assigning Operational Template and running Operational Template compliance](#).
- 4 Deploy an Operational Template to make the device template compliant. For more information, see [Deploying Operational Template](#).

NOTE:

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

Creating Storage Spaces Direct clusters by using predefined Operational Templates

To create clusters by using OMIMSSC, perform the following steps:

- 1 Discover the reference server by using the **Discovery** page. For more information, see the [Discovering servers using manual discovery](#).
- 2 Edit the predefined Operational Template. For more information, see [Modifying Operational Template](#).
- 3 Create a logical switch. For more information, see [Creating logical switch](#).
- 4 Create Storage Spaces Direct cluster. For more information, see [Creating Storage Spaces Direct clusters](#).

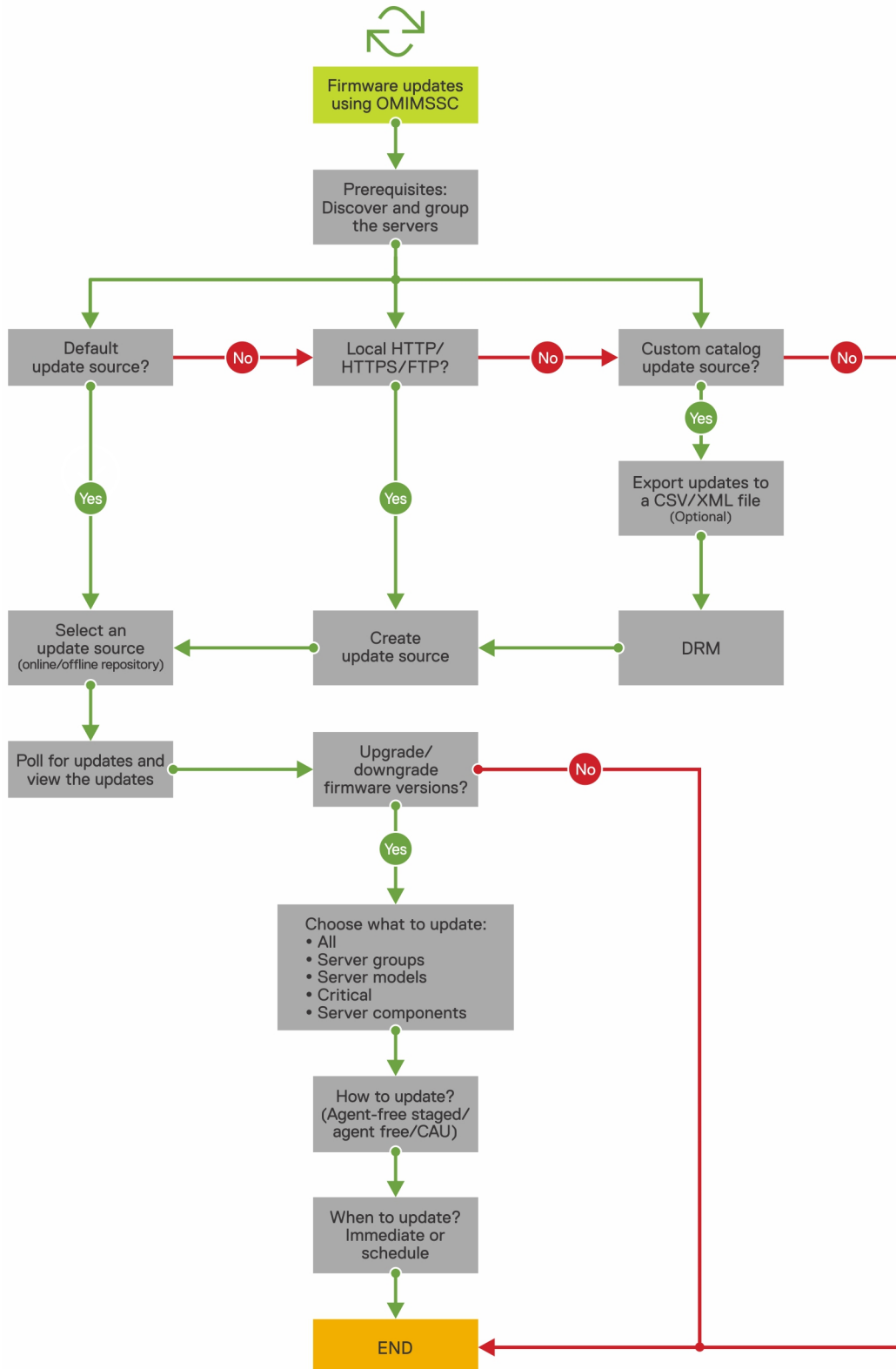
Use cases for maintaining devices

Maintain the discovered devices in OMIMSSC.

Updating the firmware of servers and MX7000 devices

About this task

Here is a pictorial representation of the firmware update workflow.



You can update the selected devices by using the following update sources:

- Online FTP or local FTP source
- Online HTTP or local HTTP source
- Online HTTPS or local HTTPS source
- Local Dell Repository Manager (DRM) source

Steps

- 1 Create or select a default update source. For more information about update source, see [Update source](#).

NOTE: Ensure that you update the update source with the latest catalog by using the polling and notification feature. For more information about polling and notification, see [Polling and notification](#).

If you are updating Storage Spaces Direct clusters, select a predefined update source specific for Storage Spaces Direct clusters. These update sources are displayed only in the **Maintenance Center** page.

If you are updating MX7000 devices, select a predefined update source specific for Modular Systems. These update sources are displayed only in **Maintenance Center** page.

- 2 Create or select the default update groups. For more information about update groups, see [Update groups](#).
- 3 Discover or synchronize the devices with a registered Microsoft console, and ensure that the device inventory is up-to-date. For more information about discovery and synchronization, see [Device discovery and synchronization](#). For more information about server inventory, see [Launching server view](#).
- 4 Update the device by using one of the following options:
 - Select the required devices, and click **Run Update**. For more information, see [Upgrading or downgrading firmware versions using run update method](#).

NOTE: To downgrade the firmware of device components, select the Allow Downgrade check-box. If this option is not selected, there is no action on the component that requires a firmware downgrade.

- Select the firmware update component in Operational Template and deploy this template. For more information about Operational Template, see [Operational Template](#).

Configuring replaced components

To match the firmware version, or the configuration settings of the replaced component to that of the old component, see [Applying firmware and configuration settings](#).

Exporting and importing server profiles

About this task

Export the server profile at a particular instance, and then import the profile to reinstate the server:

Steps

- 1 Create a protection vault. For more information about creating protection vault, see [Creating protection vault](#).
- 2 Export a server profile. For more information about exporting server profile, see [Exporting server profile](#).
- 3 Import server profile to the same server from which it was exported. For more information about importing server profile, see [Importing server profile](#).

NOTE: You can import the server profile including the RAID configuration only if the RAID configuration is exported to the profile.

Views in OMIMSSC

View all the devices discovered in OMIMSSC in **Configuration and Deployment** page along with their hardware and firmware inventory information. Also, view all the jobs with status in **Jobs and Logs Center** page.

Topics:

- [Launching Server View](#)
- [Launching Modular Systems view](#)
- [Launching Cluster View](#)
- [Launching iDRAC console](#)
- [Launching Maintenance Center](#)
- [Launching Jobs and Logs Center](#)

Launching Server View

The **Server View** page lists all unassigned and host servers that are discovered in OMIMSSC under **Unassigned Servers** and **Hosts** tabs.

About this task

In **Unassigned Servers** tab, view the iDRAC IP address, service tag, model, generation, processor speed, memory of the server, template compliance status for assigned Operational Template, Modular System's service tag if it is a modular server, and hardware compatibility information. On hovering over the **Hardware Compatibility** column, you can view the versions of BIOS, iDRAC, LC, and driver packs of the device. For more information about hardware compatibility, see [About firmware update](#).

In **Hosts** tab, view host name, iDRAC IP address, service tag, model, generation, processor speed, memory of the server, Modular System's service tag if it is a modular server, cluster's Fully Qualified Domain Name (FQDN) if the server is part of a cluster, template compliance status for assigned Operational Template, and hardware compatibility information. On hovering over the **Hardware Compatibility** column, you can view the versions of BIOS, iDRAC, LC, and driver packs of the device. For more information about hardware compatibility, see [About firmware update](#).

You can perform the following tasks on **Server View** page:

- [Discover servers](#)
- View updated information, by refreshing the page.
- [Delete servers from OMIMSSC](#).
- [Synchronize with enrolled Microsoft console](#).
- [Resolving synchronization errors](#).
- [Assign Operational Template and run Operational Template compliance](#).
- [Deploy Operational Template](#)
- Correlate servers to cluster group and the Modular System to which the server belongs to.
- [Launch iDRAC console](#)

To view servers:

Steps

- 1 In OMIMSSC console extension, click **Configuration and Deployment**, and then click **Server View**.
- 2 To view bare-metal servers, click **Unassigned Servers** tab.

- 3 To view host servers, click **Hosts** tab.
 - a To view host groups in nested format as grouped in SCCM or SCVMM, click **Select Console Hosts** drop-down menu.The **Select Console Hosts** drop-down menu lists all the host groups present in SCCM along with an internal group name. If you select the internal group name, all the hosts that are discovered and managed in SCCM and OMIMSSC are displayed.

Next steps

After discovering servers, consider the following points:

- The **Operational Template** column is displayed as **Not Assigned**, after the servers are discovered. To update firmware and deploy operating system on these servers, assign and deploy Operational Templates. For more information, see [Managing Operational Templates](#).
- The discovered servers are added to predefined groups in OMIMSSC. You can create custom update groups based on functional requirements. For more information, see [About update groups](#).
- When you log in to OMIMSSC as a delegated admin, you can view all the host and unassigned servers that are not specific to this user. Hence, ensure that you have the required privileges before performing any operations on the servers.
- If there are multiple Microsoft consoles enrolled in OMIMSSC, and then host servers are specific to the Microsoft console where they are managed. And the unassigned servers are common to all consoles.

Launching Modular Systems view

The **Modular Systems View** page lists all the Modular Systems that are discovered in OMIMSSC.

About this task

View the CMC IP address, service tag, model, firmware version, template compliance status of Modular System for an assigned Operational Template, number of servers, Input/Output (I/O) Modules, and storage devices present on that Modular System. Configure the hardware and update Modular System firmware, by deploying the Operational Template.

You can perform the following tasks on **Modular Systems View** page:

- [Discover Modular Systems using manual discovery](#)
- Delete Modular System
- To view latest inventory information, refresh the page.
- [Assign Operational Template for Modular System](#)
- [Deploy Operational Template for Modular System](#)
- [View I/O modules](#)
- [Launching I/O modules](#)

To view Modular System discovered in OMIMSSC:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**.
All the Modular Systems discovered model names are displayed.
- 2 To view a specific Modular System, click a model name under **Modular Systems View**.
All the Modular Systems of that model are displayed with their service tag.
- 3 To view all devices present in that Modular System, click service tag.
All the servers, Input Output modules, and storage devices along with their details are displayed.

NOTE: Only after a deep discovery of a Modular System, all devices in the Modular System and their information are displayed.

- By default the **Servers** tab is displayed.
All the servers that are discovered in this Modular System are displayed.
- To view all the Input Output Modules present in a Modular System, click **I/O Modules** tab.
- To view all the storage devices present in the Modular System, click **Storage Devices** tab.

Next steps

After discovering Modular Systems, consider the following points:

- The **Operational Template** column is displayed as **Not Assigned**, after the Modular Systems are discovered. To update firmware and deploy operating system on these Modular Systems, assign and deploy Operational Templates. For more information, see [Managing Operational Templates](#).
- View the count of Input/Output, storage devices, and servers present in Modular Systems after a shallow discovery. Perform a deep discovery, to view more details about the components in a Modular System.

Launching OpenManage Enterprise Modular console

About this task

To launch OpenManage Enterprise Modular console, perform the following steps:

Steps

- 1 In OMIMSSC, expand **Configuration and Deployment**, and click **Modular Systems**.
- 2 Click **Device IP** of the Modular System.

Input/Output Modules

All the network Input/Output Modules along with their IP address, service tag, Input/Output type, model, firmware version and slot information are displayed.

About this task

[Launch I/O Modules](#) console from Input/Output Modules page.

To view information about Input/Output Modules, perform the following steps:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**. Expand the **Modular Systems View**, and click service tag.
All service tag of that model are displayed.
- 2 To view the Input/Output module, click **I/O Modules** tab.

Launching Input Output Modules console

About this task

To launch Input Output Module console, perform the following steps:

Steps

- 1 In OMIMSSC, expand **Configuration and Deployment**, click **Modular Systems View**. Expand the model to individual devices level.
All devices under that model are displayed.
- 2 Click **I/O Modules** tab.
- 3 Click **IP address** of the device.

Launching Cluster View

The **Cluster View** page lists all the clusters discovered in OMIMSSC. View cluster's Fully Qualified Name (FQDN), service tag, and number of servers present in that cluster. Also, create a logical switch for clusters, and then create Storage Spaces Direct clusters using the predefined Operational Template.

About this task

You can perform the following tasks on **Cluster View** page:

- [Creating logical switch](#) (only for SC2016 VMM users)
- [Creating Storage Spaces Direct clusters](#) (only for SC2016 VMM users)
- [Launching iDRAC console](#)

- To view latest clusters discovered, refresh the page

To view cluster groups discovered in OMIMSSC:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and then click **Cluster View**.
All the different types of clusters are grouped and listed.
- 2 To view information about specific type of clusters, expand the cluster type.
All the clusters of this type are listed on the left pane.
- 3 To view servers present in a cluster, click a cluster name.

Launching iDRAC console

About this task

To launch iDRAC console, perform the following step:

Step

In OMIMSSC, expand **Configuration and Deployment**, and select one of the following:

- Click **Server View**. Based on the server (if it is a host or an unassigned server), click **Unassigned Servers** or **Hosts** tab, and click the **iDRAC IP** address of the server.
The **Unassigned Servers** tab is displayed by default.

To view the hosts tab, click **Hosts**.
- Click **Cluster View**. Expand the cluster type and expand cluster group to server level.
The **Server** tab is displayed.

Launching Maintenance Center

The **Maintenance Center** page lists all the discovered devices in groups and the resources that are required for maintaining devices in OMIMSSC. In **Maintenance Center** page, view the device's firmware inventory, manage the devices by keeping their firmware up-to-date as per the recommendations, revert the server to an earlier state if it has crashed, bring up a replaced component to the same configuration of the old component, and export server logs for troubleshooting any issues. In **Update Settings** page view all the update sources, polling and notifications for latest updates from default update source, update groups of devices that require similar management, and all the protection vaults required for server configurations.

About this task

NOTE: By default, OMIMSSC is packaged with a catalog file that displays an earlier version of the comparison report for predefined FTP, HTTP, and HTTPS update source. Hence, download the latest catalog to display the latest comparison report. To download the latest catalog, edit and save the FTP, HTTP, and HTTPS update sources.

You can perform the following tasks on **Maintenance Center** page:

- [Create update source](#)
- [Set polling frequency](#)
- Select predefined update groups or [Create custom update groups](#).
- [View and refresh firmware inventory](#)
- [Upgrade and downgrade firmware versions using run update method](#)
- [Create protection vaults](#)
- [Export server profiles](#)
- [Import server profiles](#)
- [Exporting inventory](#)

To view **Maintenance Center** page:

Step

In OMIMSSC, click **Maintenance Center**.

The **Maintenance Center** page is displayed.

Launching Jobs and Logs Center

View information about jobs initiated in OMIMSSC along with status of job's progress, and its subtask. Also, you can filter and view jobs of a particular job category.

About this task

You can view jobs that are initiated from OMIMSSC, in OMIMSSC Admin Portal and OMIMSSC console extension.

- OMIMSSC Admin portal—displays jobs that are initiated from all OMIMSSC consoles and users
- OMIMSSC console—displays jobs specific to a user and a console

Job names are either generated by the system or provided by users, and the subtasks are named after the IP address or hostname of the managed systems. Expand the subtask to view the activity logs for that job. Jobs are classified under four groups:

- **Running**—displays all the jobs that are currently running and in-progress state.
- **History**—displays all the jobs run in the past with its job status.
- **Scheduled**—displays all the jobs that are scheduled for a future date and time. Also, you can cancel these scheduled jobs.
- **Generic Logs**—displays OMIMSSC Appliance-specific, common log messages that are not specific to a task, and other activities. Every job is displayed with a user name and a console FQDN from where it was initiated.
 - **Appliance Log Messages**—displays all OMIMSSC Appliance-specific log messages such as restarting OMIMSSC Appliance. You can view this category of messages only from OMIMSSC Admin Portal.
 - **Generic Log Messages**—displays log messages that are common across different job categories that are listed in **Running**, **History**, and **Scheduled** tabs. These logs are specific to a console and a user.
For example, if a firmware update job is in-progress for a group of servers, the tab displays log messages that belong to creating the Server Update Utility (SUU) repository for that job.

The various states of a job that is defined in OMIMSSC are as follows:

- **Canceled**—job is manually canceled, or after OMIMSSC Appliance restarts.
- **Successful**—job is completed successfully.
- **Failed**—job is not successful.
- **In Progress**—job is running.
- **Scheduled**—job has been scheduled for a future date and time.

 **NOTE:** If multiple jobs are submitted simultaneously to the same device, the jobs fail. Hence, ensure that you schedule jobs for same device at different times.

- **Waiting**—job is in a queue.
- **Recurring Schedule**—job is scheduled at regular intervals.

Steps

- 1 In OMIMSSC, click **Jobs and Log Center**.
- 2 To view a specific category of jobs, such as **Scheduled**, **History**, or **Generic**, click the required tab.
Expand a job to view all the devices included in that job. Expand further to view the log messages for that job.

 **NOTE:** All the job-related generic log messages are listed under the **Generic** tab and not under the **Running** or **History** tab.

- 3 (Optional) Apply filters to view different groups of jobs and status of job in **Status** column.

Managing profiles

Profiles contain all the data that is required for performing any operations in OMIMSSC.

Topics:

- [About credential profile](#)
- [About hypervisor profile \(for SCVMM users\)](#)

About credential profile

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of the user. Each credential profile contains a user name and password for a single user account.

OMIMSSC uses credential profiles to connect to the managed systems' iDRAC. Also, you can use credential profiles to access the FTP site, resources available in Windows shares, and to work with different features of iDRAC.

You can create four types of credential profiles:

- Device Credential Profile—used to log in to iDRAC or CMC. Also, you can use this profile to discover a server, resolve synchronization issues, and deploy operating system. This profile is specific to a console. You can use and manage this profile only in a console where it is created.
- Windows Credential Profile—used for accessing share folders in Windows operating system
- FTP Credential Profile—used for accessing an FTP site
- Proxy Server Credentials—used for providing proxy credentials for accessing any FTP sites for updates.

 **NOTE:** All profiles other than device profile are shared resources. You can use and manage these profiles from any of the enrolled consoles.

Predefined credential profile

SYSTEM DEFAULT FTP account is a predefined credential profile available in OMIMSSC. The predefined credential profile is of type FTP, having **User Name**, and **Password** as **anonymous**. Use this profile to access `ftp.dell.com`

Creating credential profile

About this task

When creating a credential profile, consider the following points:

- During auto discovery, if a default credential profile is not available for iDRAC, and then the default iDRAC credentials is used. The default iDRAC user name is `root`, and password is `calvin`.
- To get information about the modular systems, the modular server is accessed with default CMC profile. The default CMC profile user name is `root` and password is `calvin`.
- (Only for SCVMM users) When a device type credential profile is created, an associated **RunAsAccount** is created in **SCVMM** to manage the device, and the name of the **RunAsAccount** is `Dell_CredentialProfileName`.
- Ensure that you do not edit, or delete the **RunAsAccount** in SCVMM.

Steps

- 1 In OMIMSSC, perform any of the following steps to create a **Credential Profile**:
 - In OMIMSSC dashboard, click **Create Credential Profile**.
 - In the navigation pane, click **Profiles > Credential Profile**, and then click **Create**.
- 2 In **Credential Type**, select the credential profile type that you want to use.
- 3 Provide a profile name and description.

 **NOTE:** Default Profile for option is applicable only for a Device type credential profile.

- 4 In **Credentials**, provide the user name and password.
 - If you are creating a **Device Credential Profile**, select to make this profile as the default profile to log in to iDRAC or CMC by selecting the **Default Profile for** option. Select **None**, if you choose not to set the profile as a default profile.
 - If you are creating a **Windows Credential Profile**, provide the domain details in **Domain**.

 **NOTE:** Provide the domain name with Top Level Domain (TLD) details while creating the credential profile for console enrollment.

For example, if the domain name is `mydomain`, and the TLD is `com`, provide the domain name in credential profile as: `mydomain.com`.

- If you are creating a **Proxy Server Credentials**, provide the proxy server URL `http://hostname:port` or `http://IPAddress:port` format in **Proxy Server URL**.
- 5 To create the profile, click **Finish**.

Modifying credential profile

About this task

Consider the following before modifying a credential profile:

- After creating, you cannot modify the type of a credential profile. However, you can modify other fields.
- You cannot modify a credential profile, if it is in use.

 **NOTE:** The steps to modify any type of credential profile are the same.

Steps

- 1 Select the credential profile that you want to modify, click **Edit**, and update the profile.
- 2 To save the changes made, click **Save**.

Next step

To view the changes made, refresh the **Credential Profile** page.

Deleting credential profile

About this task

Consider the following when you are deleting a credential profile:

- When a device type credential profile is deleted, the associated **RunAsAccount** from SCVMM is also deleted.
- When **RunAsAccount** in SCVMM is deleted, the corresponding credential profile is not available in OMIMSSC.
- To delete a credential profile that is used in discovering servers, delete the discovered server and then delete the credential profile.
- To delete a device type credential profile that is used for deployment, first delete the servers that are deployed in the SCVMM environment and then delete the credential profile.
- You cannot delete a credential profile if it is used in an update source.

 **NOTE:** The steps to delete any type of credential profile are the same.

Step

Select the credential profile that you want to delete, and then click **Delete**.

Next step

To view the changes made, refresh the **Credential Profile** page.

About hypervisor profile (for SCVMM users)

A hypervisor profile contains a customized WinPE ISO (WinPE ISO is used for hypervisor deployment), host group, and host profile taken from SCVMM, and LC drivers for injection. Only OMIMSSC console extension for SCVMM users, can create and manage hypervisor profiles.

Creating hypervisor profile

Create a hypervisor profile and use the profile to deploy hypervisors.

Prerequisites

- Update the WinPE ISO image, and have access to the share folder where the image is saved. For information about updating the WinPE image, see [WinPE update](#).
- Create a host group, and host profile or physical computer profile, in SCVMM. For information about creating host groups in SCVMM, see Microsoft documentation.


Steps

- 1 In OMIMSSC, perform any one of the following tasks:
 - In the OMIMSSC dashboard, click **Create Hypervisor Profiles**.
 - In the left navigation pane, click **Profiles and Templates, Hypervisor Profile**, and then click **Create**.

The **Hypervisor Profile Wizard** is displayed.
- 2 In the **Welcome** page click **Next**.
- 3 In **Hypervisor Profile**, provide a name and description of the profile, and then click **Next**.
- 4 In the **SCVMM Information** page,
 - a For **SCVMM Host Group Destination**, select an SCVMM host group from the drop-down menu to add the host into this group.
 - b From **SCVMM Host Profile/Physical Computer Profile**, select a host profile or physical computer profile from SCVMM that includes configuration information to be applied on servers.

In SCVMM, select one of the following disk partition methods in a **Physical Computer Profile**:

 - When booting to UEFI mode, select **GUID Partition Table (GPT)** option.
 - When booting to BIOS mode, select **Master Board Record (MBR)** option.
- 5 In **WinPE Boot Image Source**, provide the following details, and click **Next**.
 - a For **Network WinPE ISO Name**, provide the share folder path having the updated WinPE file name. For updating WinPE file, see [WinPE update](#).
 - b For **Credential Profile**, select the credentials having access to share folder having the WinPE file.
 - c (Optional) To create a windows credential profile, click **Create New**. For information about creating credential profile, see [Creating credential profile](#).
- 6 (Optional) To enable LC driver injection, perform the following steps:



NOTE: Ensure that you select **Enable Dell Lifecycle Controller Drivers Injection** check-box, because the latest operating system driver packs for NIC cards are available in the latest operating system drivers.

 - a Select the operating system that you want to deploy so that the relevant drivers are selected.
 - b Select **Enable LC Drivers Injection**.
 - c Select the hypervisor version **Hypervisor Version**.
- 7 In **Summary**, click **Finish**.

Next step

To view the changes made, refresh the **Hypervisor profile** page.

Modifying hypervisor profile

About this task

Consider the following when you are modifying a hypervisor profile:

- You can modify host profile, host group, and drivers from Lifecycle Controller.
- You can modify the WinPE ISO name. However, you cannot modify the ISO image.

Steps

- 1 Select the profile that you want to modify and click **Edit**.
- 2 Provide the details, and click **Finish**.

Next step

To view the changes made, refresh the **Hypervisor profile** page.

Deleting hypervisor profile

Step

Select the hypervisor profile that you want to delete, and click **Delete**.

Next step

To view the changes made, refresh the **Hypervisor profile** page.

Discovering devices and synchronizing servers with MSSC console

Discovery is the process of adding supported modular systems and PowerEdge bare-metal servers or host servers or nodes in to OMIMSSC.

Synchronization with MSSC console is the process of adding host servers from registered Microsoft console (SCCM or SCVMM) in to OMIMSSC. Hence, using any one of the processes, you can add devices in to OMIMSSC . Only after discovering the devices, you can manage them in OMIMSSC.

Topics:

- [About reference server configuration](#)
- [About reference Modular System configuration](#)
- [Discovering devices in OMIMSSC](#)
- [Synchronization of OMIMSSC console extension with enrolled SCCM](#)
- [Resolving synchronization errors](#)
- [Viewing System Lockdown Mode](#)
- [Deleting servers from OMIMSSC](#)

About reference server configuration

A server configuration with a preferred boot sequence, BIOS, RAID settings, hardware configuration, firmware update attributes, and operating system parameters that is ideally suited for an organization is called reference server configuration.

Discover a reference server and capture the reference server settings in an Operational Template, and replicate it across different servers with same hardware configuration.

About reference Modular System configuration

A Modular System configuration with a preferred network configuration, user account, security, and alerts that is ideally suited for an organization is called reference Modular System configuration or reference chassis.

Discover a reference Modular System and capture the reference Modular System settings in an Operational Template, and replicate it across different Modular Systems of the same models.

Discovering devices in OMIMSSC

Discover MX7000 Modular Systems, hosts, and unassigned servers in OMIMSSC. Information about discovered devices is saved in OMIMSSC Appliance.

Using the following methods, you can discover Dell EMC servers using their iDRAC IP address:

- [Discovering servers using auto discovery](#)
- [Discovering servers using manual discovery](#)

① **NOTE:** The discovered device is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS that are required to work with OMIMSSC. For information about supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.

Discover Modular Systems with device IP address using [Discovering modular systems using manual discovery](#) method.

Device discovery in OMIMSSC console extension for SCCM

Discover devices in OMIMSSC console extension for SCCM. After discovering a server, the server is added to a predefined group in OMIMSSC, and one of the following SCCM predefined groups or collections—**All Dell Lifecycle Controller Servers collection** and **Import Dell Server collection** that are created under the **Device Collections**.

If the discovered server is not present in SCCM, or if there are no predefined groups or collections in SCCM, the predefined collections are created and the discovered server is and then added to the respective group.

Device discovery in OMIMSSC console extension for SCVMM

Discover Modular Systems, hyper-V hosts, and unassigned servers in OMIMSSC console extension for SCVMM. After discovery, the devices are added to respective predefined update groups.

System requirements for managed systems

Managed systems are the devices that are managed using OMIMSSC. The system requirements for discovering servers using OMIMSSC console extensions are as follows:

- OMIMSSC console extension for SCCM supports modular, monolithic, and tower server models on 11th and later generations of servers.
- OMIMSSC console extension for SCVMM supports modular and monolithic server models on 11th and later generations of servers.
- For source configuration and destination configuration, use same type of disks—only Solid-state Drive (SSD), SAS, or only Serial ATA (SATA) drives.
- For successful hardware profile RAID cloning, for destination system disks, use same or greater size and number of disks as present in the source.
- RAID sliced virtual disks are not supported.
- iDRAC with shared LOM is not supported.
- RAID configured on external controller is not supported.
- Enable Collect System Inventory on Restart (CSIOR) in managed systems. For more information, see iDRAC documentation.

Discovering servers using auto discovery

To automatically discover servers, connect servers to the network and power on the servers. OMIMSSC auto discovers the unassigned servers by using the remote enablement feature of iDRAC. OMIMSSC works as a provisioning server and uses iDRAC reference to auto discover servers.

- 1 In OMIMSSC, create a device type credential profile by providing the iDRAC credentials and make it as default for servers. For information about creating a credential profile, see [Creating a credential profile](#).
- 2 Disable the existing Administrator account in iDRAC settings in the managed device.

① **NOTE:** It is recommended that you have a guest user account with operator privileges to log in to iDRAC in case auto discovery fails.

- 3 Enable the auto discovery feature in managed device's iDRAC settings. For more information, see iDRAC documentation.
- 4 In managed device's, iDRAC Settings, provide OMIMSSC Appliance IP in **provision server IP**, and then restart the server.

Discovering servers using manual discovery

To manually discover PowerEdge servers by using an IP address or an IP range. To discover servers, provide the iDRAC IP address and the device type credentials of a server. When you are discovering servers by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of a server.

Prerequisite

Ensure that a default credential profile is available.

Steps

- 1 In OMIMSSC console, perform any one of the following steps:
 - In the dashboard, click **Discover Servers**.
 - In the navigation pane, click **Configuration and Deployment**, click **Server View**, and then click **Discover**.
- 2 In the **Discover** page, select the required option:
 - **Discover Using an IP Address**—to discover a server using an IP address.
 - **Discover Using an IP Range**—to discover all servers within an IP range.
- 3 Select the device type credential profile, or click **Create New** to create a device type credential profile.
The selected profile is applied to all the servers.
- 4 In **iDRAC IP address**, provide the IP address of the server that you want to discover.
- 5 In **Discover Using an IP Address or IP Address Range**, do any of the following:
 - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
 - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.
- 6 Provide a unique job name, description for the job, and click **Finish**.
To track this job, the **Go to the Job List** option is selected by default.

The **Jobs and Logs Center** page is displayed. Expand the discovery job to view the progress of the job in **Running** tab.

After discovering a server, the server is added to **Hosts** tab, or **Unassigned** tab in the **Server View** page of **Configuration and Deployment** section.

- When you discover a server with an operating system that is deployed on it, and the server is already present in SCCM or SCVMM console, and then the server is listed as a host server under the **Hosts** tab.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, and then the server is listed as an unassigned server under the **Unassigned** tab in all the OMIMSSC console extensions, in case of multiple Microsoft consoles enrolled to single OMIMSSC Appliance.

After discovering a server, the server is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS to work with OMIMSSC. To view the firmware versions of the server components, hover the hover over the **Hardware Compatibility** column against the server row. For information about the supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.

A license is consumed for each discovered server. The **Licensed Nodes** count in **License Center** page decreases as the number of servers are discovered.

NOTE: To work with the servers discovered in the prior versions of OMIMSSC Appliance, rediscover the servers.

NOTE: When you log in to OMIMSSC as a delegated admin, you can view all the host servers and unassigned servers that are not specific to the logged in user. Hence, you cannot perform any operations on such servers. Make sure that you have the required privileges before performing any operations on such servers.

Discovering MX7000 by using manual discovery

To manually discover PowerEdge MX7000 Modular System by using an IP address or an IP range, provide a Modular System's IP address and device type credentials of the Modular System. When you are discovering Modular Systems by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of the Modular Systems.


Prerequisite

Ensure that the default credential profile of a Modular System you want to discover is available.

About this task

To discover Modular Systems, perform the following steps:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, click **Modular Systems View**, and then click **Discover**.
 - 2 In the **Discover** page, select the required option:
 - **Discover Using an IP Address**—to discover a Modular System using an IP address.
 - **Discover Using an IP Range**—to discover all Modular Systems within an IP range.
 - 3 Select the device type credential profile, or click **Create New** to create a device type credential profile.
The selected profile is applied to all the servers.
 - 4 In **IP address**, provide the IP address of the Modular System that you want to discover.
 - 5 In **Discover Using an IP Address or IP Address Range**, do one of the following:
 - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
 - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.
 - 6 In **Modular Systems Discovery Methods**, select one of the following:
 - **Shallow discovery**—discovers Modular Systems and also number of servers in the Modular System.
 - **Deep discovery**—discovers Modular Systems and devices present in the Modular System such as Input Output Modules (IOM) and storage devices.
-  **NOTE:** To deep discover MX7000 and its components, ensure that PowerEdge MX7000 and all its components are enabled with IPv4 address.
- 7 Provide a unique job name, and click **Finish**.
To track this job, the **Go to the Job List** option is selected by default.

To view the progress of the job in the **Running** tab, expand the discovery job in **Jobs and Logs Center**.

Synchronization of OMIMSSC console extension with enrolled SCCM

You can synchronize all servers (hosts and unassigned) from enrolled SCCM to OMIMSSC. Also, you get the latest firmware inventory information about the servers after synchronization.

Before synchronizing OMIMSSC and the enrolled SCCM console, ensure that the following requirements are met:

- Have details of default iDRAC credential profile for servers.
- Update the **Dell Default Collection** before synchronizing OMIMSSC with SCCM. However, if an unassigned server is discovered in SCCM, it is added to **Import Dell server collection**. To add this server in **Dell Default Collection**, add the server's iDRAC IP address in the **OOB** page.
- Ensure that there are no duplicate entries of devices in SCCM.

After synchronizing OMIMSSC with SCCM, if the device is not present in SCCM, and then the **All Dell Lifecycle Controller Servers** collection and the **Import Dell server** collection under **Device Collections** is created and the server is added to that respective group.

Synchronization of OMIMSSC console extension with enrolled SCVMM

You can synchronize all hyper-V hosts, hyper-V host clusters, modular hyper-V hosts, and unassigned servers from SCVMM consoles with OMIMSSC console extension for SCVMM. Also, you get the latest firmware inventory information about the servers after synchronization. Consider the following before synchronizing OMIMSSC with SCVMM:

- Have details of default iDRAC credential profile for servers.
- If the host server's Baseboard Management Controller (BMC) is not configured with the iDRAC IP address, and then you cannot synchronize the host server with OMIMSSC. Hence, configure BMC in SCVMM (for more information, see MSDN article at technet.microsoft.com), and then synchronize OMIMSSC with SCVMM.
- SCVMM supports numerous hosts in the environment, due to which synchronization is a long running task.

Synchronizing with enrolled Microsoft console

About this task

To add servers managed in Microsoft console to OMIMSSC, perform the following step:

Step

In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Synchronize with OMIMSSC** to synchronize all the hosts that are listed in enrolled MSSC with the OMIMSSC Appliance.

Resolving synchronization errors

The servers that are not synchronized with OMIMSSC are listed with their iDRAC IP address and host name.

About this task

- ① **NOTE:** All servers that are not synchronized due to issues such as invalid credentials, or the iDRAC IP address, or connectivity, or other issues; ensure that you resolve the issues first, and then synchronize.
- ① **NOTE:** During resynchronization, host servers that are deleted from the enrolled MSSC environment are moved to the **Unassigned Servers** tab in the OMIMSSC console extensions. If a server is decommissioned, and then remove that server from the list of unassigned servers.

To resynchronize servers with credential profile issues:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Resolve Sync Errors**.
- 2 Select the servers for resynchronization, and select the credential profile, or to create a credential profile click **Create New**.
- 3 Provide a job name, and if necessary select the **Go to the Job List** option to view the job status automatically once the job is submitted.
- 4 Click **Finish** to submit the job.

Viewing System Lockdown Mode

The System Lockdown Mode setting is available in iDRAC for 14th generation of servers and later. The setting when turned on locks the system configuration including firmware updates. After the System Lockdown mode is enabled, users cannot change any configuration settings. This setting is intended to protect the system from unintentional changes. To perform any operations on the managed servers, ensure that you disable the setting on its iDRAC console. In OMIMSSC console, the System Lockdown mode status is represented with a lock image before the iDRAC IP address of the server.

- A lock image is displayed along with the servers's iDRAC IP if the setting is enabled on that system.

- An unlocked image is displayed along with the servers's iDRAC IP if the setting is disabled on that system.

NOTE: Before launching the OMIMSSC console extensions, verify the iDRAC System Lockdown Mode setting on the managed servers.

For more information about iDRAC System Lockdown Mode, see iDRAC documentation available at dell.com/support.

Deleting servers from OMIMSSC

About this task

To delete a server, perform the following steps:

Consider the following points before deleting a server:

- After you delete a server, the consumed license is relinquished.
- You can delete a server that is listed in OMIMSSC based on the following criteria:
 - An unassigned server that is listed in the **Unassigned servers** tab.
 - If you delete a host server that is provisioned in enrolled SCCM or SCVMM and present in OMIMSSC under the **Hosts** tab, first delete the server in SCCM or SCVMM, and then delete the server from OMIMSSC.

Steps

- 1 In the OMIMSSC console, click **Configuration and deployment**, and then click **Server View**:
 - To delete unassigned servers—in the **Unassigned Servers** tab, select the server, and click **Delete**.
 - To delete host servers—in the **Host Servers** tab, select the server, and click **Delete**.
- 2 In the confirmation dialog box, click **Yes**.

Deleting Modular Systems from OMIMSSC

About this task

To delete a Modular System, perform the following steps:

Steps

- 1 In OMIMSSC console, click **Configuration and deployment**, and then click **Modular Systems View**.
- 2 Select the Modular Systems, and click **Delete**.

Preparing for operating system deployment

Before deploying Windows operating system on the managed servers, update the WinPE image, create a task sequence, LC boot media file, and task sequence media bootable ISO file. The steps vary for SCCM and SCVMM console users. Refer the below section for more details. For deploying non-windows operating system remember the points mentioned in [Preparing for non-Windows OS deployment](#) section.

Topics:

- [About WinPE image](#)
- [Preparing for operating system deployment on SCCM console](#)
- [Preparing for non-Windows operating system deployment](#)

About WinPE image

Windows Preinstallation Environment (WinPE) image is used for deploying operating system. Use an updated WinPE image for deploying operating system as the WinPE image available from SCCM or SCVMM may not contain the latest drivers. To create a WinPE image having all the required drivers, update the image using DTK. Ensure that relevant operating system-related driver packs are installed in Lifecycle Controller.

 **NOTE:** Do not change the filename of boot.wim file.

Providing WIM file for SCCM

Copy the **boot.wim** file from the following location `\\shareip\sms_sitecode\OSD\boot\x64\boot.wim`, and then paste it to a share folder accessible by OMIMSSC.

For example, location of shared path: `\\shareip\sharefolder\boot.wim`

Providing WIM file for SCVMM

- 1 Install Windows Deployment Server (WDS) role on a server, and then add the PXE server to SCVMM.
For information about adding the WDS role on a server, and adding a PXE server to SCVMM, see Microsoft documentation.
- 2 Copy the **boot.wim** file from the PXE server present at the following location `C:\RemoteInstall\DCMgr\Boot\Windows\Images`, and then paste it to a share folder accessible by OMIMSSC.
For example, location of shared path: `\\shareip\sharefolder\boot.wim`

Extracting DTK drivers

A DTK file contains the necessary firmware versions that are required for servers on which you are deploying the operating systems.

About this task

 **NOTE:** While using the latest version of DTK for creating a WinPE ISO image, use the Dell EMC OpenManage Deployment Toolkit for Windows file. The Dell EMC OpenManage Deployment Toolkit for Windows file contains the necessary firmware versions that are required for systems on which you are deploying the operating systems. Use the latest version of the file, and do not use the Dell EMC OpenManage Deployment Toolkit Windows Driver Cabinet file for the WinPE update.

Steps

- 1 Double-click the DTK executable file.
- 2 To unzip the DTK drivers, select a folder.
For example, C:\DTK501.
- 3 Copy the unzipped DTK folder to a share folder.
For example, \\Shareip\sharefolder\DTK\DTK501

NOTE: If you are upgrading from SCVMM SP1 to SCVMM R2, and then upgrade to Windows PowerShell 4.0. and create a WinPE ISO image.

Updating WinPE image

About this task

A unique job name is assigned to each WinPE update job.

Steps

- 1 In OMIMSSC, select **WinPE Update**.
The **WinPE Update** page is displayed.
- 2 In **Image Source**, for **Custom WinPE Image Path**, enter the WinPE image path along with the file name where the image is present.
For example, \\Shareip\sharefolder\WIM\boot.wim.
- 3 Under **DTK Path**, for **DTK Drivers Path**, enter the location for the Dell EMC Deployment Toolkit drivers.
For example, \\Shareip\sharefolder\DTK\DTK501
- 4 Under **Output File**, for **ISO or WIM File Name**, enter a name for the file along with the file type that will be generated after updating the WinPE image.
Enter one of the output file types:
 - WIM file for SCCM
 - ISO file for SCVMM
- 5 Under **Credential Profile**, for **Credential Profile**, enter the credentials that have access to the share folder where the WinPE image is saved.
- 6 (Optional) To view the job list, select **Go to the Job List**.
A unique job name is assigned to each Windows Preinstallation Environment (WinPE) update.
- 7 Click **Update**.
WinPE image with the file name that is provided in the preceding step is created under \\Shareip\sharefolder\WIM.

Preparing for operating system deployment on SCCM console

Before deploying operating system on managed servers discovered using OMIMSSC in SCCM console, create a Dell EMC specific or a custom task sequence, an LC boot media file, and task sequence media bootable ISO file.

Task sequence-SCCM

Task sequence is a series of commands that is used to deploy operating system on the managed system using SCCM.

Before creating Operational Template, Dell EMC recommends that you complete the following prerequisites.

- In Configuration Manager, ensure that the system is discovered and present under **Assets and Compliance > Device Collections > All Dell Lifecycle Controller Servers**. For more information, see [Discover servers](#).
- Install the latest BIOS version on the system.

- Install the latest version of Lifecycle Controller on the system.
- Install the latest version of iDRAC firmware on the system.

NOTE: Always launch the Configuration Manager console with administrator privileges.

Types of task sequence

You can create a task sequence in two ways:

- Create a Dell-specific task sequence using OMIMSSC Deployment template.
- Create a custom task sequence.

The task sequence goes to the next task sequence step irrespective of the success or failure of the command.

Creating Dell specific task sequence

About this task

To create a Dell-specific task sequence by using **OMIMSSC Server Deployment Template** option in SCCM:

Steps

- 1 Launch Configuration Manager.
The Configuration Manager console screen is displayed.
- 2 In the left pane, select **Software Library > Overview > Operating Systems > Task Sequences**.
- 3 Right-click **Task Sequences**, and then click **OMIMSSC Server Deployment > Create OMIMSSC Server Deployment Template**.
The **OMIMSSC Server Deployment Task Sequence Wizard** is displayed.
- 4 Type the name of the task sequence in the **Task Sequence Name** field.
- 5 Select the boot image that you want to use from the drop-down list.

NOTE: It is recommended that you use the Dell custom boot image that you created.
- 6 Under **Operating System Installation**, select the operating system installation type. The options are:
 - **Use an OS WIM image**
 - **Scripted OS install**
- 7 Select an operating system package from the **Operating system package to use** drop-down menu.
- 8 If you have a package with **unattend.xml**, and then select it from the **Package with unattend.xml info** menu, else select **<do not select now>**.
- 9 Click **Create**.
The **Task Sequence Created** window is displayed with the name of the task sequence you created.
- 10 Click **Close** in the confirmation message box that is displayed.

Creating a custom task sequence

- 1 Launch the Configuration Manager.
The Configuration Manager console is displayed.
- 2 In the left pane, select **Software Library > Overview > Operating Systems > Task Sequences**.
- 3 Right-click **Task Sequences**, and then click **Create Task Sequence**.
The **Create Task Sequence Wizard** is displayed.
- 4 Select **Create a new custom task sequence**, and click **Next**.
- 5 Enter a name for the task sequence in the **Task sequence name** text box.
- 6 Browse for the Dell boot image that you had created, and click **Next**.
The **Confirm the Settings** screen is displayed.
- 7 Review your settings and click **Next**.

- Click **Close** in the confirmation message box that is displayed.

Editing a task sequence

About this task

- NOTE:** While editing task sequence on SCCM 2016, the missing objects references messages does not list Setup windows and ConfigMgr package. Add the package and then save the task sequence.

Steps

- Launch the Configuration Manager.
The Configuration Manager screen is displayed.
- In the left pane, select **Software Library > Operating Systems > Task Sequence**.
- Right-click the task sequence that you want to edit and click **Edit**.
The **Task Sequence Editor** window is displayed.
- Click **Add > Dell Deployment > Apply Drivers from Dell Lifecycle Controller**.
The custom action for your Dell server deployment is loaded. You can now make changes to the task sequence.

- NOTE:** When editing a task sequence for the first time, the error message, Setup Windows and Configuration Manager is displayed. To resolve the error, create and select the Configurations Manager Client Upgrade package. For more information about creating packages, see the Configuration Manager documentation at technet.microsoft.com.

Setting a default share location for the Lifecycle Controller boot media

About this task

To set a default share location for the Lifecycle Controller boot media:

Steps

- In **Configuration Manager**, select **Administration > Site Configuration > Sites**.
- Right-click **<site server name>** and select **Configure Site Components**, and then select **Out of Band Management**.
The **Out of Band Management Component Properties** window is displayed.
- Click the **Lifecycle Controller** tab.
- Under **Default Share Location for Custom Lifecycle Controller Boot Media**, click **Modify** to modify the default share location of the custom Lifecycle Controller boot media.
- In the **Modify Share Information** window, enter a new share name and share path.
- Click **OK**.

Creating a task sequence media bootable ISO

- In Configuration Manager under **Software Library**, right-click **Task Sequences**, and select **Create Task Sequence Media**.
NOTE: Ensure that you manage and update the boot image across all distribution points before starting this wizard.
NOTE: OMIMSSC does not support the Standalone Media method to create Task Sequence Media.
- From the **Task Sequence Media Wizard**, select **Bootable Media**, select **Allow unattended operating system deployment** option, and click **Next**.
- Select **CD/DVD Set**, and click **Browse** and select the location to save the ISO image.
- Click **Next**.
- Clear the **Protect Media with a Password** check box and click **Next**.

- 6 Browse and select **PowerEdge server Deployment Boot Image**.

 **NOTE:** Use the boot image created using DTK only.

- 7 Select the distribution point from the drop-down menu, and select the **Show distribution points from child sites** check box.

- 8 Click **Next**.

The **Summary** screen is displayed with the task sequence media information.

- 9 Click **Next**.

The progress bar is displayed.

- 10 On completion of creation of the image, close the wizard.

Preparing for non-Windows operating system deployment

Ensure that you remember the following points for deploying non-windows operating systems on managed systems:

- ISO file is available in either Network File System Version (NFS) or Common Internet File System (CIFS) share with read and write access.
- Confirm that virtual drive is available on the managed system.
- After deploying ESXi operating system, the server is moved to **Managed Lifecycle Controller (ESXi)** collection in SCCM.
- After deploying any type of non-windows operating system, the servers are moved to **Default Non-Windows Host Update Group**.
- It is recommended that the network adapter is connected to the network port in the server on which the operating system is being deployed.

Managing Operational Templates

Operational Templates contain complete device configuration and are used for deploying operating system and update firmware for PowerEdge servers and Modular Systems within Microsoft environment.

Operational Templates capture the complete configurations from a reference server, or reference Modular System. Then you can modify the hardware configurations, set firmware update attributes, and operating system parameters (only for servers) in an Operational Template if required and deploy this template across devices. Also, you can check the compliance status against an assigned Operational Template and view the compliance report in a summary page.

For information about reference server and reference Modular System, see [About reference server configuration](#) and [About reference Modular System configuration](#).

The following table lists all the features that Operational Template supports:

Table 2. Functionality of OMIMSSC

Component	Configuration and deployment	Firmware update	View inventory	Operational Template compliance status
BIOS	Yes	Yes	Yes	Yes
iDRAC	Yes	Yes	Yes	Yes
NIC/CNA	Yes	Yes	Yes	Yes
RAID	Yes	Yes	Yes	Yes
FC	Yes	No	Yes	Yes
Windows	Yes	—	No	—
RHEL	Yes	—	No	—
ESXI	Yes	—	No	—
Management Module	Yes	Yes	Yes	Yes
PSU	No	No	No	No
Storage	No	No	No	No
Input/Output	No	No	No	No
Network Input/Output	No	No	No	No

Topics:

- [Predefined Operational Templates](#)
- [Creating Operational Template from reference servers](#)
- [Creating Operational Template from reference Modular Systems](#)
- [Viewing Operational Template](#)
- [Modifying Operational Template](#)
- [Deleting Operational Template](#)
- [Assigning Operational Template and running Operational Template compliance for servers](#)

- [Deploying Operational Template on servers](#)
- [Assigning Operational Template for Modular Systems](#)
- [Deploying Operational Template for Modular System](#)
- [Unassigning Operational Template](#)

Predefined Operational Templates

Predefined templates have all the configurations that are required to create Storage Spaces Direct clusters or Windows Server Software-Defined (WSSD). OMIMSSC supports creating clusters on R740XD and R640 Storage Spaces Direct Ready Node models along with their specific network adapters.

Table 3. List of predefined Operational Templates

Operational Template name	Description
R740XD_Mellanox_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having Mellanox card.
R740XD_QLogic_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having QLogic card.
R640_Mellanox_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having Mellanox card.
R640_QLogic_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having QLogic card.

Consider the following points before deploying an Operational Template:

- The predefined templates are available only for management systems running SC2016 VMM.
- The predefined Storage Spaces Direct template shows NIC card in slot 1. However, while deploying the Operational Template the NIC configuration is applied on the right slot. And if there are multiple NIC cards on the device, all the NIC cards are configured with the same configuration that is specified in the Operational Template.

Creating Operational Template from reference servers

Prerequisites

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a reference server by using the **Discovery** feature. For information about discovering servers, see [Discovering servers using manual discovery](#).
- For SCCM users:
 - Create a task sequence. For more information, see [Creating task sequence](#).
 - For non-Windows operating system deployment, have a device type credential profile. For more information, see [Creating credential profile](#).
- For SCVMM users:
 - Create a hypervisor profile. For information about creating hypervisor profile, see [Creating hypervisor profile](#).
 - For Windows deployment, have a device type credential profile. For more information, see [Creating credential profile](#).
- If you are not using the default update source, and then create an update source. For more information, see [Creating update source](#).

About this task

You can create an Operational Template by capturing the configuration of the reference server. After capturing the configuration, you can directly save the template, or edit the attributes for update source, hardware configuration, and Windows component as per your requirement. Now you can save the template, which can be used on PowerEdge homogeneous servers.

Steps

- 1 In OMIMSSC, do any of the following to open an Operational Template:

- In the OMIMSSC dashboard, click **Create Operational Template**.
- In the navigation pane, click **Profiles > Operational Template**, and then click **Create**.

The **Operational Template** wizard is displayed.

- 2 Enter a name and description for the template.
- 3 Select the type of device, and enter the IP address of reference device, and then click **Next**.

NOTE: You can capture the configuration of reference server with iDRAC 2.0 and later.

- 4 In **Device Components**, click a component to view the available attributes and their values.

The components are as follows:

- Firmware update
- Hardware components, which are RAID, NIC, and BIOS.

NOTE: In iDRAC Embedded 1 component, following are the privileges and their values for User Admin Privilege attribute.

Table 4. Privilege value table

Value	Privilege
1	Login
2	Configure
4	Configure Users
8	Logs
16	System Control
32	Access Virtual Console
64	Access Virtual Media
128	System Operations
256	Debug
499	Operator Privileges

- Operating system—select either Windows, or ESXi, or RHEL.

- 5 Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
- 6 Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.

NOTE: Irrespective of the selection made in the check box against each component, all the configurations are captured in the template.

In **Operating System** component, perform the steps in either of the following options, as per your requirement:

- For Windows operating system deployment on SCCM, see [Windows component for the OMIMSSC console extension for SCCM](#).
- For Windows operating system deployment on SCVMM, see [Windows component for the OMIMSSC console extension for SCVMM](#).
- OMIMSSC
- For non-Windows operating system deployment, see [Non-Windows component for the OMIMSSC console extensions](#).

- 7 To save the profile, click **Finish**.

Windows OS component for OMIMSSC console extension for SCCM

About this task

While creating or editing Operational Template for server, perform the following steps for windows component:

Steps

- 1 Select a task sequence and deployment method.

NOTE: Only the task sequences deployed on collections are listed in the drop-down menu.

For information about task sequence, see [Task sequence](#).

- 2 Select one of the following options for the **Deployment method**:
 - **Boot to network ISO**—reboots specified ISO.
 - **Stage ISO to vFlash and Reboot**—downloads the ISO to vFlash and reboots.
 - **Reboot to vFlash**—reboots to vFlash. Ensure that the ISO is present in the vFlash.

NOTE: To use the Reboot to vFlash option, the label name of the partition that is created on vFlash must be ISOIMG.

- 3 (Optional) To use the image present in the network share, select the **Use Network ISO as Fallback** option.
- 4 enter an LC boot media image file.
- 5 Select the drivers required for the operating system.

Windows component for OMIMSSC console extension for SCVMM

About this task

While creating or editing Operational Template for server, perform the following steps for windows component:

Step

Select **Hypervisor Profile**, **Credential Profile**, and **Server IP** from.

NOTE: Host Name, and Server Management NIC are always pool values.

If you select **Server IP** from as **Static**, and then ensure that you have configured the logical network in SCVMM, and the following fields are pool values:

- **Console Logical Network**
- **IP Subnet**
- **Static IP Address**

Non-Windows component for OMIMSSC console extensions

About this task

While creating or editing Operational Template for server, perform the following steps for non-windows component:

Step

Select a non-windows operating system, operating system version, type of share folder, ISO file name, location of the ISO file and the password for the root account of the operating system.

(Optional) Select a Windows type credential profile for accessing the CIFS share.

Host name is a pool value and if you disable DHCP option, and then the following fields are pool values:

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- Secondary DNS

NOTE: Network File System (NFS) and Common Internet File System (CIFS) share types are supported for non-Windows operating system deployment.

Creating Operational Template from reference Modular Systems

Prerequisites

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a Modular System by using the **Discovery** feature. For information about discovering Modular Systems, see [Discovering Modular System using manual discovery](#).
- If you are not using the default update source, and then create an update source. For more information, see [Creating update source](#).

About this task

You can create an Operational Template by capturing the configuration of the reference Modular Systems. After capturing the configuration, you can directly save the template, or edit the attributes for update source and hardware configuration as per your requirement. Now you can save the template, that can be used to configure other Modular Systems of the same model.

NOTE: If you want to configure Active Directory (AD) users on other MX7000 devices ensure that you create an Operational Template from an MX7000 Modular System where all the AD users are configured.

NOTE: User account's passwords are not captured in Operational Template, from reference Modular System for security reasons. Edit the Operational Template to add a new user account and password, and then apply the Operational Template on the managed Modular Systems. Else, you can apply the Operational Template without any changes to user accounts, and the same passwords that are used in the reference Modular System are applied on the managed Modular System.

Steps

- 1 In OMIMSSC, do any of the following to open an Operational Template:
 - In the OMIMSSC dashboard, click **Create Operational Template**.
 - In the navigation pane, click **Profiles > Operational Template**, and then click **Create**.

The **Operational Template** wizard is displayed.

- 2 Enter a name and description for the template.
- 3 In **Device Components**, click a component to view the available attributes and their values.

The components are as follows:

- Firmware update
- Management Module Embedded

NOTE: Ensure that the Web Server attribute is enabled. If this component is not enabled, and then the MX7000 Modular Systems cannot be accessed through OMIMSSC after deploying the Operational Template.

NOTE: For SNMP Configuration and Syslog Configuration, ensure that you select all four configurations available in each attribute, to apply them on managed devices.

- 4 Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
- 5 Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.
- 6 To save the profile, click **Finish**.

Viewing Operational Template

To view Operational Templates created:

In OMIMSSC console, click **Profiles and Templates**, and then click **Operational Template**. All the templates that are created are listed here.

Modifying Operational Template

About this task

You can modify the update source, hardware configurations, and operating system of an operational template.

Consider the following before modifying an Operational Template:

- The values of few attributes depend on the values of other attributes. When you change attribute values manually, ensure that you also change the interdependent attributes. If these interdependent values are not changed appropriately, and then applying the hardware configurations may fail. Hence, Dell EMC recommends that you do not edit these configurations that are captured in an Operational Template.
- The step to modify predefined Operational Templates and custom created Operational Templates are the same.
- (For SCCM users and servers only) When editing a task sequence on SCCM 2016, the **missing objects references** messages do not list the **Setup windows and ConfigMgr** package. Hence, you must add the package and then save the task sequence.
- (For SCVMM users and servers only) All the Storage Spaces Direct specific attributes are read-only attributes in the predefined Storage Spaces Direct template. However, you can edit the name of the template, operating system components, and hardware configurations.

NOTE: The steps to modify any Operational Template are the same.

Steps

- 1 Select the template that you want to modify and click **Edit**.

The Operational Template page is displayed.

- 2 (Optional) Edit the name and description of the template, and then click **Next**.
- 3 To view the available attributes and their values in **Device Components**, click a component.
- 4 Modify the values of the available attributes.

NOTE: Select the check box against each component since only the selected component's configurations are applied on the managed system, when the Operational Template is applied.

NOTE: When editing Operational Template, few Advanced Host Controller Interface (AHCI) component attributes that are read-only are listed as editable. However, when these read-only attributes are set and the Operational Template is deployed, there are no changes that are made to the device.

- For MX7000 Modular Systems:
 - Configurations are applied only if all the attributes for a group are selected. Hence, ensure that you select all the attributes in a group, even if you want to change one of the attributes in the group.
 - To add a new user through an Operational Template, select all the attributes of existing users that were exported when capturing the Operational Template, select the recently added user groups, and save the Operational Template.
 - To provide the time zone values, see [Appendix](#).
- 5 For the operating system component, perform either of the following tasks depending on your requirement:
 - For Windows operating system deployment on SCCM, see [Windows component for the OMIMSSC console extension for SCCM](#).
 - For Windows operating system deployment on SCVMM, see [Windows component for the OMIMSSC console extension for SCVMM](#).
 - OMIMSSC
 - For non-Windows operating system deployment, see [Non-Windows component for the OMIMSSC console extensions](#).
 - 6 To save the profile, click **Finish**.

Deleting Operational Template

To delete an Operational Template, perform the following steps:

About this task

Before deleting an Operational Template, ensure that:

- The selected Operational Template is not associated with any server or Modular System. If it is associated with a device, and then, unassign the template and then delete the template.
- No jobs that are associated with Operational Template are running.
- You have not selected a predefined Operational Template, since you cannot delete a predefined template.
- The steps to delete any type of Operational Template are the same.

Step

Select the templates that you want to delete and click **Delete**. To confirm, click **Yes**.

Assigning Operational Template and running Operational Template compliance for servers

Assign an Operational Template to a server, and run the Operational Template compliance. Only after assigning an Operational Template to a server, you can view its Operational Template compliance status. You can compare a server's configuration with an Operational Template by assigning the template to a server. Once you assign an Operational Template, the compliance job runs and the Operational Template status is displayed on completion.

About this task

To assign an Operational Template, perform the following steps:

Steps

- 1 In OMIMSSC click **Configuration and Deployment**, and then click **Server View**. Select the required servers and click **Assign Operational Template and Run Compliance**.

The **Assign Operational Template and Run Compliance** page is displayed.

- 2 Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

The Operational Template drop-down lists templates, of the same type as that of the devices selected in the previous step.

If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

To view a detailed report, perform the following steps:

- a Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.
 - Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.
 - Red color box—represents that the component is not present on the device.

Deploying Operational Template on servers

Prerequisite

For deploying operating system on managed servers, ensure that you have the 4093492 KB article or later installed on your management system and on the operating system image that is used for deployment.

About this task

You can deploy Windows and non-Windows operating system—ESXi and RHEL by deploying the Operational Template assigned to servers.

NOTE: Download and install appropriate drivers from Dell.com/support if a yellow bang is displayed under Device Manager after you deploy Windows 2016 operating system on 12th generation of the servers.

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and click **Server View**. Select the servers on which you want to deploy a template on, and then click **Deploy Operational Template**.

The **Deploy Operational Template** page is displayed.

- 2 (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.

NOTE: Before exporting the pool values, add the IP address of the OMIMSSC Appliance where the OMIMSSC console extension is installed, to the local intranet site. For more information about adding the IP address in IE browser, see *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

- 3 If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.

The format of a .CSV file is `attribute-value-pool.csv`

NOTE: Ensure that you select a .CSV file which has all proper attributes and the iDRAC IP or iDRAC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the iDRAC IP or iDRAC credentials changes and is marked as failed though the job may be successful in iDRAC.

- 4 Enter a unique job name, description for the job, and click **Deploy**.

To track this job, the **Go to the Job List** option is selected by default.

Assigning Operational Template for Modular Systems

Assign an Operational Template to a Modular System and run the Operational Template compliance. This operation compares the configuration of a Modular System and an Operational Template by assigning the selected template to a Modular System. After you assign an Operational Template, the compliance job runs and the compliance status is displayed on completion.

About this task

To assign an Operational Template for Modular Systems, perform the following steps:

Steps

- 1 In OMIMSSC click **Configuration and Deployment**, and click **Modular Systems View**. Select the required Modular System and click **Assign Operational Template**.

The **Assign Operational Template** page is displayed.

- 2 Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

NOTE: The Operational Template compliance status excludes any changes that are made to user attributes.

If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

To view a detailed report, perform the following steps:

- a Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.

- Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.
- Red color box—represents that the component is not present on the device.

Deploying Operational Template for Modular System

About this task

You can configure Modular System components, and update the Modular System firmware versions by deploying the assigned Operational Template.

NOTE: In a Multi-Chassis Management (MCM), if lead chassis is configured with Propagation to member chassis, and then configuring and updating lead chassis and member chassis from OMIMSSC will override the changes done through propagation.

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and click **Modular Systems View**. Select the Modular System on which you have assigned the template, and then click **Deploy Operational Template**.
The **Deploy Operational Template** page is displayed.
- 2 (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.
- 3 If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.
The format of a .CSV file is `attribute-value-pool.csv`

NOTE: Ensure that you select a .CSV file which has all proper attributes and the CMC IP or CMC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the CMC IP or CMC credentials changes.

- 4 Enter a unique job name, description for the job, and click **Deploy**.

NOTE: There are no supported system-specific pool value attributes for Modular System. Hence, there are no pool values to be exported.

To track this job, the **Go to the Job List** option is selected by default.

Unassigning Operational Template

- 1 In OMIMSSC, perform any one of the following tasks:
 - Click **Configuration and Deployment**, and click **Server View**.
 - Click **Configuration and Deployment**, and click **Modular System View**.

Select the required devices and click **Assign Operational Template and Run Compliance**.

The **Assign Operational Template and Run Compliance** page is displayed.

- 2 Select **Unassign** from **Operational Template** drop-down menu, and click **Assign**.
Operational Template is unassigned to selected devices.

Firmware update in OMIMSSC

Maintain Dell EMC devices up-to-date by upgrading to the latest firmware to use security, issue fixes, and enhancements, using OMIMSSC. Update the firmware of devices using Dell EMC update repositories.

Updating firmware is supported only on hardware compatible devices. For using the features available in OMIMSSC on the managed devices, the managed devices must have the minimum required firmware versions of iDRAC, Lifecycle Controller (LC), and BIOS. Devices having the required firmware versions are hardware compatible.

Topics:

- [About update groups](#)
- [About update sources](#)
- [Integration with Dell EMC Repository Manager\(DRM\)](#)
- [Setting polling frequency](#)
- [Viewing and refreshing device inventory](#)
- [Applying filters](#)
- [Upgrading and downgrading firmware versions using run update method](#)

About update groups

Update groups are a group of devices that require similar update management. There are two types of update groups that are supported in OMIMSSC:

- **Predefined update groups**—You cannot manually create, modify, or delete the predefined update groups.
- **Custom update groups**—You can create modify and delete devices in these groups.

NOTE: All server groups that exist in SCVMM are listed in OMIMSSC. However, the list of servers in OMIMSSC is not user-specific. Therefore, ensure that you have access to perform any operations on those devices.

Predefined update groups

After discovering a device, the discovered device is added to one of the following predefined groups.

- **Default host groups**—this group consists of servers that are deployed with Windows operating system or are synchronized with a registered Microsoft console.
- **Default unassigned groups**—this group consists of unassigned or bare-metal servers discovered.
- **Default non-windows host groups**—this group consists of servers that are deployed with non-windows operating systems.
- **Chassis update groups**—this group consists of modular servers and chassis or Modular Systems. 12th generation of servers and later are discovered along with their chassis information. By default, a group is created with the following name format, **Chassis-Service-tag-of-Chassis-Group**. For example, **Chassis-GJDC4BS-Group**. If a modular server is deleted from a cluster update group, and then the server is added to the chassis update group along with its CMC information. Even if there are no modular servers in the corresponding chassis update group, since all modular servers in the chassis are in a cluster update group, the chassis update group continues to exist, but displays only the CMC information.
- **Cluster update groups**—this group consists of **Windows Server Failover clusters**. If a 12th generation and later modular server is part of cluster, and then the CMC information is also added in the inventory in the **Maintenance Center** page.

Custom update groups

Create custom update groups of type **Generic update groups** by adding the discovered devices into groups that require similar management. However, you can add a device into a custom update group only from **Default unassigned update groups** and **Default host update groups**. To add the servers in custom update group, search for the required device using their service tag. After you add a device into a custom update group, the device is removed from the predefined update group and is available, only in the custom update group.

Viewing update groups

To view update groups:

- 1 In **OMIMSSC**, click **Maintenance Center** and then click **Maintenance Settings**.
- 2 In **Maintenance Settings**, click **Update Groups**.
All the custom groups created are displayed with name, group type, and number of servers in the group.

Creating custom update groups

- 1 In OMIMSSC console, click **Maintenance Center**, and then click **Maintenance Settings**.
- 2 In **Maintenance Settings**, click **Update Groups**, and then click **Create**.
The **Firmware Update Group** page is displayed.
- 3 Provide a group name, description, and select the type of update group that you want to create.
Custom update groups can have servers only from the following update group types:
 - Generic update group—consists servers from default unassigned update groups and default host update groups.
 - Host update group—consists servers from default host update groups.
Also, you can have a combination of servers from the two types of server groups.
- 4 To add servers in the update group, search for the servers by using their service tag, and to add servers into the **Servers Included in the Update Group** table, click the right arrow.
- 5 To create the custom update group, click **Save**.

Modifying custom update groups

About this task

Consider the following points when you are modifying a custom update group:

- You cannot change the type of an update group after it is created.
- To move servers from one custom update group to another custom update group, you can:
 - a Remove the server from an existing custom update group. It is then automatically added into the predefined update group.
 - b Edit the custom group to add the server into, and then search for the server by using the service tag.

Steps

- 1 In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
- 2 In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Edit** to modify the update group.

Deleting custom update groups

About this task

Consider the following points when you are deleting a custom update group in the following circumstances:

- You cannot delete an update group if it has a job that is scheduled, in-progress, or waiting. Hence, delete the scheduled jobs that are associated with a custom update group before deleting the server group.
- You can delete an update group even if servers are present in that update group. However, after deleting such an update group, the servers are moved to their respective predefined update groups.
- If a device that is present in custom update group, is deleted from MSSC, and you synchronize OMIMSSC with enrolled MSSC, the device is removed from the custom update group and is moved to the appropriate predefined group.

Steps

- 1 In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
- 2 In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Delete** to delete the update group.

About update sources

Update sources have reference to the catalog files that contain Dell EMC updates (BIOS, driver packs such as management components, network cards) and carry the self-contained executable file called Dell Update Packages (DUPs).

You can create an update source or a repository, and set it as a default update source for generating a comparison report, and receiving alerts when new catalog files are available at the repository.

Using OMIMSSC, you can keep the devices firmware up-to-date using online or offline update sources.

Online update sources are repositories that are maintained by Dell EMC.

Offline update sources are local repositories and used when there is no Internet connection.

It is recommended that you create custom repositories and place the network share in the local intranet of OMIMSSC Appliance. This would save the Internet bandwidth and also provide a secure internal repository.

Update firmware using one of the following update sources:

- **DRM repository**—is an offline repository. Export the inventory information of discovered devices from OMIMSSC Appliance to prepare a repository in DRM. For information about integration with DRM, and creating an update source through DRM, see [Integration with DRM](#). After creating a repository in DRM, in OMIMSSC, select the update source that is created through DRM, relevant devices, and initiate an update on the devices. For information about DRM, see *Dell Repository Manager* documents available at dell.com/support.
- **FTP, HTTP, or HTTPS**—can be an online or offline repository. Update specific components of devices with respect to the latest update provided on FTP, HTTP, or HTTPS site. Dell EMC prepares a repository at every two months cadence and publishes the following updates through PDK catalogs:
 - Server BIOS and firmware
 - Dell EMC certified operating system driver packs—for operating system deployment

NOTE: If you select an online update source, while deploying the Operational Template, the latest firmware versions are downloaded and applied on the managed devices. Hence, the firmware versions might differ between reference and deployed device.

- **Reference firmware inventory and comparison**—can be converted to an offline repository through DRM. Create a reference inventory file that contains the firmware inventory of the selected devices. The reference inventory file can contain inventory information of a device of the same type or model, or can have multiple devices of different types or models. You can compare the inventory information of devices present in OMIMSSC against the saved reference inventory file. To pass the exported file to DRM and create a repository, see *Dell Repository Manager* documents available at dell.com/support.

Predefined and default update source

OMIMSSC includes three predefined update sources that are available after a fresh installation, or upgrade. **DELL ONLINE FTP CATALOG** is a predefined update source of type FTP, **DELL ONLINE HTTP CATALOG** is a predefined update source of type HTTP, and **DELL ONLINE HTTPS CATALOG** is a predefined default update source of type HTTPS. However, you can create another update source and mark it as a default update source.

 **NOTE:** If you are using proxy server, to access the repository, edit the update source to add the proxy details and save the changes.

Predefined and default update sources for Storage Spaces Direct clusters

OMIMSSC supports updating Storage Spaces Direct clusters through specific predefined update sources. These update sources have reference to catalog files that contain latest and recommended firmware versions of components for Storage Spaces Direct clusters. They are listed only on **Maintenance Center** page.

DELL ONLINE FTP S2D CATALOG is a predefined update source of type FTP, and is part of **DELL ONLINE FTP CATALOG**.

DELL ONLINE HTTP S2D CATALOG is a predefined update source of type HTTP, and is part of **DELL ONLINE HTTP CATALOG**.

DELL ONLINE HTTPS S2D CATALOG is a predefined default update source of type HTTPS, and is part of **DELL ONLINE HTTPS CATALOG**.

Predefined and default update sources for Modular Systems

OMIMSSC supports updating Modular Systems through specific predefined update sources. These update sources have reference to catalog files that contain latest and recommended firmware versions of components for Modular Systems. They are listed only on **Maintenance Center** page.

DELL ONLINE FTP MX7000 CATALOG is a predefined update source of type FTP, and is part of **DELL ONLINE FTP CATALOG**.

DELL ONLINE HTTP MX7000 CATALOG is a predefined update source of type HTTP, and is part of **DELL ONLINE HTTP CATALOG**.

DELL ONLINE HTTPS MX7000 CATALOG is a predefined default update source of type HTTPS, and is part of **DELL ONLINE HTTPS CATALOG**.

Validating data using test connection

To verify if the location of the update source is reachable by using the credentials that are mentioned while creating the update source, use **Test Connection**. Only after the connection is successful, you are enabled to create an update source.

Setting up local FTP

To set up local FTP:

- 1 Create a folder structure in your local FTP that is an exact replica of the online FTP, **ftp.dell.com**.
- 2 Download the **catalog.gz** file from online FTP and unzip the files.

- 3 Open the **catalog.xml** file and change the **baseLocation** to your local FTP URL, and compress the file with **.gz** extension.
For example, change the **baseLocation** from **ftp.dell.com** to **ftp.yourdomain.com**.
- 4 Place the catalog file and the DUP files in your local FTP folder replicating the same structure as in **ftp.dell.com**.

Setting up local HTTP

About this task

To set up local HTTP:

Steps

- 1 Create a folder structure in your local HTTP that is an exact replica of **downloads.dell.com**.
- 2 Download the **catalog.gz** file from the online HTTP which is from the following location: **http://downloads.dell.com/catalog/catalog.xml.gz** and extract the files.
- 3 Extract the **catalog.xml** file and change the **baseLocation** to your local HTTP URL, and compress the file with **.gz** extension.
For example, change the **baseLocation** from **downloads.dell.com** to host name or IP address such as **hostname.com**.
- 4 Place the catalog file with the modified catalog file, and the DUP files in your local HTTP folder replicating the same structure in **downloads.dell.com**.

Setting up local HTTPS

About this task

To set up local HTTPS:

Steps

- 1 Create a folder structure in your local HTTPS that is an exact replica of **downloads.dell.com**.
- 2 Download the **catalog.gz** file from the online HTTPS which is from the following location: **https://downloads.dell.com/catalog/catalog.xml.gz** and extract the files.
- 3 Extract the **catalog.xml** file and change the **baseLocation** to your local HTTPS URL, and compress the file with **.gz** extension.
For example, change the **baseLocation** from **downloads.dell.com** to host name or IP address such as **hostname.com**.
- 4 Place the catalog file with the modified catalog file, and the DUP files in your local HTTPS folder replicating the same structure in **downloads.dell.com**.

Viewing update source

- 1 In **OMIMSSC**, click **Maintenance Center**.
- 2 In **Maintenance Center**, click **Maintenance Settings**, and then click **Update Source**.
All the update sources created along with their description, source type, location, and credential profile name are displayed.

Creating update source

Prerequisites

- Based on the update source type, ensure that a Windows or an FTP credential profile is available.
- Ensure that you install and configure DRM having Administrator roles, if you are creating a DRM update source.

Steps

- 1 In the OMIMSSC console, click **Maintenance Center** and then click **Maintenance Settings**.
- 2 In the **Update Source** page, click **Create New** and provide the update source name and description.
- 3 Select any of the following types of update source from the **Source Type** drop-down menu:

- FTP Sources—select to create an online or local FTP update source.

NOTE: If you are creating an FTP source, provide your FTP credentials along with proxy credentials if the FTP site is reachable by using proxy credentials.

- HTTP Sources—select to create an online or local HTTP update source.

NOTE: If you are creating an update source of type HTTP, provide the complete path of catalog with the catalog name and your proxy credentials to access the update source.

- HTTPS Sources—select to create an online HTTPS update source.

NOTE: If you are creating an update source of type HTTPS, provide the complete path of catalog with the catalog name and your proxy credentials to access the update source.

DRM Repository—select to create a local repository update source. Ensure that you have installed DRM.

NOTE: If you are creating a DRM source, provide your Windows credentials and ensure that the Windows shared location is accessible. In the location field, provide the complete path of the catalog file with the file name.

- Inventory Output files—select to view the firmware inventory against reference server configuration.

NOTE: You can view a comparison report by using Inventory Output files as an update source. The reference server's inventory information is compared against all other servers that are discovered in OMIMSSC.

- In **Location**, provide the URL of the update source of an FTP or HTTP or HTTPS source and the Windows shared location for DRM.

NOTE: The local FTP site must replicate the online FTP.

NOTE: The local HTTP site must replicate the online HTTP.

NOTE: Providing HTTP or HTTPS in the URL for an FTP source is not mandatory.

- To access the update source, select the required credential profile in **Credentials**.

- In **Proxy Credentials**, select the appropriate proxy credentials if proxy is required to access the FTP or HTTP source.

- (Optional) To make the created update source as a default update source, select **Make this as default source**.

- To verify that the location of the update source is reachable by using the mentioned credentials, click **Test Connection**, and then click **Save**.

NOTE: You can create the update source only after the test connection is successful.

Modifying update source

About this task

Consider the following points before, modifying an update source:

- To edit **DELL ONLINE FTP S2D CATALOG**, **DELL ONLINE HTTP S2D CATALOG**, or **DELL ONLINE HTTPS S2D CATALOG** update source, edit the respective predefined update source, and save the changes. This update reflects in **DELL ONLINE FTP S2D CATALOG**, **DELL ONLINE HTTP S2D CATALOG**, or **DELL ONLINE HTTPS S2D CATALOG** update source.
- You cannot change the type of an update source and the location after the update source is created.
- You can modify an update source even if the update source is in use by an in-progress or a scheduled job, or if it is used in a deployment template. A warning message is displayed while modifying the in-use update source. Click **Confirm** to go to the changes.
- When a catalog file is updated in the update source, the locally cached catalog file is not automatically updated. To update the catalog file saved in cache, edit the update source or delete and re-create the update source.

Step

Select the update source that you want to modify, click **Edit**, and then update the source as required.

Deleting update source

About this task

Consider the following points before, deleting an update source:

- You cannot delete a predefined update source.
- You cannot delete an update source if it is used in an in-progress, or a scheduled job.
- You cannot delete an update source if it is a default update source.

Step

Select the update source that you want to delete, and click **Delete**.

Integration with Dell EMC Repository Manager(DRM)

OMIMSSC is integrated with DRM to create custom update sources in OMIMSSC. The integration is available from DRM version 2.2 onwards. Provide the discovered device information from OMIMSSC Appliance to DRM, and using the available inventory information, you can create a custom repository in DRM and set it as an update source in OMIMSSC for performing firmware updates and creating clusters on managed devices. For more information about creating a repository in DRM, see *Dell EMC Repository Manager* documents available at Dell.com/support/home.

Integrating DRM with OMIMSSC

About this task

- ① **NOTE:** Consider factors such as testing on test environment, security updates, application recommendations, Dell EMC advisories, to prepare the required updates.
- ① **NOTE:** To view the latest inventory information about discovered devices, after upgrading OMIMSSC, reintegrate DRM with OMIMSSC Appliance.

Steps

- 1 Launch the **Dell Repository Manager Data Center** version.
- 2 Click **My Repositories**, click **New**, and then click **Dell OpenManage Essentials (OME) inventory**.
- 3 Enter the **URL (Rest API)** in the following format: `https:// IP address of appliance/genericconsolerepository/` and then click **Next**.
- 4 Provide the user name and password of OMIMSSC Appliance, click **OK**. To confirm your selection, click **OK**.

Next step

After integrating DRM with OMIMSSC, see *Obtain firmware catalog for Storage Spaces Direct Ready Nodes Using Dell Repository Manager* section from *Dell EMC Microsoft Storage Spaces Direct Ready Node Operations Guide* for managing and monitoring Ready Node life cycle at dell.com/support

Setting polling frequency

Configure polling and notifications, to receive alerts when there is a new catalog file available at the update source, that is selected as default. OMIMSSC Appliance saves a local cache of the update source. The color of the notification bell changes to orange color when there is a new catalog file available at the update source. To replace the locally cached catalog available in OMIMSSC Appliance, click the bell icon. After replacing the old catalog file with the latest catalog file, the bell color changes to green.

About this task

To set the polling frequency:

Steps

- 1 In OMIMSSC, click **Maintenance Center**, and then click **Polling and Notification**.
- 2 Select how frequently the polling should happen:
 - **Never**—this option is selected by default. Select to never receive any updates.
 - **Once a week**—select to receive updates about new catalogs available at update source on a weekly basis.
 - **Once every 2 weeks**—select to receive updates about new catalogs available at update source once every two weeks.
 - **Once a month**—select to receive updates about new catalogs available at update source on a monthly basis.

Viewing and refreshing device inventory

View comparison report for devices against an update source in **Maintenance Center** page. On selecting an update source, a report is displayed comparing existing firmware to the firmware present in the selected update source. The report is generated dynamically on changing the update source. Server inventory is compared with update source, and suggestive actions are listed. This activity takes considerable time based on the number of devices and device components present. You cannot perform other tasks during this process. Refreshing inventory refreshes the entire device's inventory even though you select a single component in that device.

About this task

Sometimes, the inventory of the device is updated, but the page does not display the latest inventory. Hence, use the refresh option to view the latest inventory information of the discovered devices.

- NOTE:** 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, Dell HTTP, or Dell HTTPS update source cannot download the catalog file. Hence, the comparison report is not available. To view a comparison report for the default update source, edit the default Dell online FTP, the Dell HTTP, or the Dell HTTPS update source, (provide the proxy credentials if required), and then select the same from the Select Update Source drop-down menu. For more information about editing an update source, see [Modifying update source](#).
- NOTE:** A local copy of the catalog file is in OMIMSSC when the product is delivered. Therefore, the latest comparison report is not available. To view the latest comparison report, update the catalog file. To update the catalog file, edit the update source and save it, or delete and re-create an update source.
- NOTE:** In SCCM, even after refreshing the inventory information, server details such as Driver Pack Version, and Drivers Available For operating system, are not updated in Dell Out of Band Controllers (OOB) properties page. To update the OOB properties, synchronize OMIMSSC with the enrolled SCCM.
- NOTE:** When you upgrade OMIMSSC, information about servers that are discovered in prior versions are not displayed. For the latest server information and correct comparison report, rediscover the servers.

To refresh and view firmware inventory of discovered devices:

Steps

- 1 In **OMIMSSC**, click **Maintenance Center**.
The **Maintenance Center** page is displayed with a comparison report for all the devices that are discovered in OMIMSSC against the selected update source.
- 2 (Optional) To view a comparison report only for specific group of devices, select only the required devices.
- 3 (Optional) To view a comparison report, for another update source, change the update source by selecting an update source from **Select Update Source** drop-down list.
- 4 To view firmware information of device components such as current version, baseline version, and the update actions that are recommended by Dell EMC, expand the server group from **Device Group/Servers** to the server level, and then to the component level. Also, view the number of recommended updates for devices. Hover your cursor on the available updates icon to see the corresponding details of updates, such as number of critical updates, recommended updates.

The available updates icon indicator color is based on overall criticality of the updates and following are the critical update categories:

- The color is red even if there is a single critical update in the server or server group.
- The color is yellow if there are no critical updates.
- The color is green if the firmware versions are up-to-date.

Following update actions are suggested after populating the comparison report:

- Downgrade—an earlier version is available, and you can downgrade the existing firmware to this version.
- No Action Required—existing firmware is same as the one in update source.
- No Update Available—updates are not available for this component.

- NOTE:** There are no updates available for Power Supply Unit (PSU) components for MX7000 Modular Systems and servers in online catalogs. In case you want to update the PSU component for MX7000 Modular System, see *Updating Power Supply Unit component for Dell EMC PowerEdge MX7000 devices*. For updating PSU component for servers, contact Dell EMC support.

- Upgrade - Optional—updates are optional, and they consist of new features or any specific configuration upgrades.

- Upgrade - Urgent—updates are critical, and used for resolving security, performance, or break-fix situations in components such as BIOS.
- Upgrade - Recommended—updates are issue fixes, or any feature enhancements for components. Also, compatibility fixes with other firmware updates are included.

Consider the following points for NIC-related information for the 11th generation of servers:

- After applying filters based on **Nature of Update** as **Urgent**, a report with the components only with urgent updates are displayed. If this report is exported, and then components with downgrade action which in turn have critical update is also exported.
- When there are multiple network interfaces available in a single NIC card, there is only one entry for all the interfaces in the **Component Information** list. After the firmware updates are applied, all the NIC cards are upgraded.
- When a NIC card is added along with the existing cards, the newly added NIC card is listed as another instance in the **Component Information** list. After the firmware updates are applied, all the NIC cards are upgraded.

Applying filters

Apply filters to view selected information in the comparison report.

About this task

Filter the comparison report based on available server components. OMIMSSC supports three categories of filters:

- **Nature Of Update**—select to filter and view only the selected type of updates on servers.
- **Component Type** —select to filter and view only the selected components on servers.
- **Server Model** —select to filter and view only the selected server models.

NOTE: You cannot export and import server profiles if the filters are applied.

To apply the filters:

Step

In OMIMSSC, click **Maintenance Center**, click the filters drop-down menu, and then select the filters.

Removing filters

About this task

To remove filters:

Step

In OMIMSSC, click **Maintenance Center**, and then click **Clear Filters**, or clear the selected check boxes.

Upgrading and downgrading firmware versions using run update method

Prerequisites

Before applying updates on devices, ensure that the following conditions are met:

- An update source is available.

NOTE: Select Storage Spaces Direct update source or MX7000 update sources, for applying firmware updates on Storage Spaces Direct clusters or MX7000 Modular Systems since, these update sources see a modified reference to catalog that contains recommended firmware versions of components for Storage Spaces Direct clusters and Modular Systems.

- iDRAC or Management Module (MM) job queue is cleared before applying the updates, on the managed devices.

About this task

Apply updates on selected device groups which are hardware compatible with OMIMSSC. Updates can be applied immediately, or scheduled. The jobs that are created for firmware updates are listed under the **Jobs and Logs Center** page.

Consider the following points before upgrading or downgrading firmware:


- When you start this task, the task takes considerable time based on the number of devices and device components present.
- You can apply firmware updates on a single component of a device, or to the entire environment.
- If there are no applicable upgrades or downgrades for a device, performing a firmware update on the devices cause no action on the devices.
- For updating chassis, see *Updating CMC firmware* section in *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide*.
 - For updating chassis firmware in VRTX, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide*.
 - For updating chassis firmware in FX2, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide*.


Steps

- 1 In OMIMSSC, click **Maintenance Center**, select the servers or Modular System groups, and an update source, and then click **Run Update**.
- 2 In **Update Details**, provide the firmware update job name and description.
- 3 To enable downgrading the firmware versions, select the **Allow Downgrade** check-box.
If this option is not selected, and then there is no action on the component that requires a firmware downgrade.
- 4 In **Schedule Update**, select one of the following:
 - **Run Now**—select to apply the updates immediately.
 - Select a date and time to schedule a firmware update in future.
- 5 Select any one of the following methods, and click **Finish**.
 - **Agent-free staged updates**—updates that are applicable without a system restart are applied immediately, and the updates that require a restart are applied when the system restarts. To check if all the updates are applied, refresh the inventory. The entire update job fails, if the operation fails on even one device.

 **NOTE:** OMIMSSC supports only Agent-free staged updates for MX7000 Modular Systems.

- **Agent-free updates**—updates are applied and the system restarts immediately.

 **NOTE:** Cluster-Aware Updating (CAU)—automates the update process by using Windows CAU feature on cluster update groups to maintain server's availability. Updates are passed to cluster update coordinator that is present on the same system where the SCVMM server is installed. The update process is automated to maintain server's availability. The update job is submitted to Microsoft Cluster-Aware-Update (CAU) feature, irrespective of the selection made from the Update Method drop-down menu. For more information, see [Updates using CAU](#).

 **NOTE:** After submitting a firmware update job to iDRAC, OMIMSSC interacts with iDRAC for the status of the job and displays it in the Jobs and Logs page in the OMIMSSC Admin Portal. If there is no response from iDRAC about the status of the job for a long time, and then the status of the job is marked as failed.

Updates using CAU

Updates on servers (that are part of cluster) happen through cluster update coordinator which is present on the same system where SCVMM server is installed. The updates are not staged and are applied immediately. Using Cluster Aware Update (CAU), you can minimize any disruption or server downtime enabling continuous availability of the workload. Hence, there is no impact to the service provided by the cluster group. For more information about CAU, see Cluster-Aware Updating Overview section at technet.microsoft.com.

Before applying the updates on cluster update groups, verify the following:

- Ensure that the enrolled user has administrator privileges for updating clusters through CAU feature.
- Connectivity to selected update source.
- Availability of failover clusters.
- Ensure that Windows Server 2012 or Windows Server 2012 R2 or Windows 2016 operating system is installed on all failover cluster nodes to support the CAU feature.

- Configuration of automatic updates is not enabled to automatically install updates on any failover cluster node.
- Enable firewall rule that enables remote shutdown on each node in the failover cluster.
- Cluster group should have minimum of two nodes.
- Check for cluster update readiness and ensure that there are no major errors and warnings in the Cluster Readiness report for applying the CAU method. For more information about CAU, see Requirements and Best Practices for Cluster—aware Updating section at [Technet.microsoft.com](https://technet.microsoft.com).

NOTE:

For information about applying the updates, see [Upgrading and downgrading firmware versions using run update method](#) .

Creating clusters using Operational Template

This chapter covers information about creating the Storage Spaces Direct clusters.

Creating logical switch for Storage Spaces Direct clusters

About this task

Create logical switch from OMIMSSC in SCVMM.

NOTE: The IP address that is entered in Configuration for Management section overrides the IP address that is entered in operating system component of Storage Spaces Direct predefined Operational Template.

Steps

- 1 In OMIMSSC, expand **Configuration and Deployment**, click **Cluster View**, and then click **Create logical switch for Cluster**.
- 2 Provide a name for the logical switch, and select the host group present in SCVMM for associating the logical switch.
- 3 Provide the following details, and click **Create**.
 - a In **Configuration for Management**, provide the **Subnet**, **Start IP**, **End IP**, **DNS Server**, **DNS Suffix**, and **Gateway** details.

NOTE: Provide the subnet information in Classless InterDomain Routing (CIDR) notation.
 - b In **Configuration for Storage**, provide the **VLAN**, **Subnet**, **Start IP**, and **End IP** details.
- 4 enter a unique job name, description for the job, and click **Create**.
To track this job, the **Go to the Job List** option is selected by default.

Next steps

To verify that the logical switch is created successfully, check for the logical switch name in the drop-down menu listed in **Create Cluster** page.

To view the details of the logical switch, perform the following steps in SCVMM:

- 1 To view the logical switch name, click **Fabric**, and in **Networking**, click **Logical Switches**.
- 2 To view the logical switch's Uplink Port Profile (UPP), click **Fabric**, and in **Networking**, click **Logical Switches**.
- 3 To view the logical switch's network, click **Fabric**, and in **Networking**, click **Logical Networks**.

Creating Storage Spaces Direct clusters

Prerequisites

- Ensure that you create a logical network by using the **Configure Network for Cluster** feature.
- Ensure that you are using SC2016 VMM.
- Ensure that you are using Windows Server 2016 Datacenter edition
- Ensure that the managed servers configurations match the Storage Spaces Direct solution firmware and driver versions requirements. For more information, see *Dell EMC Storage Spaces Direct Ready Nodes PowerEdge R740XD and PowerEdge R640 Support Matrix* documentation.
- For infrastructure and management details of Storage Spaces Direct, see *Dell EMC Microsoft Storage Spaces Direct Ready Node Deployment Guide for scalable hyper-converged infrastructure with R740xd and R640 Storage Spaces Direct Ready Nodes* documentation.

About this task

Consider the following before creating Storage Spaces Direct clusters:

- You can create Storage Spaces Direct cluster in OMIMSSC by providing static IP address only.
- Virtual disk size is displayed as zero in the Storage Spaces Direct predefined Operational Template. But, after applying the Storage Spaces Direct predefined Operational Template, the virtual drive is created only of size equal to the full size of the M.2 physical storage media. For more information about the virtual drive space, see iDRAC User's Guide available at dell.com/support.

To create Storage Spaces Direct cluster, perform the following steps:

Steps

- 1 In OMIMSSC, click **Configuration and Deployment** and then click **Cluster View**.
The **Cluster View** page is displayed.
- 2 Provide a cluster name, and select the predefined Operational Template for creating Storage Spaces Direct clusters.
 - Unassigned servers that belong only to a specific server model and NIC card are displayed based on the Operational Template you select from **Operational Template** drop-down menu.
- 3 To add servers into a cluster, select the servers by using the check box.
- 4 To add system-specific pool values, click **Export Attribute Value Pool**.
Edit and save the file so that you can provide the system-specific pool values.
- 5 (Optional) If you have to set system-specific values, in **Attribute Value Pool**, click **Browse** and select the edited .CSV file.
- 6 Provide a unique job name, and click **Create**.
To track this job, the **Go to the Job List** option is selected by default.

Next steps

To check if the clusters are created successfully:

- 1 Check for success status of cluster job creation.
- 2 View the cluster in **Cluster View** page.
- 3 View the cluster in SCVMM.

Managing devices in OMIMSSC

Maintain servers and Modular Systems up-to-date by scheduling jobs for upgrading firmware for server and Modular Systems components. Manage servers by recovering servers to an earlier state by exporting its earlier configuration, applying the configurations of the old component on replaced component, and exporting LC logs for troubleshooting.

Topics:

- [Server recovery](#)
- [Applying firmware and configuration settings on replaced component](#)
- [Collecting LC logs for servers](#)
- [Exporting inventory](#)
- [Cancelling scheduled jobs](#)

Server recovery

Save a server's configurations in protection vault by exporting a server's configurations to a profile and importing the profile on same server to reinstate it to an earlier state.

Protection vault

Protection vault is a secure location where you can save server profiles. Export server profile from a server or a group of servers and import them to same server or group of servers. You can save this server profile on a shared location in the network by creating an external vault or on a vFlash Secure Digital (SD) card by creating an internal vault. You can associate a server or a group of servers with only one protection vault. However, you can associate one protection vault with many servers or group of servers. You can save a server profile on only one protection vault. However, you can save any number of server profiles on a single protection vault.


Creating protection vault

Prerequisite

Ensure that vault location is accessible.

Steps

- 1 In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
- 2 In **Maintenance Center**, click **Protection Vault**, and then click **Create**.
- 3 Select a type of protection vault you want to use and provide the details.
 - If you are creating a protection vault of type **Network Share**, provide a location to save the profiles, credentials to access this location and a passphrase to secure the profile.

 **NOTE:** This type of protection vault provides support file sharing of type Common Internet File System (CIFS).
 - If you are creating a protection vault of type **vFlash**, provide the passphrase to secure the profile.

Modifying protection vault

About this task

You cannot modify the name, description, type of protection vault, and passphrase.

Steps

- 1 In **OMIMSSC**, click **Maintenance Center > Maintenance Settings > Protection Vault**.
- 2 To modify the vault, select the vault and click **Edit**.

Deleting protection vault

About this task

You cannot delete a protection vault in the following circumstances:

- The protection vault is associated with a server or a group of servers.
To delete such a protection vault, delete the server or group of servers, and then delete the protection vault.
- There is a scheduled job associated with the protection vault. However, to delete such a protection vault, delete the scheduled job, and then delete the protection vault.

Steps

- 1 In **OMIMSSC**, click **Maintenance Center > Maintenance Settings > Protection Vault**.
- 2 Select the vault to delete and click **Delete**.

Exporting server profiles

Export a server profile including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and the configuration of those components. OMIMSSC Appliance creates a file containing all the configurations, which you can save on a vFlash SD card or network share. Select a protection vault of your choice to save this file. You can export the configuration profiles of a server or a group of servers immediately or schedule it for later. Also, you can select a relevant recurrence option as to how frequently the server profiles have to be exported.

Prerequisite

Disable the **F1/F2 Prompt on Error** option in **BIOS Settings**.

About this task

Consider the following before exporting server profiles:

- At an instance, you can schedule only one export configuration job for a group of servers.
- You cannot perform any other activity on that server or group of servers whose configuration profiles are being exported.
- Ensure that the **Automatic Backup** job in iDRAC is not scheduled at the same time.
- You cannot export server profiles if the filters are applied. To export server profiles, clear all the applied filters.
- To export server profiles, ensure that you have the iDRAC Enterprise license.
- Before exporting server profile, ensure that the IP address of the server is not changed. If the server IP has changed due to any other operation, then rediscover this server in OMIMSSC, and then schedule the export server profile job.

Steps

- 1 In OMIMSSC, click **Maintenance Center**. Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
The **Export Server Profile** page is displayed.
- 2 In the **Export Server Profile** page, provide the job details, and then select a protection vault.
For more information about protection vaults, see [Creation of protection vault](#).

In **Schedule Export Server Profile** select one of the following:

- **Run Now**—export the server configuration immediately of the selected servers, or group of servers.
- **Schedule**—provide a schedule to export the server configuration of the selected group of servers.
 - **Never**—select to export the server profile only once during the scheduled time.
 - **Once a week**—select to export the server profile on a weekly basis.

- **Once every 2 weeks**—select to export the server profile once every two weeks.
- **Once every 4 weeks**—select to export the server profile once every four weeks.

Importing server profile

You can import a server profile that was previously exported for that same server, or group of servers. Importing server profile is useful in restoring the configuration and firmware of a server to a state stored in the profile.

About this task

You can import server profiles in two ways:

- Quick import server profile—allows you to automatically import the latest exported server profile for that server. You need not select individual server profiles for each of the servers for this operation.
- Custom import server profile—allows you to import server profiles for each of the individually selected servers. For example, if exporting server profile is scheduled, and the server profile is exported every day, this feature allows you to select a specific server profile that is imported from the list of server profiles available in the protection vault of that server.

Import server profile notes:

- You can import a server profile from a list of exported server profiles for that server only. You cannot import the same server profiles for different servers or server groups. If you try to import server profile of another server or server group, the import server profile job fails.
- If a server profile image is not available for a particular server or group of servers, and an import server profile job is attempted for that particular server or group of servers, the import server profile job fails for those particular servers that do not have server profile. A log message is added in the Activity logs with the details of the failure.
- After exporting a server profile, if any component is removed from the server, and then an import profile job is started, all the components information are restored except the missing component information is skipped. This information is not available in the activity log of OMIMSSC. To know more about the missing components, see iDRAC's **LifeCycle Log**.
- You cannot import a server profile after applying the filters. To import server profiles, clear all the applied filters.
- To import server profiles, you must have the iDRAC Enterprise license.

Steps

- 1 In OMIMSSC, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.

The **Import Server Profile** page is displayed.

- 2 Provide the details, select the **Import Server Profile Type** you want.

NOTE: A server profile is exported along with the existing RAID configuration. However, you can import the server profile including or excluding the RAID configuration on the server or group of servers. Preserve Data is selected by default and preserves the existing RAID configuration in the server. Clear the check box if you want to apply the RAID settings stored in the server profile.

- 3 To import the server profile, click **Finish**.

Applying firmware and configuration settings on replaced component

The part replacement feature automatically updates a replaced server component to the required firmware version or the configuration of the old component, or both. The update occurs automatically when you reboot the server after replacing the component.

About this task

To set the configurations for part replacement:

Steps

- 1 In OMIMSSC, click **Maintenance Center**, select the servers or group of servers, and then click **Part Replacement**.

NOTE: The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

The **Part Replacement Configuration** window is displayed.

- 2 You can set **CSIOR**, **Part Firmware Update**, and **Part Configuration Update**, to any of the following options, and then click **Finish**:
 - Collect System Inventory On Restart (CSIOR)—collects all the component information on every system restart.
 - **Enabled**—the software and hardware inventory information of the server components are automatically updated during every system restart.
 - **Disabled**—the software and hardware inventory information of the server components are not updated.
 - **Do not change the value on the server**—the existing server configuration is retained.
 - Part firmware update—restores, or upgrades, or downgrades the component firmware version based on the selection made.
 - **Disabled**—the part firmware update is disabled and the same is applied on the replaced component.
 - **Allow version upgrade only**—the upgraded firmware versions are applied on the replaced component, if the firmware version of the new component is earlier than the existing version.
 - **Match firmware of replaced part**—the firmware version on the new component is matched to the firmware version of the original component.
 - **Do not change the value on the server**—the existing configuration of the component is retained.
 - Part configuration update—restores or upgrades the component configuration based on the selection made.
 - **Disabled**—the part configuration update is disabled and the saved configuration of the old component is not applied on the replaced component.
 - **Apply always**—the part configuration update is enabled and the saved configuration of the old component is applied on the replaced component.
 - **Apply only if firmware matches**—the saved configuration of the old component is applied on the replaced component, only if their firmware versions match.
 - **Do not change the value on the server**—the existing configuration is retained.

Collecting LC logs for servers

About this task

LC logs provide records of past activities in a managed server. These log files are useful for server administrators since they provide detailed information about recommended actions and some other technical information that is useful for troubleshooting purpose.

The various types of information available in LC logs are alerts-related, configuration changes on the system hardware components, firmware changes due to an upgrade or downgrade, replaced parts, temperature warnings, detailed timestamps of when the activity has started, severity of the activity, and so on.

The exported LC log file is saved in a folder and the folder is named after the server's service tag. LC logs are saved in the format: `<YYYYMMDDHHMMSSSS>.<file format>`. For example, `201607201030010597.xml.gz` is the LC file name, which includes the date and time of the file when it was created.

There are two options to collect LC logs:

- Complete LC logs—exports active and archived LC log files. They are large in size, and hence compressed to `.gz` format and exported to the specified location on a CIFS network share.
- Active LC logs—exports recent LC log files immediately or schedule a job to export the log files at regular intervals. View, search, and export these log files to OMIMSSC Appliance. In addition, you can save a backup of log files in a network share.

To collect LC logs, perform the following steps:

Steps

- 1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and then click **Collect LC Logs**.
- 2 In **LC Log Collection**, select one of the following options, and click **Finish**:
 - **Export Complete LC Logs (.gz)**—select to export complete LC logs to a CIFS network share by providing Windows credentials.
 - **Export Active Logs (Run now)**—select to export the active logs immediately to OMIMSSC Appliance.
 - (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

NOTE: Ensure that you update the firmware versions of iDRAC and LC before, exporting active LC logs for 11th generation of servers.

- **Schedule LC Log Collection**—select select to export the active logs at regular intervals.
In **Schedule LC Log Collection**, select a date and time to export the log files.

Select a radio button depending on how frequently the files have to be exported. The available options for scheduling frequency to determine how often you want to collect the LC logs are:

- **Never**—this option is selected by default. Select to export the LC logs only once at the scheduled time.
- **Daily**—select to export the LC logs daily at the scheduled time.
- **Once a week**—select to export the LC logs on a weekly basis at the scheduled time.
- **Once every 4 weeks**—select to export the LC logs in every four weeks at the scheduled time.
- (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

NOTE: Provide a share folder with sufficient storage space, since the exported files are large in size.

To track this job, the **Go to the Job List** option is selected by default.

Viewing LC logs

View all the active LC logs, search for detailed description, and download the logs in CSV format.

Prerequisite

Add OMIMSSC Appliance in **Local Intranet site** list as mentioned in *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

Steps

- 1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and click **View LC Logs**.
- 2 All the servers in the selected group and the servers for which LC logs are collected are listed with their LC log files. Click a file name to view all the log entries in the LC log file specific to that server. For more information, see [File description](#).
- 3 (Optional) Use the search box to search description in all the log files, and export the file in CSV format.

There are two ways to search message description in an LC file:

- Click a file name to open the LC log file and search for a description in the search box.
- Provide a description text in the search box, and then view all the LC files with these instances of text.

NOTE: If the LC log message description is long, the message is truncated to 80 characters.

NOTE: The time displayed against the LC log messages follows the iDRAC time zone.

File description

Use this page to view detailed information about recommended actions and some other technical information that are useful for tracking or alert purposes for a particular server.

To view the contents of a file, click a file name:

- You can search for particular message descriptions.
- You can either view the log files in the window or download the file to view additional log messages.
- You can view any comments provided by a user for an activity.

❗ **NOTE:** When using the search option, only the search results are exported to CSV file.

❗ **NOTE:** If the message is long, the message is truncated to 80 characters.

❗ **NOTE:** Click Message ID to view more information about the message.

Exporting inventory

Export the inventory of selected servers or a group of server to an XML or CSV format file. You can save this information in a Windows shared directory or on a management system. Use this inventory information to create a reference inventory file in an update source.

Prerequisite

Ensure that you set the browser settings as mentioned in *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

❗ **NOTE:** You can import the XML file into DRM and create a repository based on the inventory file.

About this task

❗ **NOTE:** Though you select only the component information of a server and export it, the complete inventory information of the server is exported.

Steps

- 1 In OMIMSSC, click **Maintenance Center**.
- 2 Select the servers for which you want to export the inventory, and select the format from **Export Inventory** drop-down menu.
The file is exported in CSV or XML format based on the selection. The file consists of details such as server groups, service tag of the server, host name or IP address, device model, component name, current firmware version on that component, firmware version from the update source, and update action on that component.

Cancelling scheduled jobs

Prerequisite

Ensure that the job is in **Scheduled** state.

Steps

- 1 In OMIMSSC, do any of the following:
 - In the navigation pane, click **Maintenance Center**, and then click **Manage Jobs**.
 - In the navigation pane, click **Jobs and Log Center**, and then click **Scheduled** tab.
- 2 Select jobs that you want to cancel, click **Cancel**, and then to confirm, click **Yes**.

Configuration and deployment

About this task

Discover

Steps

- 1 In OMIMSSC console, perform any one of the following steps:
 - In the dashboard, click **Discover Servers**.
 - In the navigation pane, click **Configuration and Deployment**, click **Server View**, and then click **Discover**.
- 2 Click **Discover**.

Next step

To view the changes made, refresh the **Credential Profile** page.

Topics:

- [Use cases](#)
- [Creating Operational Templates](#)
- [Installer folders](#)
- [Assign Operational Templates](#)
- [Deploy Operational Templates](#)
- [Windows OS component for the OMIMSSC console extension for SCCM](#)
- [Windows component for the OMIMSSC console extension for SCVMM](#)
- [Non-Windows component for the OMIMSSC console extension for SCCM/SCVMM](#)
- [Discovery in enrolled MSSC](#)
- [Importing server profile](#)
- [Export server profile](#)
- [Viewing LC logs](#)
- [Collect LC logs](#)
- [Part replacement](#)
- [Polling and notification](#)
- [Launch iDRAC](#)
- [Launch Input Output Module](#)
- [Resolving synchronization errors](#)
- [Synchronizing OMIMSSC with enrolled Microsoft console](#)

Use cases

- 1 Discover the reference server by using the **Discovery** page. For more information, see the [Discovering servers using manual discovery](#).
- 2 Create an Operational Template, by capturing all the details of the discovered server. For more information, see [Creating Operational Template from reference servers](#).
- 3 Assign an Operational Template on managed device, and check for the template compliance. For more information, see [Assigning Operational Template and running Operational Template compliance for servers](#).
- 4 Deploy an Operational Template to make the device template compliant. For more information, see [Deploying Operational Template on servers](#).

- 5 View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see [Launching Jobs and Logs Center](#).

Creating Operational Templates

Prerequisites

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a reference server by using the **Discovery** feature. For information about discovering servers, see [Discovering servers using manual discovery](#).
- Discover a Modular System by using the **Discovery** feature. For information about discovering Modular Systems, see [Discovering MX7000 by using manual discovery](#).
- If you are not using the default update source, and then create an update source. For more information, see [Creating update source](#).
- For SCCM users:
 - Create a task sequence. For more information, see [Types of task sequence](#).
 - For non-Windows operating system deployment, have a device type credential profile. For more information, see [Creating credential profile](#).
- For SCVMM users:
 - Create a hypervisor profile. For information about creating hypervisor profile, see [Creating hypervisor profile](#).
 - For Windows deployment, have a device type credential profile. For more information, see [Creating credential profile](#).

Steps

- 1 In OMIMSSC, do any of the following to open an Operational Template:
 - In the OMIMSSC dashboard, click **Create Operational Template**.
 - In the navigation pane, click **Profiles > Operational Template**, and then click **Create**.

The **Operational Template** wizard is displayed.

- 2 Click **Create**.
The **Operational Template** wizard is displayed.
- 3 Enter a name and description for the template.
- 4 Select the type of device, and enter the IP address of reference device, and then click **Next**.

 **NOTE:** You can capture the configuration of reference server with iDRAC 2.0 and later.

- 5 In **Device Components**, click a component to view the available attributes and their values.
The components are as follows:
 - Firmware update
 - Hardware components, which are RAID, NIC, and BIOS.

NOTE: In iDRAC Embedded 1 component, following are the privileges and their values for User Admin Privilege attribute.

Table 5. Privilege value table

Value	Privilege
1	Login
2	Configure
4	Configure Users
8	Logs
16	System Control
32	Access Virtual Console
64	Access Virtual Media
128	System Operations
256	Debug
499	Operator Privileges

- Operating system—select either Windows, or ESXi, or RHEL.
- 6 Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
 - 7 Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.

NOTE: Irrespective of the selection made in the check box against each component, all the configurations are captured in the template.

In **Operating System** component, perform the steps in either of the following options, as per your requirement:

- For Windows operating system deployment on SCCM, see [Windows OS component for OMIMSSC console extension for SCCM](#).
 - For Windows operating system deployment on SCVMM, see [Windows component for OMIMSSC console extension for SCVMM](#).
 - OMIMSSC
 - For non-Windows operating system deployment, see [Non-Windows component for OMIMSSC console extensions](#).
- 8 To save the profile, click **Finish**.

Installer folders

The following folders are created after installing the console extension:

- Log—this folder consists of console-related log information.

NOTE: If the credentials for domain administrator account and local administrator account are different, do not use domain administrator account to log in to SCCM or SCVMM. Instead use a different domain user account to log in to SCCM or SCVMM.

Assign Operational Templates

- 1 In OMIMSSC click **Configuration and Deployment**, and then click **Server View**. Select the required servers and click **Assign Operational Template and Run Compliance**.
The **Assign Operational Template and Run Compliance** page is displayed.
- 2 Select the required servers and click **Assign Operational Template and Run Compliance**.
- 3 In OMIMSSC click **Configuration and Deployment**, and click **Modular Systems View**. Select the required Modular System and click **Assign Operational Template**.

The **Assign Operational Template** page is displayed.

- 4 Select the required Modular Systems, and click **Assign Operational Template and Run Compliance**.

The **Assign Operational Template** page is displayed.

- 5 Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

The Operational Template drop-down lists templates, of the same type as that of the devices selected in the previous step.

If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

To view a detailed report, perform the following steps:

- a Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.
 - Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.
 - Red color box—represents that the component is not present on the device.

Deploy Operational Templates

About this task

- NOTE:** Ensure that you do not enable attributes that change the credentials to log in to the device after deploying the Operational Template.

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, and click **Server View**. Select the servers on which you have applied the template, and then click **Deploy Operational Template**.

The **Deploy Operational Template** page is displayed.

- 2 In OMIMSSC, click **Configuration and Deployment**, and click **Modular Systems View**. Select the Modular System on which you have assigned the template, and then click **Deploy Operational Template**.

The **Deploy Operational Template** page is displayed.

- 3 (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.

- NOTE:** Before exporting the pool values, add the IP address of the OMIMSSC Appliance where the OMIMSSC console extension is installed, to the local intranet site. For more information about adding the IP address in IE browser, see *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

- 4 If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.

The format of a .CSV file is `attribute-value-pool.csv`

- NOTE:** Ensure that you select a .CSV file which has all proper attributes and the iDRAC IP or iDRAC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the iDRAC IP or iDRAC credentials changes and is marked as failed though the job may be successful in iDRAC.

- 5 Enter a unique job name, description for the job, and click **Deploy**.

To track this job, the **Go to the Job List** option is selected by default.

Windows OS component for the OMIMSSC console extension for SCCM

- 1 Select a task sequence and deployment method.

 **NOTE:** Only the task sequences deployed on collections are listed in the drop-down menu.

For information about task sequence, see [Task sequence-SCCM](#).

- 2 Select one of the following options for the **Deployment method**:
 - **Boot to network ISO**—reboots specified ISO.
 - **Stage ISO to vFlash and Reboot**—downloads the ISO to vFlash and reboots.
 - **Reboot to vFlash**—reboots to vFlash. Ensure that the ISO is present in the vFlash.

 **NOTE:** To use the Reboot to vFlash option, the label name of the partition that is created on vFlash must be ISOIMG.

- 3 (Optional) To use the image present in the network share, select the **Use Network ISO as Fallback** option.
- 4 enter an LC boot media image file.
- 5 Select the drivers required for the operating system.

Windows component for the OMIMSSC console extension for SCVMM

Select **Hypervisor Profile**, **Credential Profile**, and **Server IP** from.

 **NOTE:** Host Name, and Server Management NIC are always pool values.

If you select **Server IP** from as **Static**, and then ensure that you have configured the logical network in SCVMM, and the following fields are pool values:

- **Console Logical Network**
- **IP Subnet**
- **Static IP Address**

Non-Windows component for the OMIMSSC console extension for SCCM/SCVMM

About this task

Step

Select a non-windows operating system, operating system version, type of share folder, ISO file name, location of the ISO file and the password for the root account of the operating system.

(Optional) Select a Windows type credential profile for accessing the CIFS share.

Host name is a pool value and if you disable DHCP option, and then the following fields are pool values:

- **IP Address**
- **Subnet Mask**
- **Default Gateway**
- **Primary DNS**
- **Secondary DNS**

NOTE: Network File System (NFS) and Common Internet File System (CIFS) share types are supported for non-Windows operating system deployment.

Discovery in enrolled MSSC

After discovery, the server is added to the **Hosts** tab or the **Unassigned** tab. Also, the discovered server is marked as compliant or noncompliant when it contains minimum versions of LC firmware, iDRAC, and BIOS that are required to work with OMIMSSC.

- When discover a PowerEdge server with an operating system on it and already be present in SCCM or SCVMM console, and then the server is listed as a host server under the **Hosts** tab in the OMIMSSC console where the discovery job is initiated.
 - If the host is a modular server, and then the service tag of the Modular System containing the server is also displayed.
 - If the host is part of a cluster, and then the Fully Qualified Domain Name (FQDN) of the cluster is displayed.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, and then the server is listed as an unassigned server under the **Unassigned** tab in all the enrolled OMIMSSC consoles.
- A license is consumed after discovering a server. The **Licensed Nodes** count decreases as the number of licenses are discovered.

Importing server profile

- 1 In OMIMSSC, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.
The **Import Server Profile** page is displayed.
- 2 Select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.
The **Import Server Profile** page is displayed.

Export server profile

- 1 In OMIMSSC, click **Maintenance Center**. Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
The **Export Server Profile** page is displayed.
- 2 Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
The **Export Server Profile** page is displayed.

Viewing LC logs

- 1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and click **View LC Logs**.
- 2 Select the servers' whose logs you want to view, click **LC Logs** drop-down menu, and then click **View LC Logs**.

Collect LC logs

- 1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and then click **Collect LC Logs**.
- 2 Select the servers' whose logs you want to export, and then click **LC Logs** drop-down menu and then click **Collect LC Logs**.

Part replacement

- 1 In OMIMSSC, click **Maintenance Center**, select the servers or group of servers, and then click **Part Replacement**.

NOTE: The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

The **Part Replacement Configuration** window is displayed.

- 2 Select the servers' whose component you want to configure, and then click **Part Replacement**.

 **NOTE:** The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

The **Part Replacement Configuration** window is displayed.

Polling and notification

- 1 In OMIMSSC, click **Maintenance Center**, and then click **Polling and Notification**.
- 2 Click **Polling and Notification**.

Launch iDRAC

- 1 In OMIMSSC, expand **Configuration and Deployment**, and select one of the following:
 - Click **Server View**. Based on the server (if it is a host or an unassigned server), click **Unassigned Servers** or **Hosts** tab, and click the **iDRAC IP** address of the server.
The **Unassigned Servers** tab is displayed by default.

To view the hosts tab, click **Hosts**.
 - Click **Cluster View**. Expand the cluster type and expand cluster group to server level.
The **Server** tab is displayed.
- 2 To launch iDRAC console, click **IP address**.
- 3 To launch iDRAC console, click **IP address**.

Launch Input Output Module

About this task

To launch Input Output Module console, perform the following steps:

Steps

- 1 In OMIMSSC, expand **Configuration and Deployment**, click **Modular Systems View**. Expand the model to individual devices level.
All devices under that model are displayed.
- 2 Click **I/O Modules** tab.
- 3 Click **IP address** of the device.

Resolving synchronization errors

- 1 In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Resolve Sync Errors**.
- 2 Click **Resolve Sync Errors**.

Synchronizing OMIMSSC with enrolled Microsoft console

About this task

Steps

- 1 In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Synchronize with OMIMSSC** to synchronize all the hosts that are listed in enrolled MSSC with the OMIMSSC Appliance.
- 2 To synchronize all the hosts that are listed in the enrolled MSSC with Appliance, click **Synchronize with OMIMSSC**.
Synchronization is a long running task. View the job status in **Jobs and Logs** page.

Assign and deploy

In OMIMSSC, click **Configuration and Deployment**, and then click **Server View**. Select the servers on which you want to deploy a template on, and then click **Deploy Operational Template**.

The **Deploy Operational Template** page is displayed.

Run update

- 1 In OMIMSSC, click **Maintenance Center**, select the servers or Modular System groups, and an update source, and then click **Run Update**.
- 2 Select the servers or Modular System groups, and an update source, and then click **Run Update**.
- 3 enter a unique job name, description for the job, and click **Create**.

To track this job, the **Go to the Job List** option is selected by default.

Appendix

Provide the time zone attribute values manually in MX7000 devices by referring to the below table:

Table 6. Time zone details

Time zone ID	Time zone difference
TZ_ID_1	(GMT-12:00) International Date Line West
TZ_ID_2	(GMT+14:00) Samoa
TZ_ID_3	(GMT-10:00) Hawaii
TZ_ID_4	(GMT-09:00) Alaska
TZ_ID_5	(GMT-08:00) Pacific Time (US and Canada)
TZ_ID_6	(GMT-08:00) Baja California
TZ_ID_7	(GMT-07:00) Arizona
TZ_ID_8	(GMT-07:00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07:00) Mountain Time (US and Canada)
TZ_ID_10	(GMT-06:00) Central America
TZ_ID_11	(GMT-06:00) Central Time (US and Canada)
TZ_ID_12	(GMT-06:00) Guadalajara, Mexico City, Monterrey
TZ_ID_13	(GMT-06:00) Saskatchewan
TZ_ID_14	(GMT-05:00) Bogota, Lima, Quito
TZ_ID_15	(GMT-05:00) Eastern Time (US and Canada)
TZ_ID_16	(GMT-05:00) Indiana (East)
TZ_ID_17	(GMT-04:30) Caracas
TZ_ID_18	(GMT-04:00) Asuncion
TZ_ID_19	(GMT-04:00) Atlantic Time (Canada)
TZ_ID_20	(GMT-04:00) Cuiaba
TZ_ID_21	(GMT-04:00) Georgetown, La Paz, Manaus, San Juan
TZ_ID_22	(GMT-04:00) Santiago
TZ_ID_23	(GMT-03:30) Newfoundland
TZ_ID_24	(GMT-03:00) Brasilia
TZ_ID_25	(GMT-03:00) Buenos Aires
TZ_ID_26	(GMT-03:00) Cayenne, Fortaleza

Time zone ID	Time zone difference
TZ_ID_27	(GMT-03:00) Greenland
TZ_ID_28	(GMT-03:00) Montevideo
TZ_ID_29	(GMT-02:00) Mid-Atlantic
TZ_ID_30	(GMT-01:00) Azores
TZ_ID_31	(GMT-01:00) Cape Verde Is
TZ_ID_32	(GMT+00:00) Casablanca
TZ_ID_33	(GMT+00:00) Coordinated Universal Time
TZ_ID_34	(GMT+00:00) Dublin, Edinburgh, Lisbon, London
TZ_ID_35	(GMT+00:00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
TZ_ID_37	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
TZ_ID_38	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
TZ_ID_39	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
TZ_ID_40	(GMT+01:00) West Central Africa
TZ_ID_41	(GMT+02:00) Windhoek
TZ_ID_42	(GMT+02:00) Amman
TZ_ID_43	(GMT+03:00) Istanbul
TZ_ID_44	(GMT+02:00) Beirut
TZ_ID_45	(GMT+02:00) Cairo
TZ_ID_46	(GMT+02:00) Damascus
TZ_ID_47	(GMT+02:00) Harare, Pretoria
TZ_ID_48	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
TZ_ID_49	(GMT+02:00) Jerusalem
TZ_ID_50	(GMT+02:00) Minsk
TZ_ID_51	(GMT+03:00) Baghdad
TZ_ID_52	(GMT+03:00) Kuwait, Riyadh
TZ_ID_53	(GMT+03:00) Moscow, St. Petersburg, Volgograd
TZ_ID_54	(GMT+03:00) Nairobi
TZ_ID_55	(GMT+03:30) Tehran
TZ_ID_56	(GMT+04:00) Abu Dhabi, Muscat
TZ_ID_57	(GMT+04:00) Baku
TZ_ID_58	(GMT+04:00) Port Louis
TZ_ID_59	(GMT+04:00) Tbilisi
TZ_ID_60	(GMT+04:00) Yerevan

Time zone ID	Time zone difference
TZ_ID_61	(GMT+04:30) Kabul
TZ_ID_62	(GMT+05:00) Ekaterinburg
TZ_ID_63	(GMT+05:00) Islamabad, Karachi
TZ_ID_64	(GMT+05:00) Tashkent
TZ_ID_65	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
TZ_ID_66	(GMT+05:30) Sri Jayawardenepura
TZ_ID_67	(GMT+05:45) Kathmandu
TZ_ID_68	(GMT+06:00) Astana
TZ_ID_69	(GMT+06:00) Dhaka
TZ_ID_70	(GMT+06:00) Novosibirsk
TZ_ID_71	(GMT+06:30) Yangon (Rangoon)
TZ_ID_72	(GMT+07:00) Bangkok, Hanoi, Jakarta
TZ_ID_73	(GMT+07:00) Krasnoyarsk
TZ_ID_74	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
TZ_ID_75	(GMT+08:00) Irkutsk
TZ_ID_76	(GMT+08:00) Kuala Lumpur, Singapore
TZ_ID_77	(GMT+08:00) Perth
TZ_ID_78	(GMT+08:00) Taipei
TZ_ID_79	(GMT+08:00) Ulaanbaatar
TZ_ID_80	(GMT+08:30) Pyongyang
TZ_ID_81	(GMT+09:00) Osaka, Sapporo, Tokyo
TZ_ID_82	(GMT+09:00) Seoul
TZ_ID_83	(GMT+09:00) Yakutsk
TZ_ID_84	(GMT+09:30) Adelaide
TZ_ID_85	(GMT+09:30) Darwin
TZ_ID_86	(GMT+10:00) Brisbane
TZ_ID_87	(GMT+10:00) Canberra, Melbourne, Sydney
TZ_ID_88	(GMT+10:00) Guam, Port Moresby
TZ_ID_89	(GMT+10:00) Hobart
TZ_ID_90	(GMT+10:00) Vladivostok
TZ_ID_91	(GMT+11:00) Magadan, Solomon Is New Caledonia
TZ_ID_92	(GMT+12:00) Auckland, Wellington
TZ_ID_93	(GMT+12:00) Fiji
TZ_ID_94	(GMT+13:00) Nuku'alofa

Time zone ID	Time zone difference
TZ_ID_95	(GMT+14:00) Kiritimati
TZ_ID_96	(GMT+02:00) Athens, Bucharest


Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — www.dell.com/esmmanuals
- For Dell EMC OpenManage documents — www.dell.com/openmanagemanuals
- For Dell EMC Remote Enterprise Systems Management documents — www.dell.com/esmmanuals
- For iDRAC and Dell Lifecycle Controller documents — www.dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — www.dell.com/esmmanuals
- For Dell EMC Serviceability Tools documents — www.dell.com/serviceabilitytools
- a Go to www.dell.com/support.
- b Click **Browse all products**.
- c From **All products** page, click **Software**, and then click the required link from the following:
 - **Analytics**
 - **Client Systems Management**
 - **Enterprise Applications**
 - **Enterprise Systems Management**
 - **Public Sector Solutions**
 - **Utilities**
 - **Mainframe**
 - **Serviceability Tools**
 - **Virtualization Solutions**
 - **Operating Systems**
 - **Support**
- d To view a document, click the required product and then click the required version.
- Using search engines:
 - Type the name and version of the document in the search box.

Contacting Dell

Prerequisite

 **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.

About this task

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:

Steps

- 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.