Dell OpenManage Enterprise-Modular Edition Version 2.00.00 for PowerEdge MX7000 Chassis

User's Guide

February 2023
Rev. A04

DELL Technologies

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.

Revision history

Table 1. Revision history

Date	Document revision	Description of changes
February 2023	A04	v2.00.00-Updated for MX760c platform
January 2023	A03	v2.00.00-Updated MXG610s FOS version support
December 2022	A02	v2.00.00 ● Updated validated stack catalog version ● Updated MXG610s FOS version support ● Updated iDRAC version support ● Updated IOM upgrade matrix
October 2022	A01	v2.00.00 ● Supports BIOS version 1.7.5 for MX750c
August 2022	A00	v2.00.00 ● Local RSA multifactor authentication solution ● Secured Component Verification (SCV) for MX chassis ● Automatic installation and renewal of TLS certificates ● TLS 1.3 version ● Back up or restore enhancements: ○ HTTPS share to support backup or restore ○ Periodic and scheduled backups ○ Back up option on lead dashboard under **Group Configuration** drop-down ○ Security SSL certificates ● Template or profile updates without changing assigned identities ● Sort or search options while editing template or customer request ● Alerts when an NTP address cannot be resolved ● Selecting one or more chassis, compute, or SAS IOM to extract troubleshooting logs simultaneously ● Storage-NVME/TCP Network Type option when creating a VLAN ● Minimum restriction on available data path VLANs ● Increased VLAN scaling in Full switch and SmartFabric mode ● Default uplink feature through OpenManage Network Integration UI ● VLAN stacking in Full switch mode
May 2022	A01	v1.40.20 ● Added support for NVMe/TCP
March 2022	A00	v1.40.20 ● Includes Apache log4j version 2.17.1 ● Added VMware ESXi-MX Baseline validation matrix
December 2021	A00	v1.40.10 ● Supports Apache log4j patch for CVE-2021-044228, CVE-2021-4104, CVE-2021-45046
December 2021	A00	v1.40.00 ● Supports phased update order for OME-Modular 1.40.00 and later versions ● Supports backup and restore of chassis and network IOM ● Supports enhanced validated stack catalog creation ● Supports SNMP v3 protocols ● Supports adding devices to existing baseline ● Increased VLANs ● Displays security banner on the login page ● Supports syncing OME-Modular firmware if there is any mismatch

Table 1. Revision history (continued)

Date	Document revision	Description of changes
		• Supports detection and display of the GPU acceleration module of Amulet Hotkey
July 2021	A02	v1.30.10 • Support for DC PSU • Updates for solution baselines v1.20.00, v1.20.10, v1.30.00 • Updates for OS10 firmware update matrix
May 2021	A01	v1.30.00—Updates for MX750c platform
April 2021	A00	v1.30.00—Updates for new features and enhancements
August 2020	A00	v1.20.10—Updates for new features and enhancements
June 2020	A00	v1.20.00—Updates for new features and enhancements
March 2020	A00	v1.10.20—Updates for new features and enhancements
November 2019	A00	v1.10.10—Updates for new features and enhancements
September 2019	A01	v1.10.00—Updates for new features and enhancements
August 2019	A00	v1.10.00—Updates for new features and enhancements
February 2019	A00	v1.00.10—Updates for new features and enhancements

Contents

1

Overview

The Dell OpenManage Enterprise Modular (OME-Modular) application runs on the PowerEdge MX9002m management module (MM) firmware. OME-Modular facilitates configuration and management of a stand-alone PowerEdge MX chassis or group of MX chassis using a single Graphical User Interface (GUI). You can use OME-Modular to deploy servers and update firmware. You can also manage the overall health of the chassis and the chassis components such as compute sleds, network devices, input or output modules (IOMs), and storage devices. OME-Modular also facilitates the following activities on the hardware:

- Connectivity of management network.
- Discovery and inventory.
- Monitoring and power control operations and thermal functions.

You can use OME-Modular to manage key workloads on the MX7000 platforms.

- Large and unstructured data and analytics
- Hyper converged and traditional workloads
- Database workloads
- Software defined storage
- HPC and performance workloads

The lead chassis in the Multi Chassis Management (MCM) enables you to perform the following tasks:

- Manage servers across multiple MX chassis.
- Deploy or update servers from lead chassis without launching the member chassis web interface.
- Manage fabric switch engines in fabric mode using the OME-Modular web interface.
- Manage alert log and actions.
- Manage virtual MAC/WWN identity pools.
- Deploy compute sleds easily using server profiles and templates.

OME-Modular offers simple and static roles such as the chassis administrator, compute manager, fabric manager, storage manager, and viewer roles while, OpenManage Enterprise offers static and dynamic groups with role-based access control (RBAC).

Topics:

Key features

The key features of OME-Modular are:

- End-to-end life cycle management for servers, storage, and networking.
- Addition of a new chassis to add server, storage, and networking capacity.
- Multiple chassis management using a single interface—web or RESTful interface.
- Management of network IOMs and SmartFabric Services.
- Usage of the automation and security features of iDRAC9.

New in this release

This release of OME-Modular 2.00.00 supports:

- PowerEdge MX760c platform.
- Local RSA multi-factor authentication solution.
- Secured Component Verification (SCV) for MX chassis.
- Automatic installation and renewal of TLS certificates.
- TLS 1.3 version
- Back up or restore enhancements
  - HTTPS share to support backup or restore
  - Periodic and scheduled backups
  - Backup option on lead dashboard under **Group Configuration** drop-down
  - Security SSL certificates
- Template or profile updates without changing assigned identities.
- Sort or search options while editing template.
- Alerts when an NTP address cannot be resolved.
- Selecting one or more chassis, compute, or SAS IOM to extract troubleshooting logs simultaneously.
- Storage-NVME/TCP Network Type option when creating a VLAN.
- Minimum restriction on available data path VLANs .
- Increased VLAN scaling in Full switch and SmartFabric mode.
- Default uplink feature through OpenManage Network Integration UI.
- VLAN stacking in Full switch mode.

1.40.20

- Apache log4j version 2.17.1
- NVMe/TCP

1.40.10

- Apache log4j patch for CVE-2021-044228, CVE-2021-4104, CVE-2021-45046.

1.40.00

- Phased update order for OME-Modular 1.40.00 and later versions.
- Backup and restore of chassis and network IOM.
- Enhanced backup and restore for management configuration recovery.
  - System configurations
  - Catalog baselines
  - Alert policies
  - SmartFabric
- Enhanced validated stack catalog creation.
- SNMP v3 trap forwarding.
- Adding devices to existing baseline.
- Increased VLANs.
- Security banner on the Login page.
- Syncing OME-Modular firmware if there is any mismatch.

1.30.10

- DC power supply
- Compatible BIOS 2.11.2 for MX740c and MX840c
- Compatible iDRAC 4.40.29.00 for MX750c
- Compatible OS10 version 10.5.0.9, 10.5.1.9, and 10.5.2.6
- Revised OS10 update restrictions in section OS10 firmware update matrix

1.30.00

- PowerEdge MX750c platform.
- Group configuration option on the **Home** page in multichassis environment.
- Profiles menu to create, assign, edit, and redeploy profiles with identities separately from templates.
- Editing templates.
- Advanced license for:
  - Chassis telemetry for power, thermal, and fans. For more information, see the OpenManage Enterprise Modular Edition RESTful API Guide.
  - OpenID Connect Provider for delegated authentication.
- Redfish alert forwarding. For more information, see the OpenManage Enterprise Modular Edition RESTful API Guide.
- Ethernet IOM switch replacement wizard for easy replacement of faulty fabric switches.
- L2 Multicast in SmartFabric Services.
- LCD enhancement using PIN entry to unlock emergency access to local actions such as chassis power off.
- Reminder to select backup chassis.
- Same SSO login session sharing in tabs and not counting against the limit on number of sessions.
- Fabric creation progress banner.
- OS10 DUP to be posted in the validated stack catalog.
- Link to Release Notes from the info icon on the **Compliance Report** page.
- Displaying pre-requisites and dependencies for components in compliance report.
- Automatic restoration of configuration to Right Control Panel (RCP) on replacement. For more information, see the Dell PowerEdge MX7000 Enclosure Field Service Manual.

1.20.10

- Quad-Port Ethernet adapters in up to 5 MX7000 chassis in a Scalable Fabric
- Increased the VLAN scale for SmartFabric services
- More topologies for Fabric Expander Module connectivity
- Compliance status **Unknown** in the Compliance Report. The **Unknown** status highlights the component or device firmware that is missing from the catalog and must be compared manually for compliance.

1.20.00

- Deploying templates on empty slots or slots that compute sleds occupy.
- Reclaiming MAC identities after removing profiles that are associated with blade servers.
- Synchronizing VLAN definitions of OME-Modular and OpenManage Enterprise.
- Alert notifications when a chassis is onboarded.
- Configuring Forward Error Correction (FEC) for SmartFabric.
- Propagating VLANs without server reboot.
- Deploying operating system using Boot to ISO after applying profile.
- Enhancements to Uplink Failure Detection.
- Enabling `racadm connect` to MXG610s.
- Performing Hard Reset only on iDRAC instead of whole sled.
- Setting Name field as the default sort order in device grids.
- Enhanced alert pop-ups to appear on the upper right corner of the user interface.
- New SmartFabric Uplink type—Ethernet - No Spanning Tree.
- Reduction in alert volumes API to replace failed Ethernet switch Autodetection of Scalable Fabric expansion from one to two chassis.

1.10.20

- Customization of chassis backup file name.
- Customization of host operating system reboot if a template deployment fails.
- Hard reset of slot-based iDRAC interface from the **Chassis Slots** page.

- Updating MX7000 components.

1.10.00

- Group management through LCD.
- Assigning member chassis in MCM as backup chassis and promoting backup chassis as lead chassis.
- Configuring hot spare for the chassis.
- Accessing chassis using USB.
- Customizing strings that are displayed on the chassis LCD.
- Configuring network session inactivity timeout.
- Extracting logs to a local drive on your system.
- Downloading the Management Information Base (MIB) file to a local drive on your system.

1.00.10

- Twenty chassis in a multichassis management (MCM) group.
- Editing VLANs that are already deployed to a server, using a template.
- Federal Information Processing Standard (FIPS) 140-2 standards. For details, see certificate #2861 at csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2861.

Supported platforms

OME - Modular supports the following platforms and components:

Platforms:

- PowerEdge MX7000
- PowerEdge MX740c
- PowerEdge MX750c
- PowerEdge MX760c
- PowerEdge MX840c
- PowerEdge MX5016s
- PowerEdge MX5000s SAS Switch
- PowerEdge MX 25 Gb Ethernet Pass-Through Module
- MX 10GBASE-T Ethernet Pass-Through Module
- Dell MX9116n Fabric Switching Engine
- Dell MX5108n Ethernet Switch
- Dell MX7116n Fabric Expander Module
- Dell MXG610s Fibre Channel Switching Module
- PowerEdge MX9002m Management module

Supported web browsers

OME–Modular is supported on the following web browsers:

- Google Chrome version 94
- Google Chrome version 95
- Mozilla Firefox version 92
- Mozilla Firefox version 93
- Microsoft EDGE 94
- Microsoft EDGE 95
- Microsoft Internet Explorer 11
- Safari version 15

For the OME–Modular web interface to load properly in the web browsers, ensure that the Active X or Java script and font download options are enabled.

Other documents you may need

For more information about managing your system, access the following documents:

Table 2. List of other documents for reference

Name of the document	Brief introduction of the document
OpenManage Enterprise Modular RACADM Command Line Reference Guide	This document contains information about the RACADM subcommands, supported interfaces, and property database groups and object definitions.
OpenManage Enterprise Modular Release Notes	This document provides the latest updates to the system or documentation or advanced technical reference material that is intended for experienced users or technicians.
OpenManage Enterprise and OpenManage Enterprise – ModularRESTful API Guide	This document provides information about integrating your applications with OpenManage Enterprise Modular, using the RESTful API commands.
Integrated Dell Remote Access Controller (iDRAC) User's Guide	This document provides information about installation, configuration, and maintenance of the iDRAC on managed systems.
OS10 Enterprise Edition User Guide	This document provides information about the features of the OS10 switches and using commands in the IOM CLI to configure the switches.
Dell PowerEdge MX Networking Deployment Guide	This document provides information about configuring and troubleshooting SmartFabric Services running on PowerEdge MX systems.
Dell PowerEdge MX7000 Enclosure Installation and Service Manual	This document provides information about installing and replacing components in the PowerEdge MX7000 enclosure.
Dell PowerEdge MX5016s and MX5000s Installation and Service Manual	This document provides information about installing and replacing components in the PowerEdge MX5016s storage sled and PowerEdge MX5000s SAS IOM.
SFSS Deployment Guide	This document demonstrates the planning and deployment of SmartFabric Storage Software (SFSS) for NVMe/TCP.
NVMe/TCP Host/Storage Interoperability Simple Support Matrix	This document provides information about NVMe/TCP Host/ Storage Interoperability support matrix
NVMe/TCP Supported Switches Simple Support Matrix	This document provides information about NVMe/TCP Supported Switches Simple Support Matrix

Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:
  - For OpenManage documents—https://www.dell.com/openmanagemanuals
  - For iDRAC and Lifecycle Controller documents—https://www.dell.com/idracmanuals
  - For all Enterprise Systems Management documents—https://www.dell.com/esmmanualsDell.com/SoftwareSecurityManuals
  - For OpenManage Connections Enterprise Systems Management documents—https://www.dell.com/esmmanuals
  - For Serviceability Tools documents—https://www.dell.com/serviceabilitytools
  - For Client Command Suite Systems Management documents—https://www.dell.com/omconnectionsclient
  - For SmartFabric OS10 documents—infohub.delltechnologies.com
  - For Dell Simple Support Matrices—https://elabnavigator.dell.com/eln/modernHomeSSM
  - For SmartFabric Storage Software Deployment Guide—https://infohub.delltechnologies.com/t/smartfabric-storage-software-deployment-guide/
- From the Dell Support site:

1. Go to https://www.dell.com/support.
2. Click **Browse all products**.
3. Click the required product category, such as Servers, Software, Storage, and so on.
4. Click the required product and then click the required version if applicable.

   NOTE: For some products, you may have to navigate through the subcategories.
5. Click **Manuals & documents**.

Positioning OME-Modular with other Dell applications

OME–Modular works with the following applications to manage, simplify, and streamline operations:

- OME–Modular discovers and inventories MX7000 chassis in the data center using the OME–Modular REST API commands.
- integrated Dell Remote Access Controller (iDRAC)—OME–Modular manages virtual consoles through iDRAC.
- Repository Manager—OME–Modular uses Repository Manager to create custom repositories in shared networks for creating catalogs. The catalogs are used for firmware updates.
- OME–Modular extracts the OpenManage SupportAssist logs from iDRAC for resolving issues.

2

Updating firmware for PowerEdge MX solution

Component and device firmware for the MX solution are rigorously tested as a validated solution stack or firmware baseline. The details are listed in the table Updating MX7000 components using OME-Modular containing current and previous baselines. When the Dell update packages (DUPs) are available on https://www.dell.com/support , a validated solution stack of the chassis firmware catalog referencing them is published. OME-M compares the update packages with currently installed versions using a Compliance Report, for more information, see Managing Firmware chapter.

The advantages of using OME-M to perform updates using the catalog:

- Automatically downloads the DUPs from the support site.
- Updating all the components simultaneously in the required order.

The sequence to update components and devices manually is described in Component update order section. For pre-requisite firmware versions for updating OME-M, see Firmware update matrix.

In an MCM environment, perform the firmware update for all devices from the lead chassis. Also, select the IOMs and storage sleds as individual devices and not as chassis components, for a successful firmware update.

Topics:

MX7000 Solution Baselines

You can upgrade the following components of MX7000 using OME-Modular web interface. The following table lists the new versions of the MX7000 components:

NOTE: For more information about the previous OME-M baseline versions, see MX7000 Solution Baselines for previous versions

Table 3. MX7000—OME-Modular 2.00.00 and previous solution baselines

Validated MX Stack Catalog Version	**21.04.00**	**21.09.00**	**21.12.00**	**22.03.00**	**22.11.00** **23.03.00** ******	**—**
Component	**v1.30.00**	**v1.30.10**	**v1.40.00** **v1.40.10**	**v1.40.20**	**v2.00.00**	**Catalog exceptions**
iDRAC with Lifecycle Controller for PowerEdge MX740c and MX840c	4.40.10.00	4.40.10.00	5.10.00.00	5.10.00.00	• 5.10.50.00 • 6.00.30.00	None
iDRAC with Lifecycle Controller for PowerEdge MX750c	• 4.40.20.00 • 4.40.29.00 **	• 4.40.20.00 ** • 4.40.29.00	5.10.00.00	5.10.00.00	• 5.10.50.00 • 6.00.30.00	None
iDRAC with Lifecycle Controller for PowerEdge MX760c	N/A	N/A	N/A	N/A	6.10.05.00	None
Dell Server BIOS PowerEdge MX740c and 840c	• 2.10.2 • 2.11.2**	• 2.10.2 • 2.11.2**	2.12.2	2.13.3	2.15.1	None

Table 3. MX7000—OME-Modular 2.00.00 and previous solution baselines (continued)

Validated MX Stack Catalog Version	**21.04.00**	**21.09.00**	**21.12.00**	**22.03.00**	**22.11.00** **23.03.00** ******	**—**
Component	**v1.30.00**	**v1.30.10**	**v1.40.00** **v1.40.10**	**v1.40.20**	**v2.00.00**	**Catalog exceptions**
Dell Server BIOS PowerEdge MX750c	1.1.3	1.2.4	1.4.4	1.5.4	• 1.6.5 • 1.7.4—Factory install only • 1.7.5	None
Dell Server BIOS PowerEdge MX760c	N/A	N/A	N/A	N/A	1.0.0	None
QLogic 26XX series Fibre Channel adapters	15.20.14	15.20.14	15.30.08	15.30.08	15.35.08	None
QLogic 27XX series Fibre Channel adapters	15.20.14	15.20.14	15.30.08	15.30.08	• 15.35.08 • 16.10.04*****	None
QLogic 41xxx series adapters	15.20.16	15.20.16	15.30.05	15.30.05	• 15.35.06 • 16.10.00*****	None
Broadcom 57504 Quad Port device adapters	• 21.80.16.92—Factory install only • 21.80.16.95—Recommended upgrade version	• 21.80.16.92—Factory install only • 21.80.16.95—Recommended upgrade version	21.85.21.91	21.85.21.91	• 22.00.07.60 • 22.31.11.61*****	None
Mellanox ConnectX-4 Lx Ethernet Adapter Firmware	14.28.45.12	14.28.45.12	14.31.20.06	14.31.20.06	14.32.20.04	None
Intel NIC Family Version Firmware for X710, XXV710, and XL710 adapters	20.0.17	20.0.17	20.5.13	20.5.13	20.5.13	None
Intel NIC Family Version Firmware for X810 adapters	N/A	N/A	N/A	N/A	21.5.9*****	None
Emulex Fibre Channel Adapter Firmware 32G	03.04.24	3.04.24	03.05.20	03.05.20	• 03.06.55 • 03.06.63*****	None
OpenManage Enterprise Modular	1.30.00	1.30.10	• 1.40.00** • 1.40.10	1.40.20	2.00.00	None
MX9116n Fabric Switching Engine OS10	• 10.5.2.3—Factory install only*** • 10.5.2.4*** • 10.5.2.6	10.5.2.6	10.5.3.1	10.5.3.1	10.5.4.1	None
MX5108n Ethernet Switch OS10	• 10.5.2.3—Factory install only***	10.5.2.6	• 10.5.3.1 • 10.5.3.7**	• 10.5.3.1 • 10.5.3.7**	• 10.5.4.1 • 10.5.4.6**	None

Table 3. MX7000—OME-Modular 2.00.00 and previous solution baselines (continued)

Validated MX Stack Catalog Version	**21.04.00**	**21.09.00**	**21.12.00**	**22.03.00**	**22.11.00** **23.03.00** ******	**—**
Component	**v1.30.00**	**v1.30.10**	**v1.40.00** **v1.40.10**	**v1.40.20**	**v2.00.00**	**Catalog exceptions**
	• 10.5.2.4*** • 10.5.2.6					
MX5016s Storage Sled	2.40	2.40	2.40	2.40	2.40	None
MX5000s SAS IOM	1.0.9.8	1.0.9.8	1.0.9.8	1.0.9.8	1.0.9.8	None
MXG610s	• 8.1.0_lnx2 • 8.1.0_lnx3 • 9.0.1e1 • 9.1.1b	• 8.1.0_lnx2 • 8.1.0_lnx3 • 9.0.1e1 • 9.1.1b	• 8.1.0_lnx2 • 8.1.0_lnx3 • 9.0.1e1 • 9.1.1b	• 8.1.0_lnx2 • 8.1.0_lnx3 • 9.0.1e1 • 9.1.1b	• 9.0.1e1 • 9.1.1b	No catalog update or DUP
Network IOM ONIE	3.35.5.1-23	3.35.5.1-23	3.35.5.1-24	3.35.5.1-24	3.35.5.1-24	None
Delta AC PSU	68.5F	68.5F	68.5F	68.5F	68.5F	Manual DUP
Artesyn AC PSU	36.6C	36.6C	36.6C	36.6C	36.6C	Manual DUP
Artesyn DC PSU					00.17.17	Manual DUP
NVMe/TCP	NA	NA	NA	Supported****	Supported*****	None

*Update to operating system 10.5.0.9 and then to 10.5.1.9 or 10.5.2.6. Run the X.509v3 certificate upgrade script before upgrading any operating system versions. For more details see, OS10 firmware update matrix.

**Update using individual DUP or obtain from the Latest component firmware versions on Dell.com catalog.

***Update restrictions apply. For more information, see OS10 firmware update matrix.

****NVMe/TCP and SmartFabric Storage Software (SFSS) solutions with PowerEdge MX require PowerEdge MX Baseline 22.03.00 (1.40.20) or 22.09.00 (2.00.00), and are supported in full switch mode only. Converged FCoE and NVMe/TCP on the same IOM is not supported. NVMe/TCP and SFSS solutions with SmartFabric Mode are not supported. The new "Storage - NVMe/TCP" VLAN type is defined for future support with SmartFabric Mode.

*****Supported only for MX760c platforms.

******Support added in catalog for MX760c platforms.

Before updating MX7000, check the PSU version. If the PSU version is 00.36.6B, and then update the PSU. For details, see https://www.dell.com/support/home/en-us/drivers/driversdetails?driverid=5tc17&oscode=naa&productcode=poweredge-mx7000.

NOTE: For details on VMware ESXi versions validated with MX baselines, see the VMware ESXi MX Validation Matrix.

NOTE: Updating the MXG610s IOM is not supported from the OME-Modular user interface. Use the MXG610s interface on the IOM.

NOTE: Updating MX9116n or MX5108n using catalog method is not supported for OME-Modular versions 1.20.10 and lower. It is supported from 1.30.00 onwards.

NOTE: As these update instructions include updates to various components of the solution, there is a possibility of traffic impact to existing workloads. It is recommended that the updates are applied only during a regular maintenance window.

NOTE: Upgrades from baselines before 1.20.00 might need a power cycle (cold boot) of the MX7000 chassis. Updating all applicable solution components after power cycle may be necessary as a last troubleshooting step. For details, see Controlling chassis power.

Updating the firmware using catalog-based compliance method

NOTE: The migration of compute sled workloads in batches to perform compute sled updates is supported during the required maintenance window for MX Solution update process.

Updating firmware using catalog-based compliance is a best practice and a recommended update process.

To update the firmware using the catalog-based compliance method:

1. Update the device adapter operating system drivers followed by the device adapter firmware.
   NOTE: For device adapter firmware versions, see, the respective user's guide and release notes.
2. Go to the **Configuration Firmware** page to create the catalog and baseline using Validated Stack catalog.
3. Select the baseline and click **View Report**. **Compliance Report** page is displayed.
4. Update the devices in the following sequential order.
   a. **Compute**
      i. From the **Advance Filters**, select **Compute** from the **Type**. The list of Compute devices is displayed.
      ii. Click **Select all** checkbox and then click **Make Compliant**.
      iii. Go to the **Monitor > Jobs** page to view the job status.
      iv. Wait for the Compute updates to complete and then start the Chassis update.
   b. **Chassis**
      i. From the **Advance Filters**, select **Chassis** from the **Type** and enter **OpenManage Enterprise Modular** in the **Component Contains** box.
      ii. Click **Select all** checkbox and then click **Make Compliant**.
      iii. Go to the **Monitor > Jobs** page to view the job status.
      iv. Wait for the Chassis updates to complete and then start the Network IOM update.
   c. **Network IOM**
      i. From the **Advance Filters**, select **Network IOM** from the **Device Type**. The list of Network IOM devices is displayed.
      ii. Select the required number of IOMs and click **Make Compliant**.
      NOTE: See the IOM Firmware update matrix and Grouping IOMs for firmware update from updating Firmware section to view the combination of IOMs that can be updated.
      iii. Go to the **Monitor > Jobs** page to view the job status.
      iv. Wait for the Network IOM updates to complete and then start the ONIE component update.
   d. **ONIE Component**
      i. Select the baseline and click **View Report**. **Compliance Report** page is displayed. After performing all the updates, you can view only the list of ONIE component for update.
      NOTE: ONIE component are listed only when all the IOMs are updated to 1.30.00 baseline.
      ii. Click **Select all** checkbox and then click **Make Compliant**.
      iii. Go to the **Monitor > Jobs** page to view the job status.

Component update order for individual package method

WARNING: Read the update instructions before implementing the update procedure. Collate the current versions of the MX7000 components in your environment and note any special instructions that may be called out in the update procedure.

NOTE: You can also update the components in the phased update order to manually orchestrate MX component updates with no workload disruption. See Updating components in phased update order through manual orchestration topic for step-by-step instructions. The phased update order is supported for OME-M 1.40.00 and later versions only.

NOTE: The migration of compute sled workloads in batches to perform compute sled updates is supported during the required maintenance window for MX Solution update process.

Before proceeding with the update, review and resolve any recurring port alerts that are reported on the OME-Modular **Alerts** page.

NOTE: The message ID for an **operational** port is **NINT0001** and for a **non operational** port, is **NINT0002**.

Update the components in the following order:

1. Operating system drivers
   - Update the device adapter operating system drivers followed by the device adapter firmware. See MX7000 Solutions Baselines for device adapters and the supported firmware versions.
2. Compute Sleds

   NOTE: Compute sled updates have no dependencies and can be updated directly to their corresponding OME-Modular 2.00.00 baseline versions identified in Table 2, in MX7000 Solution Baselines.
3. OME-Modular application
4. Fabric Switching Engine MX9116n and Ethernet Switch MX5108n

To update MXG610s IOM, see the section, **software upgrade or downgrade**, in Chapter 6 of the MXG610s Fibre Channel Switch Module Installation Guide, available at https://dl.dell.com/manuals/all-products/esuprt_networking_int/esuprt_networking_switches_series.

NOTE: If you have MX5016s storage sled or MX5000s SAS IOM installed, update them in the compute sled or IOM component order respectively.

NOTE: To update Intel Device Adapter and BOSS firmware, first upgrade OME-Modular to 1.10.10 or later, or use the iDRAC web interface.

OME-Modular firmware update matrix

NOTE: For more information about the earlier versions, see OME-Modular firmware update matrix for previous versions.

Table 4. OME-Modular firmware update matrix

OME-M versions		To							
		OME-M 1.20.00	OME-M 1.20.10	OME-M 1.30.00	OME-M 1.30.10	OME-M 1.40.00	OME-M 1.40.10	OME-M 1.40.20	OME-M 2.00.00
From	OME-M 1.00.01	—	—	—	—	—	—	—	
	OME-M 1.00.10	—	—	—	—	—	—	—	
	OME-M 1.10.00	Yes	Yes	Yes	Yes	—	—	—	
	OME-M 1.10.10	Yes	Yes	Yes	Yes	—	—	—	
	OME-M 1.10.20	Yes	Yes	Yes	Yes	—	—	—	
	OME-M 1.20.00	Yes	Yes	Yes	Yes	—	—	—	
	OME-M 1.20.10	—	Yes	Yes	Yes	—	—	—	
	OME-M 1.30.00	—	—	Yes	Yes	Yes	Yes	Yes	Yes
	OME-M 1.30.10	—	—	—	Yes	Yes	Yes	Yes	Yes
	OME-M 1.40.00	—	—	—	—	Yes	Yes	Yes	Yes
	OME-M 1.40.10	—	—	—	—	—	Yes	Yes	Yes
	OME-M 1.40.20	—	—	—	—	—	—	Yes	Yes

NOTE: Installing an earlier version of OME-Modular resets the configuration to factory defaults. This option allows you to maintain a certain firmware level.

Updating iDRAC with Lifecycle Controller using individual package method

1. If OME-Modular is managing a chassis group, then log in to OME-Modular interface of the Lead chassis.
2. Click **Devices** > **Compute**. A list of the available compute devices in the chassis or chassis group is displayed.
3. In the list header, select the checkbox to select all compute devices on the current page. If there are multiple pages, then go to each page and select the checkbox.
4. After selecting all the compute devices, click **Update**.
5. In the **Device Update** wizard, select the individual package and click **Browse** to select the **iDRAC with Lifecycle Controller** DUP.
6. Once the DUP is uploaded, click **Next** and select the **Compliance** checkbox.
7. Click **Finish** to start the update on all compute devices.
8. Allow the job to complete before proceeding to update the components, Dell Server BIOS PowerEdge MX740c, MX750c, MX760c, and MX840c.

NOTE:

- Updating iDRAC to 4.40.10.00 using individual DUPs from OME-M version 1.10.20 or lower does not display compliance details and may fail. Use the recommended catalog update method.
- It is recommended that you reset iDRAC before performing individual compute sled updates with iDRAC 5.x or earlier versions.

NOTE: As an alternative method for updating compute hosts and storage sleds or storage sleds only, you can implement catalog based updates once the catalogs are updated with the baseline versions. For more information, see Managing catalogs.

Updating PowerEdge MX740c, MX750c, MX760c, and MX840c Server BIOS

Repeat the steps described in the section, *Updating iDRAC with Lifecycle Controller using individual package method*, to update Dell Server BIOS PowerEdge MX740c, MX750c, MX760c, and MX840c as applicable.

Updating adapters

Download and install the operating system drivers for your device adapter that released with the device adapter firmware. Follow the device adapter driver installation instructions for your operating system.

Repeat the steps described in the section to update the following adapter firmware:

Table 5. Updating adapters

Follow the section	To update
Updating iDRAC with Lifecycle Controller using individual package method	QLogic 26XX series Fibre Channel adapters
	QLogic 27XX series Fibre Channel adapters
	QLogic 41xxx series adapters
	Broadcom 57504 Quad Port device adapter
	Mellanox ConnectX-4 Lx Ethernet Adapter Firmware
	Intel NIC Family Version 19.5.x Firmware for X710, XXV710, and XL710 adapters
	Emulex Picard-16/Picard-32 adapters

Go to dell.com to download the latest device drivers associated with the firmware update.

Updating OME-Modular to 2.00.00

You can update to OME-Modular 2.00.00 from different versions. For more information, see OME-M firmware update matrix section.

NOTE: If you select all the management modules in an MCM group, OME-M updates them in a required order.

NOTE: Updating to 1.10.x or later may result in the alert log alert HWC7522. You may have to perform a system reseat power action on the MX7116n or pass-through module (PTM) IOMs.

NOTE: If the firmware update of a member chassis is nonresponsive for more than two hours, cancel the job using **Stop Job** option on the **Job Details** page. Check the firmware update status on the member chassis directly. The **Stop Job** option would stop the firmware update on specific target which was nonresponsive and goes to the next target update. For any firmware update failures on member chassis, restart the firmware update only on the specific target from **Lead chassis**.

Best practices for updating to 2.00.00

While updating the management module to 2.00.00 from an earlier version, ensure that there are no failed template deployment jobs on the **Jobs** page. If failed deployment jobs exist, the virtual identities that are reserved for the device for those failed deployments, are added back to the free pool after upgrading to 2.00.00.

Updating management module firmware

NOTE: Ensure that you upgrade the OME-Modular firmware before upgrading OS10.

You can update the management module firmware using the following methods:

1. Individual package method—Through OME–Modular web interface or RESTful API
2. Catalog-based compliance method

To update the firmware using the Individual package method:

1. Download the DUP from the **www.dell.com/support/drivers**.
2. On the OME–Modular web interface, go to **Devices** > **Chassis** and select the chassis for which you want to update the firmware.
3. Click **Update Firmware**.
   The **Select Firmware Source** window is displayed.
4. Select the **Individual package** option and click **Browse** to go to the location where you have downloaded the DUP and click **Next**.
   Wait for the comparison report. The supported components are displayed.
5. Select the required components, for example: OME–Modular, and click **Update** to start the firmware update.
   You can schedule the update process to start at the time you want.
6. Go to the **Monitor** > **Jobs** page to view the job status.

NOTE: The console is inaccessible during the OME–Modular update process. After the OME–Modular update process, wait for the console to reach a steady state.

During MM part replacement, when the standby MM is replaced causing a firmware mismatch, an alert is displayed on the web interface with a link to synchronize MM firmware. Wait for about 15 minutes after the alert is displayed and click the link to perform the synchronization.

NOTE: Set the TLS protocol settings to **TLS 1.2 and Higher** before:

- Downgrading OME-Modular from version 2.00.00 to earlier versions.
- Performing MM part replacement and MM synchronization with modules earlier than 2.00.00.

Recovering failed Management Module firmware update process

If the firmware update of a management module (MM) fails, perform the following steps:

1. Perform a failover on the MM. If the failover fails, go to step 2.
2. Reset the active MM manually.
3. After the failover or reset is complete, check the firmware version to verify if the active MM is running the same or a later version of OME-Modular, as the standby MM. If not, perform a reset on the MM to force failover.
4. Retry the firmware update.

Upgrading Ethernet switch using DUP

WARNING: For IOMs in full-switch mode, do not select both IOMs in a redundant pair simultaneously. This action causes network outage.

NOTE: Upgrade the MX9116n and MX5108n switches only after updating the other MX7000 components to their corresponding PowerEdge MX 2.00.00 baseline versions.

NOTE: The DUP update procedure is recommended for upgrading OS10, firmware, and ONIE on the MX9116n and MX5108n switches.

NOTE: To upgrade MX9116n and MX5108n switches, see the OS10 firmware update matrix.

Upgrade time for a switch may take between 30 to 120 minutes. Sometimes the upgrade time can be up to 4.5 hours.

To check the upgrade status, you can see OME-Modular job page or you can log in to the switch and run show `smart-fabric upgrade-status`.

Upgrading networking OS10 using DUP

To upgrade OS10 using DUP, follow these steps:

1. Download the latest DUP file for the switch from https://www.dell.com/support.
2. On the OME-Modular web interface, go to **Devices** > **I/O Modules**.
3. Select the IOM module on which you must carry out the OS10 upgrade.
4. Click **Update Firmware**.
5. Select the Individual package option, and then click **Browse** and go to the location where the OS10 DUP was downloaded earlier. Wait for the compliance report, once done, the supported components are displayed.
6. Select the required components and click **Update**, to start the update.

   For upgrading from different versions earlier than 10.5.0.7, see Upgrading networking switch using different DUP versions section.
7. Go to **Monitoring** > **Jobs** page, to view the job status.

   NOTE: The new MX9116n hardware supports DUP update to OS10 version 10.5.3.1 and later. Updates on the new MX9116n hardware using IOM DUPs earlier than 10.5.3.1 are not recommended. Use OS10 binary image to update through IOM CLI.

   NOTE: If you update the OS01 DUP when all IOMs are with ONIE firmware version 3.35.5.1.23 and later, the ONIE firmware that is bundled in the DUP is upgraded automatically.

Upgrading Firmware and ONIE using DUP

NOTE: ONIE upgrade using DUP method is supported only if all the IOMs in the group are in 10.5.2.4 and later.

To upgrade ONIE using DUP, follow these steps:

1. Download the latest ONIE DUP file for the switch from https://www.dell.com/support.
2. On the OME-Modular web interface, go to **Devices** > **I/O Modules**.
3. Select the IOM module on which you must carry out the ONIE upgrade.
4. Click **Update Firmware**.

5. Select the Individual package option, and then click **Browse** and go to the location where the ONIE DUP was downloaded earlier. Wait for the compliance report, once done, the supported components are displayed.
6. Select the required components and click **Update**, to start the update.
7. Go to **Monitoring** > **Jobs** page, to view the job status.

OS10 firmware update matrix

Table 6. OS10 firmware update matrix

		To										
	OS10 version	**10.4.0E(R3SP2)**	**10.4.0E(R4SP2)**	**10.5.0.1**	**10.5.0.3P1**	**10.5.0.5**	**10.5.0.9**	**10.5.1.9**	**10.5.2.4**	**10.5.2.6**	**10.5.3.x**	**10.5.4.x**
From	**10.4.0E(R3SP2)**	—	—	—	—	—	Yes*	—	—	—	—	
	10.4.0E(R4SP2)	—	—	—	—	—	Yes*	—	—	—	—	
	10.5.0.1	—	—	—	—	—	Yes	—	—	—	—	
	10.5.0.3P1	—	—	—	—	—	Yes	—	—	—	—	
	10.5.0.5	—	—	—	—	—	Yes	—	—	—	—	
	10.5.0.7	—	—	—	—	—	—	Yes	—	Yes	Yes	
	10.5.0.9	—	—	—	—	—	—	Yes	—	Yes	Yes	
	10.5.1.6 / 10.5.1.7 / 10.5.1.9 /	—	—	—	—	—	—	—	Yes	Yes	Yes**	
	10.5.2.4	—	—	—	—	—	—	—	—	Yes	Yes	
	10.5.2.6	—	—	—	—	—	—	—	—	Yes	Yes	Yes
	10.5.3.X	—	—	—	—	—	—	—	—	—	Yes	Yes

- *—Upgrading IOM VLT peers from 10.4.X to 10.5.X version impacts traffic. Regular maintenance window is recommended for this activity.
- **—Upgrading IOM VLT pairs from 10.5.1.6 to 10.5.3.x may impact traffic due to potential VLT heartbeat service failures causing IOM reboot. Regular maintenance window is recommended for this activity.

NOTE: Run the X.509v3 certificate upgrade script before upgrading from 10.5.0.1/10.5.0.3P1/10.5.0.5/10.5.0.7 OS10 versions. See PSQN before upgrading from these OS10 versions. The upgrade script is available at https://www.dell.com/support/kbdoc/000184027/dell-emc-networking-os10-certificate-expiration-and-solution.

NOTE: Upgrading IOMs in SmartFabric mode to OS10.5.1.6 with VLAN 1 as tagged, disrupts traffic. If VLAN 1 is tagged, upgrade to OS10.5.1.7. See the release notes for complete list of fixes in OS10.5.1.7.

The number of IOMs that can be updated differs based on the IOM versions. The following table displays the number of IOMs that can be updated at a time.

Table 7. IOM Firmware update matrix

IOM Version	OME-M Version	No. of IOMs
10.5.0.5	1.10.20 or later	4
10.5.0.7/10.5.0.9	1.20.00 or later	6

Table 7. IOM Firmware update matrix (continued)

IOM Version	OME-M Version	No. of IOMs
10.5.1.X	1.20.10 or later	6
10.5.2.4 or later	1.30.00 and later	No restrictions

You must group the IOMs for firmware update depending on the type of IOM. The following table displays an example of grouping 12 IOMs for firmware update.

Table 8. Grouping IOMs for firmware update

Example of 12 IOMs	Combination	Group 1	Group 2	Group 3
10.5.0.5	6 Fabrics	Fabric 1-2	Fabric 3-4	Fabric 5-6
	12 Full switch	IOM 1-4	IOM 5-8	IOM 9-12
	4 fabrics and 4 Full switch	Fabric 1-2	Fabric 3-4	4 Full switch IOM
10.5.0.7/10.5.0.9 or 10.5.1.X	6 Fabrics	Fabric 1-3	Fabric 4-6	Not Applicable
	12 Full switch	IOM 1-6	IOM 6-12	Not Applicable
	4 fabrics and 4 Full switch	Fabric 1-3	Fabric 4 and 4 full switch IOM	Not Applicable

Once all IOMs are updated to 10.5.2.4/10.5.2.6 stack, network IOMs display two software components for update. The available options are:

- Dell Networking SmartFabric OS10
- Dell Networking ONIE Firmware

Limitations for ONIE firmware update are:

- ONIE firmware update option is available only if the OS10 version is 10.5.2.4 or later versions.
- When you select the network IOM that is part of a fabric for ONIE update, other nodes in the fabric are updated automatically.
- If you insert an old version of IOM, the ONIE firmware cannot be updated before updating OS10 to 10.5.2.4 version.

NOTE: ONIE component firmware is not updated due to the issue of system not booting into ONIE, when GRUB menu is displayed with serial control character. This issue is addressed in 3.35.1.1-15 ONIE firmware version. If ONIE update fails or encounters ONIE booting issue, retry the ONIE component firmware update.

The maximum time taken for upgrading fabrics of two or more IOMs is 4 hours 40 minutes. The time that is taken for the upgrade is based on one of the following:

- Number of IOMs chosen for upgrade
- Number of IOMs in the cluster, if all IOMs are chosen for upgrade.

Work around steps for IOM upgrade failure

- When IOMs are upgraded from 10.5.0.7 or 10.5.0.9 to 10.5.2.4 or 10.5.2.6, **Jobs** page on OME-Modular displays the job as failure, but software upgrade is successful.
- When you see job failure, run the `show smartfabric nodes` command on the IOM CLI and check if the failed IOM is in OFFLINE state.
- If the OFFLINE IOM is in: 10.5.2.4 or 10.5.2.6
  - Full switch mode—No immediate action required, it recovers automatically when Fabric manager is upgraded to the latest version.
  - Fabric mode—Restarts the IOM which is OFFLNE.
- If one of the nodes of the fabric is not upgraded due to the above failure, start upgrade job once again.

Prerequisites for upgrading from 10.5.0.7 or 10.5.0.9

- When updating, ensure to update the IOMs in groups no larger than six per upgrade job.

- If there are two switches in a full-switch mode VLT, each switch should be part of different upgrade batch for redundancy.
- If there are two switches in a SmartFabric, select only one switch. The other switch is automatically updated. This is counted as "2" in that upgrade group.

3

OME-Modular licenses

OME-Modular features are based on licenses, which are available in XML format. Following are the types of licenses supported:

- Perpetual—Validity is unlimited and is effective until the license is removed or deleted. Perpetual license is bound to the chassis service tag.
- Evaluation—Validity is for a short duration and the timer starts after the license is imported or installed. The timer is a monotonic clock that counts the time that the system is operational. The time is accumulated to a checkpoint file to ensure that the license restrictions are not bypassed. The timer stops during a firmware shutdown or reboot and resumes after the firmware is ready. An alert is displayed as the license nears expiry.

The following features in OME-Modular are available when the Advanced License is installed:

- OpenID Connect (OIDC)
- Telemetry
- RSA Multifactor Authentication
- Automatic Certificate renewal

The licenses can be downloaded from the Dell Digital Locker.

You can import and view the license details on the **Installed Licenses** page. The license type is also displayed on the **Chassis Overview** page.

Topics:

Importing licenses

You can import license files of XML format.

If you have a perpetual license for OME-Modular Advanced, you cannot import an evaluation license for OME-Modular Advanced feature.

To import a license:

1. Click **Application Settings** > **Licenses**.
   The **Installed Licenses** page is displayed.
2. Click **Import**.
   The **Import License File** window is displayed.
3. Click **Select a file** to go to the location where the license is stored.
4. Select the file and click **Open** to import the file.
   The **Import License File** window is displayed.
5. Click **Finish** to import the file.
   The imported license file is displayed on the **Installed Licenses** page.

Viewing license details

To view the license details:

On the **Installed Licenses** page, select the licenses of which you want to view the details.
The license details are displayed on the right side of the installed licenses list.

The details are—Description, Entitlement ID, License Type, and Expiration timestamp.

4

Logging in to OME-Modular

You can log in to OME–Modular as a local, Active Directory, or generic Lightweight Directory Access Protocol (LDAP) user. OME–Modular supports a maximum of two Active Directory or LDAP server configurations, each.

A security notice is displayed on the **Login** page, prompting you to verify if you are accessing the OME-Modular interface in compliance with the security policy of your organization. You can customize the security policy message for both OME-Modular web interface **Login** page and SSH. But, the default security policy is displayed only on the OME-Modular web interface **Login** page.

When using SSO, configure OME-Modular and iDRAC with FQDN to avoid issues with multiple IP addresses.

Topics:

Logging in to OME–Modular as local, Active Directory, or LDAP user

OME–Modular allows authentication for 64 local user accounts. To log in to OME–Modular as an Active Directory (AD) or LDAP user:

1. Add directory service
2. Import directory group
3. Log in with directory user credentials

For Active Directory and generic LDAP user accounts, OME–Modular allows a minimum of one user account in a simple environment and a maximum of two accounts in a complex environment.

LDAP users can perform the following tasks using OME–Modular:

- Enable LDAP access.
- Upload and view a Directory Service CA certificate.

- Specify attributes while configuring LDAP. The attributes are—LDAP server address, LDAP server port, Bind DN, Bind password, user login attribute, group membership attribute, and search filter.
- Associate an LDAP group with an existing or new management module role group.

To log in as a local, Active Directory, or LDAP user:

1. Enter the **Username**.
2. Enter the **Password**.
3. Click **Login**.

   After logging in successfully, you can do the following:
   - Configure your account.
   - Change the password.
   - Recover the root password.

Integrating directory services in OME-Modular

You can use Directory Services to import directory groups from AD or LDAP for use on the web interface. OME-Modular supports integration of the following directory services:

1. Windows Active Directory
2. Windows AD-LDS
3. OpenLDAP
4. PHP LDAP

Supported attributes and pre-requisites for LDAP Integration

Table 9. OME-Modular Pre-requisites/supported attributes for LDAP Integration

	Attribute of User Login	Attribute of Group Membership	Certificate Requirement
Windows AD-LDS	Cn, sAMAccountName	Member	• Subject to availability of FQDN in Domain Controller Certificate. SAN field can have both IPv4 and IPv6 or IPv4 or IPv6, or FQDN. • Only Base64 certificate format is supported
OpenLDAP	uid, sn	Uniquemember	Only PEM certificate format is supported.
PHP LDAP	uid	MemberUid	

User pre-requisites for directory service integration

Ensure that the following user pre-requisites are met before you begin with the directory service integration:

1. BindDN user and user who is used for 'Test connection' must be the same.
2. If Attribute of User Login is provided, only the corresponding username value that is assigned to the attribute is allowed for appliance login.
3. User who is used for Test connection must be part of any non-default group in LDAP .
4. Attribute of Group Membership must have the 'userDN' or the short name (used for logging in) of the user.
5. When MemberUid is used as 'Attribute of Group Membership,' the username that is used in appliance login is considered case sensitive in some LDAP configurations.
6. When search filter is used in LDAP configuration, user login is not allowed for those users who are not part of the search criteria mentioned.
7. Group search works only if the groups have users assigned under the provided Attribute of Group Membership.

NOTE: If OME-Modular is hosted on an IPv6 network, the SSL authentication against domain controller using FQDN would fail if IPv4 is set as preferred address in DNS. To avoid this failure, do one of the following:

- DNS should be set to return IPv6 as preferred address when queried with FQDN.
- DC certificate must have IPv6 in SAN field.

Adding Active Directory service

To add the active directory service:

1. On the OME–Modular web interface, click **Application Settings** > **Users** > **Directory Services** > **Add** > **Type of Directory**.
   The **Connect to Directory Service** window is displayed.
2. From the **Type of Directory**, select the option, **AD** or **LDAP**. The default option is **AD**.
3. Enter the **Directory Name**.
4. Select the **Domain Controller Lookup**.

   If the **Domain Controller Lookup** type is DNS and the directory type is **AD**, enter the domain name and group domain.

   For the **AD** directory type, if the **Domain Controller Lookup** type is **DNS**, enter the domain name and group domain. If the **Domain Controller Lookup** type is **Manual**, enter the FQDN or IP addresses of the domain controllers. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

   In the group domain, you can look for directory groups. You can include the directory groups as application users. You can also use the group domain for authenticating users during login. The format of the group domain can be— `<Domain>.<Sub-Domain>` or `ou=org, dc=example, dc=com`.

   Use the **DNS** domain controller lookup type, if you do not know the details of the domain controllers from which you want to import the group or groups. To use the DNS domain controller, ensure that you have done the following on the **Network Settings** page:

   - Selected the **Register with DNS** check box.
   - Provided the Primary and Alternate DNS server addresses.

   After you enter the domain name, OME-Modular searches the SRV records on the DNS servers to fetch the details of the domain controllers in that domain.

   If you know the IP address or FQDN of the domain controllers, you can use the **Manual** domain controller lookup type.

5. If the RSA SecurID is configured, select the option, **Enable**. The default option is **Disable**.
   To edit the configuration, click **RSA SecurID Configuration**.
6. Under **Advanced Options**, enter the **Server Port**. If the **Type of Directory** is **AD**, go to step 6.
   For **Server Port**, the Global Catalog Address port number, 3269 is populated by default. For the **Domain Controller** access, enter 636 as the port number.
7. Select the **Network Timeout** and **Search Timeout durations**.
8. Select the **Certificate Validation** checkbox if you want to validate the directory service certificate and select the certificate for validation.
   The certificate must be a root CA Certificate encoded in Base64 format.
   The **Test Connection** option is enabled.
9. Click **Test Connection** to check the AD connection and enter the username and password of the domain you want to connect to.

   NOTE: The username must be entered in either the UPN (username@domain) or in the NetBIOS (domain\username) format.

10. Click **Test Connection**.
    The **Directory Service Information** window, indicating a successful connection, is displayed.
11. Click **Ok** and **Finish**.
    A job is created and run to add the requested directory on the **Directory Services** page.

Adding LDAP service

To add the LDAP service:

1. On the OME-Modular web interface, click **Application Settings** > **Users** > **Directory Services** > **Add** > **Type of Directory**.

The **Connect to Directory Service** window is displayed.

2. From the **Type of Directory**, select the option, **LDAP**. The default option is **AD**.
3. Enter the **Directory Name**.
4. Select the **Domain Controller Lookup**.

   If the **Domain Controller Lookup** type is **DNS**, enter the domain name.

   If the **Domain Controller Lookup** type is **Manual**, enter the FQDN or IP addresses of the domain controllers. For multiple servers, a maximum of three servers are supported, use a comma-separated list.

   Use the **DNS** domain controller lookup type, if you do not know the details of the domain controllers from which you want to import the group or groups. To use the DNS domain controller, ensure that you have done the following tasks on the **Network Settings** page:

   - Selected the **Register with DNS** check box.
   - Provided the Primary and Alternate DNS server addresses.

   After you enter the domain name, OME-Modular searches the SRV records on the DNS servers to fetch the details of the domain controllers in that domain.

   If you know the IP address or FQDN of the domain controllers, you can use the **Manual** domain controller lookup type.

5. Enter the **Bind DN** and **Bind Password**.

   NOTE: Anonymous bind is not supported for AD LDS.

6. If the RSA SecurID is configured, select the option, **Enable**. The default option is **Disable**.

   To edit the configuration, click **RSA SecurID Configuration**.

7. Under **Advanced Options**, enter the **Server Port**, **Base Distinguished Name to Search**, **Attribute of User Login**, **Attribute of Group Membership**, and **Search Filter**.

   By default, LDAP port number of 636 is populated. To change, enter a port number.

   Enter the User attributes that are configured in the LDAP system, already. It is recommended that the attributes are unique within the selected BaseDN. Else, configure a search filter to ensure that the attributes are unique. If the combination of attribute and search filter cannot identify the user DN uniquely, the login task fails.

   The **Attribute of Group Membership** stores information about groups and members in the directory.

   NOTE: Configure the user attributes in the LDAP system that is used to query before integrating on the directory services.

   NOTE: Enter the user attributes as `cn` or `sAMAccountName` for AD LDS configuration, and `UID` for LDAP configuration.

8. Select the **Network Timeout** and **Search Timeout durations**.

   The maximum timeout duration supported is 300 seconds.

9. Select the **Certificate Validation** checkbox if you want to validate the directory service certificate and select the certificate for validation.

   The certificate must be a Root CA Certificate encoded in Base64 format.

   The **Test Connection** option is enabled.

10. Click **Test Connection** to check the LDAP connection.
11. Enter the bind user credentials of the domain that you want to connect to.

    NOTE: While testing the connection, ensure that the **Test username** is the **Attribute of User Login** value entered earlier.

12. Click **Test Connection**.
    The **Directory Service Information** window, indicating a successful connection, is displayed.
13. Click **Ok** and **Finish**.
    A job is created and run to add the requested directory on the **Directory Services** page.

Logging in to OME–Modular using the directory user credentials

To log in to OME–Modular using the directory user credentials:

From the OME–Modular login page, log in using the AD user credentials. Enter the domain name, if necessary.

Importing active directory and LDAP user groups

You can import Active Directory (AD) and LDAP groups and map them to the existing OME–Modular groups.

NOTE: Users without Administrator rights cannot enable or disable the Active Directory (AD) and LDAP users.

NOTE: When you create AD or LDAP user group and login for the first time, it automatically creates one more user with the directory member user type. This user remains in the list until you delete it manually.

To import the groups:

1. On the **Users** list page, click **Import Directory Group**.
   The **Import Directory** window is displayed.
2. From the **Directory Source** drop-down, select the source from which you want to import the AD or LDAP.
3. Under **Available Groups**, you can search for directory groups.
   In the **Find a Group** text box, enter the first few letters of the group name available in the tested directory. A list of all groups names that begin with the text you entered, is displayed below under the **GROUP NAME** column.
4. Select a group and click **>>**.
   The selected group is displayed under **Groups to be Imported**.

   To remove groups, select the check box corresponding to the group you want to remove and click **<<**.
5. Click the check box corresponding to the group and from the **Assign Group Role** drop-down, select the role that you want to assign to the group and click **Assign**.
   The users in the group under the selected directory service are assigned to the selected user roles.
6. Repeat steps 3, 4, and 5, if required.
7. Click **Import**.
   The directory groups are imported and displayed in the **Users** list. However, all users in those groups use their domain username and credentials to log in to OME-Modular.

Logging in to OME-Modular using OpenID Connect

The OpenID Connect multifactor authentication feature allows users who are registered with OpenID Connect (OIDC) Provider, to access the OME-Modular web interface. For the registration, the OIDC configuration document is first queried using a RESTful API URI. The information that is obtained from the query is used to log in to OME-Modular.

NOTE: When you log in using OpenID Connect Provider credentials, the username is displayed in the **name@ProviderName@Sub** format which may result in some extra characters with the username.

NOTE: Dell Technologies recommends that you use DNS name while configuring the OIDC server and DNS name in the discovery URI, instead of IP address. Using DNS name helps avoid limitations in some OIDC servers where dynamic client registration fails when a combination of IPv6 and initial access token is used.

Important notes

- The OpenID Connect feature is available only when the OME-Modular Advanced license is installed.
- You must have the SECURITY_SETUP privilege to add, modify, and delete OIDC Providers. You can add maximum of four OIDC Providers on OME-Modular. The **Add** option is disabled if there are already four OIDC Providers added.
- When you perform add or join chassis group operation with OIDC providers that are configured in lead or member chassis, ensure that the OIDC server is reachable from the chassis.
- If the OIDC server is not reachable, the registration status is displayed as failed even if the OIDC providers are successfully propagated from lead to member when the user authentication option is enabled. For any operations related to OIDC providers in the lead or member chassis, the communication between OIDC server and chassis must be successful.
- During the firmware upgrade process, OIDC registration may fail with which the token may expire. In this scenario, re-register the OIDC provider after the firmware upgrade process.
- OIDC users who are registered with PingFederate may have to re-register with OIDC provider, as the following actions may reset the Open ID client policy that is associated with the client to **Default.**
  - Firmware upgrade

- Change in network configuration
- Change in SSL certificate

- The re-registration process with OIDC provider might reset to the default policy that is configured in the PingFederate. To avoid security concerns post any of the re-registration events, the administrator must reconfigure all the OpenManage Enterprise Client IDs on the PingFederate site. Also, it is highly recommended that client IDs are created only for administrator users with Ping federate until this issue is resolved.

NOTE: When you downgrade the management module firmware from 1.30.10 to 1.30.00, the verified OpenID Connect user details are not retained.

Following are the predefined roles that must be configured in the OIDC Provider for OIDC users to log in to OME-Modular:

Table 10. Predefined roles

Roles in OME-Modular	Roles in OIDC Provider	Description
CHASSIS_ADMINISTRATOR	CA	Can perform all tasks on the chassis.
COMPUTE_MANAGER	CM	Can deploy services from a template for compute sleds and perform tasks on the service.
STORAGE_MANAGER	SM	Can perform tasks on storage sleds in the chassis.
FABRIC_MANAGER	FM	Can perform tasks that are related to fabrics.
VIEWER	VE	Has read-only access.

To log in to OME-Modular using OpenID Connect:

1. On the **Login** page, click **Login with OpenID**.
2. Enter your username and password to log in. Once your login credentials are authenticated, you are redirected to the **OME-Modular Login** page.

Adding OpenID Connect Provider

To add an OIDC Provider:

1. On the **Application Settings** > **Users** > **OpenID Connect Providers** page, click **Add**.
   The **Add New OpenID Connect Provider** window is displayed.
2. Enter a **Name** and **Discovery URI** for the OIDC Provider.
3. Select the **Authentication Type**.
   The available options are:
   - Initial Access Token
   - Username

   If the **Authentication Type** is **Initial Access Token**, then go to step 4. Else, go to step 5.
4. Enter the **Initial Access Token**.
5. If the **Authentication Type** is **Username**, enter the **Username** and **Password** for the OIDC Provider.
6. Select the **Certificate Validation** check box.
   The **Certificate** option is displayed.
7. Click **Browse** to go to the location where the certificate is stored or drag and drop the certificate in the marked area to upload it.
8. Click **Test Connection** to check if the URI and SSL connection works.
9. Select the **Enabled** check box to use the OIDC Provider to log in to OME-Modular. By default, the **Enabled** check box is selected.

Editing OpenID Connect Provider

Registered users can edit or modify the details including name, discovery URI, authentication type, and other information. A new job carries out the changes and end user can poll the job status.

To edit an OpenID Connect Provider:

1. On the **OpenID Connect Providers** page, select the OIDC details that you want to edit and click **Edit**.
   The **Edit OpenID Connect Provider** window is displayed.
2. Make the required changes and click **Save**.

Enabling OpenID Connect Provider

To enable an OpenID Connect Provider:

1. On the **OpenID Connect Providers** page, select the OIDC provider that you want to enable and click **Enable**.
   A message is displayed prompting you to confirm to proceed with enabling the OIDC provider.
2. Click **OK** to proceed.

Disabling OpenID Connect Provider

To disable an OpenID Connect Provider:

1. On the **OpenID Connect Providers** page, select the OIDC provider that you want to enable and click **Disable**.
   A message is displayed prompting you to confirm to proceed with disabling the OIDC provider.
2. Click **OK** to proceed.

Deleting OpenID Connect Provider

You can delete one or more OIDC providers simultaneously.

To delete an OIDC provider:

1. On the **OpenID Connect Providers** page, select the OIDC provider that you want to enable and click **Delete**.
   A message is displayed prompting you to confirm to proceed with deleting the OIDC provider.
2. Click **OK** to proceed.

   In MCM environment, if you delete OIDC providers in the lead chassis, the delete job details are also displayed in the member chassis.

   If a delete OIDC provider job in the member chassis fails, you must log in to the member chassis to delete the OIDC provider.

After you delete an OIDC provider, the option to log in to OME-Modular using OIDC Providers, is not displayed.

OME-Modular home page

When you log in to OME–Modular, the home page is displayed. The menu bar at the top of the OME-Modular user interface displays the following:

- Name of the application at the top-left corner
- Search text box
- Number of jobs
- Number of alerts
- User name of the logged in user
- Help icon
- Information icon

The home page displays a dashboard with high-level information about the system and the subcomponents.

You can also view the job activity and events. To view the job activity, click  and to view events, click  .

To return to the OME–Modular home page, click the OME–Modular logo or click **Home**.

- **Chassis graphical view**—On left of the page, a graphical view of the front and rear chassis is displayed. It shows all the modules (sleds, fans, power supplies, IOMs, and MMs) present in the chassis. A hover over on each module displays a brief description and health status of the module. Click **View Devices** to see more details about the modules present in the chassis. Click **View Slot Information** to switch the display of the widget to slot information list.

- **Slot information view**—On the upper left corner of the page, a list of modules present on the chassis is displayed showing slot information, health status and a link that goes into details. Modules in this list include compute, storage sleds, and IOMs. Click **View Inventory** to see more details about the modules present in the chassis. Click **View Chassis Image** to switch the display of the widget to chassis graphical view.
- **Chassis Information**—On the left center of the page, you can view a summary of the chassis information such as FIPS status, name, model, service tag, asset tag, express service code, Management IP, firmware version, power state, faceplate power, power cap, power redundancy, location, and licenses.
- **Group Information**—On the lower left corner of the page, you can view the summary of chassis group. Group information includes, group name, lead chassis name, lead chassis service tag, lead chassis IP, redundancy, backup chassis name, backup chassis service tag, backup chassis IP, and backup sync status.
- **Chassis Subsystems**—On the upper right corner of the page, you can view the health of the chassis subsystem components—battery, fan, IOM slot, MM, miscellaneous, power supply, temperature, compute sleds and storage sleds. . When the subsystem status is unhealthy, you can click in the **Reason** to view the list of fault messages.
- **Recent Alerts**—On the top center of the page, you can view the most recent alerts for events occurring in the chassis. Click **View All**, to see all the alerts in the **Alerts** page.
- **Recent Activity**—Below the **Recent Alerts** widget, you can view the most recent activities occurring in the chassis. Click **View All**, to view all the activities or jobs in the **Jobs** page.
- **Environment**—On the lower right corner of the page, you can view the power and temperature details of the chassis. Click **View Power Usage** to the view the details of the power usage by the chassis on the **Hardware** page. Click **View Power Statistics** to view information such as the current redundancy state, peak headroom, peak power, timestamp, minimum power, and system energy consumption timestamp. Click **View Temperature Statistics** to view the temperature information—duration, peak temperature timestamp, and minimum temperature timestamp.

NOTE: When you refresh inventory and power on the chassis after you perform complete AC/DC power cycle, the inventory of the compute sled and IOM may be displayed after three to five minutes.

NOTE: If chassis has not been powered on after the complete AC/DC power cycle operation, the inventory status is displayed as **unknown**.

NOTE: The maximum number of browser connections is limited to three connections per domain. Launching the console multiple times within the same browser result in an error. Close all the unused sessions and refresh the page.

Search feature in OME-Modular

The search feature enables you to look for information about jobs, devices, alerts, links, alert policies, users, and audit logs. The feature works in English only and is case insensitive. You can search for records as you type. For example: If you are looking for alerts and start entering the word, OME-Modular suggests the matching terms.

The search feature supports:

- A maximum of 255 characters including special characters.
  - Supported special characters—#, @, %, -, :, =, &, $, +, |, /, ., _,(, and)
  - Unsupported special characters—*, <, >, {,}, ^, ~, [,], `, ;, ?, ", \, and ‘

  However, the search feature does not support the special characters— **,**,****, **_**, **%**, **#**, **'**, **)**,**+**, and **&** for usernames. For instance, if you create a username with the unsupported special characters and search for it, the username is not displayed on the **Users** page.

  NOTE: The search feature does not support spelling errors.

  You can use the special characters as prefix and suffix of the search text. For example, if you are looking for a device by ID, but you know only part of the device ID, you can search for the device using a wildcard character in beginning and end of the ID—*911*. The results matching the search are displayed below the search text box.
- Incremental search—Results are displayed as you type the search text. For example, if start typing "con.." to look for configuration records, the relevant entries are displayed in the form of a list.
- Multiple words like an "OR" condition—Search words are separated by spaces. Examples:
  - Use the terms, service tag or IDs to look for devices by service tags or IDs.
  - Use the terms firmware or alerts to look for tasks that are related to firmware updates.
- Wildcard search—OME-Modular supports suffix and prefix wildcard search for records. If you are looking for a specific model of a device, but you know only part of the model, for example, 5108, you can enter the partial information. A search is run using the wildcard characters as—Prefix and suffix—*5108*

  NOTE: For a group of input search strings that are separated by space, the wildcard search is applicable only to the last string. For example: str1 str2 str3 str4 is treated as str1 str2 str3 *str4*.

The most relevant results are displayed in a list. Click **Show More** to the view all the records. Select or clear check boxes of the components which you want to include or exclude from the search results. By default, all the options are selected. Click a search result record to go to the **Alerts Log** page.

You can use the search feature as described in the following examples:

- Search for jobs using Job IDs.
- Search for devices using the MAC address of the device as the search text.
- Search for alerts using parts of the alert message such as Message IDs.
- Search for IP addresses.
- Search audit log for information from logs.

You can use fields that are displayed on the OME-Modular pages to search for information using the search feature. The fields are listed in the following table.

Page name	Fields
Jobs	• Name • Description • Enabled/Disabled • Last Run Status • Created By/Updated By

Alert Log	• Message
	• Category
	• Definition
	• Severity
	• Status
	• Device
	  ○ Model
	  ○ Identifier
	  ○ Type
	  ○ Device Management—MAC Address, Network Address, Device Name, and Discovery Profile

Audit Log	• Category • IP Address • Message • Message Interface • Severity • User Name
Help	• Title • Content
Alert Policy	• Name • Description • Enabled/Disabled
Users	• Type • Directory Server Type • Name • Description • Email • Enabled/Disabled
All Devices	• Global Status • Model • Identifier • Type • Power State • IP Address • Asset Tag

Page name	Fields
	• Associated Chassis Service Tag • Inventory • Location—Description, Name, Details • Software—Description, Instance ID, PCI Device ID, Software Type, Status, Sub Device ID, Sub Vendor ID, Vendor ID, Version • License—Assigned Device, Entitlement ID, Description, License Type
Device Management Info	• MAC Address • Network Address • Device Name • Discovery Profile

Viewing alerts

The **Alerts** section displays the specific types of alerts such as Critical, Warning, and Unknown. You can also view alerts for specific device types such as chassis, compute, networking, and storage.

Viewing jobs and activities

The **Recent Activity** section displays a list of recent jobs and activities, and their status. Click **All Activity** to go to the **Jobs** page and view detailed information about the jobs.

Multi-chassis management dashboard

Multiple chassis are grouped to form domains called Multi-Chassis Management (MCM) groups. An MCM group can have 20 chassis, where one is the lead and the remaining 19 are members. OME–Modular supports wired MCM groups where the chassis are daisy-chained through a redundant port on the management controller.

In a multi-chassis management (MCM) group, the number of events and jobs for the entire group is displayed. The **Device Health**, **Alerts**, and **Recent Activity** sections display the consolidated details of all the devices in the group.

In an MCM group with network IOMs, it is recommended to designate the chassis which contains network IOMs as lead chassis and a backup lead.

NOTE: Maintain a minimum interval of two minutes between removing and inserting each device.

Viewing MCM home page

You can view the following information about the MCM group:

- MCM group—You can view:
  - Name of the group
  - Name, IP address, and service tag of the lead chassis
  - Name, IP address, and service tag of the member chassis

You can perform group-related actions from the dashboard. Click **Actions** to:

- View Topology
- Take Chassis Group Backup
- Add/Remove Member
- Designate Backup Lead
- Edit Group
- Delete Group
- **Device Health**—Displays the health status of the chassis subsystems—chassis, compute sled, networking, and storage. You can click the health status of the individual devices or click **All Devices**, to view a summary of the devices in the **All Devices** page.

- **Recent Alerts**—Displays the most recent alerts for events occurring in the lead chassis and the subsystems. Click **All Alerts**, to view the **Alerts** page for the lead and member chassis.
- **Recent Activity**—Displays the most recent activities occurring in the lead chassis and the subsystems. Click **All Activity**, to view the **Jobs** page for the lead and member chassis.

NOTE: If a member chassis is added to a chassis group based on a "Join Group" request from the member chassis, the status of the member chassis is displayed as "Unknown" for some time, on the MCM dashboard.

Viewing lists of chassis in an MCM group

On the OME–Modular home page, the list of chassis that are part of the group is displayed on the left. The list displays the model, IP address, and the Service Tag of the chassis. The lead chassis is labeled for easy identification. Click the name of the chassis to access the details specific to the chassis. You can also use the listed IP address to directly access the OME–Modular web interface of the chassis.

Viewing device health

The **Devices** > **All Devices** page displays the health summary of the chassis, compute and storage sleds, and networking components.

A list of all the devices at the bottom of the **All Devices** page. You can select a device to view its summary on the right side of the list. You can sort the list using **Advanced Filters**.

From the **Filter by** dropdown, select the device type to view only the required list of devices. The available options are:

- All
- Chassis
- Compute
- I/O Modules
- Storage

You can also perform the following tasks on the **All Devices** page:

- Power control
- Update firmware
- Blink LED
- Refresh inventory
- Extract Logs

NOTE: When you initiate a **Leave Chassis Group** request while the inventory refresh is in-progress, an error message is displayed on the **All Devices** page even if the **Leave Chassis Group** task is successful.

NOTE: When a compute sled is inserted into a chassis, sometimes the message, "No device image found", is displayed. To resolve the issue, refresh the inventory of the compute sled, manually.

NOTE: When you refresh inventory and power on the chassis after you perform complete AC/DC power cycle, the inventory of the compute sled and IOM may be displayed after three to five minutes.

Setting up chassis

When you log in to the OME–Modular web interface for the first time, the configuration wizard is displayed. If you close the wizard, you can access it again by clicking **Configure** > **Initial Configuration**. This option is displayed only if the chassis is not yet configured.

To configure the chassis:

1. Log into OME–Modular.
   The **Home** page is displayed.
2. Click **Configure** > **Initial Configuration**.
   The **Chassis Deployment Wizard** is displayed.

   For further steps, see Initial configuration.

Initial configuration

Dell Technologies recommends the following configuration threshold for better performance of the chassis. If the configuration exceeds the threshold, then some features including firmware update, backup, and restore may not work as expected. It may also affect system performance.

Component	Count
Templates	320
Alert Policy	50
Identity pool	501
Network (VLAN)	214
Catalog	50
Baseline	50

To configure a chassis:

1. Click **Devices** > **Chassis** > **View Details** > **Configure** > **Initial Configuration**.
   The **Chassis Deployment Wizard** is displayed.
   NOTE: You can configure the chassis using an existing chassis profile.
2. In the **Import Profile** tab, click **Import** to open the **Import Profile** window.
   Enter details of the network share, where the chassis profile is located and click **Import**.
3. In the **Time Configuration** tab, select the **Configure Time Settings** to configure the time zone and timestamp of the configuration.
4. Select the **Use NTP** check box to configure the NTP Server 1, NTP Server 2, and NTP Server 3 addresses and click **Next**.
   NOTE: It is recommended that at least three valid NTP servers, which synchronize to a single time source, are used to ensure reliable synchronization.

   If you select multiple NTP servers, OME–Modular selects the NTP server algorithmically.

   If you have an existing NTP server and configure a new NTP server, the audit log is created for both NTP1 and NTP 2 servers.

   While configuring an NTP, ensure that all NTPs are in the same time zone.

   The **Activity and Alerts** tab is displayed.
5. Configure the email, SNMP, and system log settings and click **Next**.
   The **iDRAC** tab is displayed.
6. Select the **Configure iDRAC Quick Deploy Settings** check box to configure the password to access the iDRAC web interface and the management IP, and click **Next**.

   You can select the slots to which the iDRAC Quick Deploy settings must be applied.

   The **Network IOM** tab is displayed.
7. Select the **Configure I/O Module Quick Deploy Settings** check box to configure the password to access the IOM console and management IPs, and click **Next**.
   The **Firmware** tab is displayed.
8. Select the **Configure all devices to use following catalog** check box, select the network share type and, click **Catalog** to open the **Add Firmware Catalog** window.
9. Enter a name for the catalog, select the catalog source, and click **Finish** to save the changes and return to the **Chassis Deployment Wizard**.
10. Click **Next** to view the **Proxy** tab and configure the proxy settings.

    OME–Modular uses the proxy settings to access the Dell website for the latest catalogs. You can also enable the HTTPS proxy settings and proxy authentication.
11. Click **Next** to view the **Group Definition** tab.
12. Select **Create Group** to configure the chassis group settings.
13. Click **Next** to view the **Summary** tab.

NOTE: After setting the time in the lead chassis, wait for the lead chassis time and the member chassis time to synchronize before performing any operation. The time configuration can be disruptive.

Configuring chassis settings

You can configure the following settings for a chassis:

- Power
- Network
- Network Services
- Local Access Configuration
- Location
- Quick Deploy

Configure chassis power

To configure the chassis power settings:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Power**.
   The **Power** configuration section is expanded.
2. Select **Enable Power Cap** to specify the maximum power consumption capacity for the chassis. The **Power Cap** limits the power consumption of the chassis. When the power cap is reached, the sleds are throttled based on their power priority. You can specify the capacity in Watts, BTU/h, or percentage. The **Power Cap** option is displayed only if the **Enable Power Cap** check box is selected. The recommended power cap is 0 to 32767 Watts or 0-100 %. If you change the power cap in BTU/h, the power cap in W also changes.

   MX7000 chassis supports both AC and DC power supply input types.
3. In the **Redundancy Configuration** section, select the required redundancy policy.

   Power redundancy policies facilitate management of power consumption and power failure tolerance in the chassis. The available options are:
   - **No Redundancy**—This policy distributes the enclosure power load across all PSUs. There are not any specific PSU population requirements for **No Redundancy**. The intent of the **No Redundancy** policy is to have the highest possible limit for power enablement of devices that are added to the enclosure. If there are single or multiple PSU failures, and then the enclosure limits the performance to operate within the power capabilities of the remaining PSUs.
   - **Grid Redundancy**—This policy distributes the enclosure power load across all PSUs. The six PSUs are organized into two groups: Grid A consists of PSUs 1, 2, 3, and Grid B consists of PSUs 4, 5, 6. It is recommended that the PSUs are populated in the following order: 1, 4, 2, 5, 3, 6, where an equal number of PSUs on each grid is optimized for Grid Redundancy. The grid with the largest PSU capacity determines the limit for power enablement of devices that are added to the enclosure. If there is a grid or PSU failure, and then the enclosure power is distributed among the remaining PSUs with the intent that a single healthy grid continues to provide power to the system without degrading the performance.
   - **PSU Redundancy**—This policy distributes the enclosure power load across all PSUs. There are no specific PSU population requirements for redundant PSUs. PSU redundancy is optimized for a population of six PSUs, and the enclosure limits the power enablement of devices to fit within five PSUs. If there is a single PSU failure, the enclosure power is distributed among the remaining PSUs without degrading the performance. If there are fewer than six PSUs, the enclosure limits the power enablement of devices to fit within all populated PSUs. If there is a single PSU failure, the enclosure limits the performance to operate within the power capabilities of the remaining PSUs.
4. In the **Hot Spare Configuration** section, select the **Enable Hot Spare** to configure the Hot Spare primary grid.

   The Hot Spare feature facilitates voltage regulation when power utilization by Power Supply Unit (PSUs) is low, considering the total output capacity of the PSU. By default, the Hot Spare is enabled. When the Hot Spare is enabled, a redundant PSU is put in sleep state when the power utilization is low. The Hot Spare is not enabled if the:
   - PSU redundancy is inactive.
   - Power budget of the system configuration exceeds the PSU output capacity.
   - Grid Redundancy Policy is not selected.

   The MX7000 PSUs support the Hot Spare feature with three PSU pairs. The feature enables a PSU pair to have one active PSU and one PSU in sleep mode while the enclosure power consumption is low, and the three PSU pairs meet all the power requirements for the enclosure. This enables efficient power utilization when the overall enclosure power requirement is low. The partner PSU wakes the paired PSU from sleep mode by sending a WAKE signal when the enclosure power requirement increases. The PSU pairs for MX7000 are PSUs: 1 & 4, 2 & 5, and 3 & 6.

5. From the **Primary Grid** dropdown, select the PSU Grid that hosts the Hot Spare Active PSUs. Grid 1 consists of PSU slots 1, 2, 3, and Grid 2 consists of PSU slots 4, 5, 6.
6. Click **Apply** to save the chassis power settings.

Configure chassis management network

You can configure the network settings for the management modules that are inserted into an MX7000 chassis.

- LAN or NIC interface
- IPv4
- IPv6
- DNS Information
- Management VLAN

To configure the chassis network:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Network**.
   The **Network** configuration section is expanded.
2. In the **General Settings** section, you can enable or disable NIC, **Register with DNS**, and **Auto Negotiation**. By default, the **Enable NIC** check box is selected.

   If you enable **Register with DNS**, and then enter the **DNS Name** of the chassis that you want to register with a DNS server. You can access OME-Modular using the existing FQDN even after the **Register with DNS** option is disabled in the application. This is because the earlier option remains in the Network cache or the DNS Server cache that is based on the configured Time to live (TTL).

   NOTE: You can only access the FQDN temporarily.

   NOTE: Clear the cache in the DNS after the **Register with DNS** is disabled, to prevent logging in with the FQDN address.

   NOTE: If the **Register with DNS** option is enabled, you cannot modify the **Enable VLAN** option.
3. Enter the **DNS Name**. The DNS name can have a maximum of 58 characters. The first character must be an alphanumeric character (a-z, A-Z, 0-9), followed by numeric characters or a hyphen (-).
4. Enable or disable the **Auto Config DNS Domain Name** option and turn the **Auto Negotiation** on or off.

   Enable the **Auto Config DNS Domain Name** check box to use DHCPv4, DHCPv6, or Router Advertisement to obtain the domain name. If the **Auto Config DNS Domain Name** is disabled, enter the **DNS Domain Name**.

   NOTE: You can enable **Auto Config DNS Domain Name** only if IPv4 DHCP or IPv6 **Auto Negotiation** is enabled.

   If **Auto Negotiation** is false or disabled, you can choose network port speed.

   NOTE: Setting **Auto Negotiation** to false and choosing a network port speed may result in the chassis losing link to the network switch in Top of Rack, or to the neighbor chassis, if running MCM. It is recommended that the **Auto Negotiation** is set to true for most use cases.

Table 11. Top of the Rack Support Matrix for management module and management module uplink

Top of the Rack Switch Configuration	Management Module Configuration	Supported for Management Module Uplink (YES or NO)
100 Mbps (Auto negotiation OFF)	100 Mbps (Auto negotiation OFF)	YES
10 Mbps (Auto negotiation OFF)	10 Mbps (Auto negotiation OFF)	YES
Auto Neg ON	Auto Negotiation ON	YES
100 Mbps (Auto negotiation OFF)	Auto Negotiation ON	NO
10 Mbps (Auto negotiation OFF)	Auto Negotiation ON	NO
Auto Negotiation ON	100 Mbps (Auto negotiation OFF)	NO

Table 11. Top of the Rack Support Matrix for management module and management module uplink (continued)

Top of the Rack Switch Configuration	Management Module Configuration	Supported for Management Module Uplink (YES or NO)
Auto Negotiation ON	10 Mbps (Auto negotiation OFF)	NO

5. In the **IPv4 Settings** section, configure the following:
   - **Enable IPv4**
   - **Enable DHCP**
   - **IP Address**
   - **Subnet Mask**
   - **Gateway**
   - **Use DHCP to Obtain DNS Server Addresses**
   - **Static Preferred DNS Server**
   - **Static Alternate DNS Server**
6. In the **IPv6 Settings** section, configure the following:
   - **Enable IPv6**
   - **Enable Autoconfiguration**
   - **Address Generation Mode**
   - **IPv6 Address**
   - **Prefix Length**
   - **Gateway**
   - **Static Preferred DNS Server**
   - **Static Alternate DNS Server**

   NOTE: If IPv6 Auto Configuration is enabled, OME-Modular uses the DNS information if available through Router Advertisement (RA). Also, OME-Modular tries to obtain the DNS information through DHCPv6 if the Other Config or Managed flag is set in the RA. OME-Modular uses a maximum of three DNS server in the below order of priority IPv4 static, IPv6 static, IPv4 DHCP, IPv6 DHCP, and IPv6 RA.

   The static IPv6 IP address that is already configured is applied and displayed in OME-Modular when the configuration is changed from static to Autoconfiguration.

   Use DHCPv6 to Obtain DNS Server Addresses is no longer available. DHCPv6 addresses are obtained based on the presence of managed flag in Router Advertisement only. DNS server address is obtained using DHCPv6 based on the presence of **Managed** or **OtherConfig** flag in the Router Advertisement.
7. Enable or disable the VLAN for the chassis. You can configure the VLAN settings only if the **Register with DNS** check box is cleared.

   You can change from a VLAN network to a non-VLAN network, or move from a non-VLAN network to a VLAN network, only if **Register with DNS** check box is cleared.

   By default, the IPv4 settings are enabled and the DNS registration is disabled with a default name. You can modify the name using any local interfaces such as OpenManage Mobile.

   NOTE: Ensure that the network cable is plugged to the correct port when you modify the VLAN state for the change to be effective.

   Isolate the chassis management from the data network as the uptime of a chassis that is improperly integrated into your environment cannot be supported or guaranteed. Due to the potential of traffic on the data network, the management interfaces on the internal management network are saturated by traffic that is intended for servers. It results in OME–Modular and iDRAC communication delays. These delays may cause unpredictable chassis behavior, such as OME–Modular displaying iDRAC as offline even when it is up and running, which in turn causes other unwanted behavior. If physically isolating the management network is impractical, the other option is to separate OME–Modular and iDRAC traffic to a separate VLAN. OME–Modular and individual iDRAC network interfaces can be configured to use a VLAN.

   NOTE: Any change in the attribute settings leads to IP drop or unavailability of the OME–Modular web interface for some time. However, the OME–Modular web interface recovers automatically.
8. Click **Apply** to save the chassis network settings.

Configure chassis network services

The chassis network services configuration consists of SNMP, SSH, and remote RACADM settings.

To configure network services:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Network Services**.
   The **Network Services** section is expanded.
2. In the **SNMP Settings** section, select the **Enabled** check box to enable the SNMP settings and select the **Port Number**.
   The port number can be 10 to 65535.
   NOTE: For SNMP operations, configure the timeout parameter on the client to facilitate successful completion of the task. You may have to adjust the timeout parameter based on the network latency.
3. Select the SNMP **Protocol** version from the drop-down. The available options are:
   - All (v1/v2/v3)
   - SNMP v3
4. In the **User-Configuration (SNMP Read-Only)** field, click **SNMP v3 Users** to configure the SNMP v3 users.
   The **SNMP v3 User Configuration** window is displayed.
   For steps to configure SNMP v3 users, see Configuring SNMP v3 users.
5. Enter the SNMP **Community Name**. The length of the community name must be less than or equal to 32 characters.
   The community name is applicable only to the SNMP versions 1 and 2.
6. Download the **Management Information Base (MIB) file** for SNMP, to a local drive on your system.
   Remove the old MIBs in the SNMP MIB tool before loading the new ones.
7. In the **SSH Settings** section, select the **Enabled** check box to enable the SSH settings for the chassis and select the maximum number of SSH sessions.
   By default, a chassis can have a maximum number of four SSH sessions.
8. Select the **Max Auth Retries** to specify the number of retries when the SSH session fails. By default, the maximum number of auth retries is three, which can be increased up to nine.
9. Select the **Idle Timeout**, in seconds, for which the SSH session can remain idle. The SSH session expires based on inactivity timeout configuration, and the default idle timeout is 30 minutes. When there is a change in the chassis management network, all active sessions that are listed on the User Sessions page are not terminated automatically.
   The default value or minimum value for max auth retries is three, and the maximum value is nine.
   NOTE: The audit logs are not generated when the session expires based on idle timeout.
10. Select the SSH **Port Number**. The port number can be 10 to 65535.
    The default port number is 22.
11. Enable the remote RACADM session for the chassis.
    You can view the remote RACADM option on the web interface only if you have the chassis administrator privilege.
    NOTE: A log for remote RACADM session (login or logout) is displayed in the **Audit Logs** page, irrespective of the remote RACADM status. If the remote RACADM option is disabled, the feature does not work.
    NOTE: Any change in the attribute settings leads to IP drop or unavailability of the OME–Modular web interface for some time. However, the OME–Modular web interface recovers automatically.
12. Click **Apply** to save the chassis network services settings.

Configuring SNMP v3 users

You can configure up to five SNMP v3 users.

To configure SNMP v3 users:

1. Select the **ENABLED** check box.
2. Enter the **USERNAME**.
   NOTE: The username can be 16 characters long and must be a combination of an uppercase, a lowercase, and a number. It must not contain any white space.

3. Select the **AUTHENTICATION TYPE** as **MD5** or **SHA** and enter the authentication passphrase.
4. Select the **PRIVACY TYPE** as **DES** or **AES** and enter the privacy passphrase.
5. Click **Finish** to save the changes and close the **SNMP v3 User Configuration** window.

Configuring OME-Modular to use command line consoles

This section provides information about the OME-Modular command line consoles (serial or SSH console) features. For details about setting up the system to perform systems management tasks using the console, see the white paper, https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/servers-solution-resources_white-papers22_en-us.pdf. For information about using RACADM commands in OME-Modular through the command line console, see *Dell OpenManage Enterprise Modular for PowerEdge MX7000 Chassis RACADM Command Line Reference Guide*.

OME-Modular command line console features

OME-Modular supports the following serial and SSH console features:

- RACADM support
- Integrated connect command connecting to the serial console of servers and I/O modules; also available as `racadm connect`
- Maximum of four SSH sessions
- Minimum of three and maximum of nine authentication retries for the SSH session

OME-Modular command line commands

When you connect to the OME-Modular command line, you can enter these commands:

Table 12. OME-Modular command line commands

Command	Description
`racadm`	RACADM commands begin with the keyword `racadm` followed by a subcommand. For more information, see *Dell OpenManage Enterprise Modular for PowerEdge MX7000 Chassis RACADM Command Line Reference Guide*.
`connect`	Connects to the serial console of a server or I/O module. For more information, see *Dell OpenManage Enterprise Modular for PowerEdge MX7000 Chassis RACADM Command Line Reference Guide*. **NOTE:** You can also use the racadm `connect` command.
`exit`, `logout`, and `quit`	All the commands perform the same action. They end the current session and return to a login prompt.

To end a session:

- On systems running Windows as the client host, use the keys, [Ctrl]+[A] [Ctrl]+[X].
- On systems running Linux as the client host, use [Ctrl]+[A] [Ctrl]+[A] [Ctrl]+[X].

To end a binary session in the OME-Modular serial console, use the keys, [Ctrl] +]. For IOMs, use [Ctrl] + \.

To end a nonbinary session login to OME-Modular interface, and go to **All Devices** > **Chassis** > **Overview** > **Troubleshoot** and click **Terminate Serial Connection**.

Configure local access

You can configure chassis power button, Quick Sync, KVM, LCD, and chassis USB direct accesses for a chassis.

To configure the local access settings in a chassis:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Local Access Configuration**.
   The **Local Access Configuration** section is expanded.
2. Select **Enable Chassis Power Button** to turn the chassis off or on.

If the check box is cleared, you cannot change the power state of the chassis using the chassis power button.

3. Select the **Quick Sync access** type.

   The available options are:

   - Read-only—Enables you to only view the information. You cannot apply the configuration changes.
   - Read-write—Enables full capabilities for Quick Sync 2, including changing the system settings.
   - Disabled—Disables Quick Sync 2 module.

   NOTE: The Quick Sync feature uses a lower radio frequency (RF) power when advertising and increases the RF power after the certificate authentication. The RF range is based on the environment and can vary.

4. Select **Enable Inactivity Timeout** to enable the idle timeout and enter the **Timeout Limit**.

   The Timeout limit is the time period after the last activity for which the Quick Sync module remains active. Specify inactivity timeout limit, in seconds or minutes. The timeout can be between two minutes (120 s) and 60 minutes (3600 s).

   NOTE: The **Timeout Limit** option is available only if the **Enable Inactivity Timeout** is selected.

5. Select **Enable Read Authentication** to enter user credentials to use Quick Sync functionality.

   By default, this option is selected. If you clear this check box, you can read the server health and log data. But, use must authenticate to change the system configuration.

   When the option is selected, you have to authenticate before reading the system information. When the option is not selected, you can read the system information without authenticating but prompts you to authenticate to change the system configuration.

6. Select **Enable Quick Sync Wi-Fi** to use Quick Sync 2 WiFi to activate as required to support specific use cases. If the WiFi is disabled, Quick Sync 2 WiFi cannot be activated and functionality that requires Quick Sync 2 WiFi will not be available. Quick Sync 2 BLE may remain active. By default, the **Enable Quick Sync Wi-Fi** check box is selected.

   NOTE: The mobile device activates WiFi to support specific features. Otherwise, it remains inactive even when a device is connected through Quick Sync 2 BLE.

7. Select **Enable KVM Access** to configure the settings using KVM. You can also use the RACADM or Redfish command to enable or disable KVM. For more information, see the *Dell OME - Modular for PowerEdge MX7000 Chassis RACADM Command Line Reference Guide* available at https://www.dell.com/openmanagemanuals.

   You can use the DisplayPort in the chassis to stream the video in the KVM. If the external DP to Video Graphics Array (VGA) converter is available, you can stream the KVM video in the VGA too.

8. Select the **LCD Access** option.

   The available options are:

   - Disabled
   - View Only
   - View and Modify

   NOTE: The **LCD Access** option is displayed only if there is a system with LCD available in the chassis.

9. In the **User Defined** text box, enter the text that you want to see on the LCD Home screen. The LCD Home screen is displayed when the system is reset to factory default settings. The text can have a maximum of 62 characters and supports a limited number of UTF-8 characters. If a UTF-8 character that is used in the text is not supported, a box is displayed instead of the character. The default string is the service tag of the system.
10. From the **LCD Language** drop-down, select the language in which the text on the LCD must be displayed.

    The available options are:

    - English
    - French
    - Spanish
    - German
    - Japanese
    - Chinese

    By default, the text is displayed in English.

11. Select the **Enable Chassis Direct Access** text box to enable accessing the MX7000 chassis from a host such as a laptop or server, using a USB On-The-Go (OTG) cable.

    If the **Enable Chassis Direct Access** check box is cleared, the existing chassis direct sessions are disconnected and the Chassis Direct LED turns off. When the feature is disabled, you cannot connect the laptop to the chassis. The URL

`https://ome-m.local` is inaccessible. After enabling the feature, reattach the USB cable and wait for Chassis Direct LED to turn green to access the chassis phonebook. For more information, see the section, Chassis Direct.

12. Click **Apply** to save the settings.

Chassis Direct

The Chassis Direct feature in OME-Modular enables users to access management consoles such as iDRAC and management module of devices on the chassis. The MX7000 chassis has several USB ports. The Right Control Panel (RCP) on the front of the chassis has three USB ports. Two ports are regular sized USB-A ports, for keyboards and mouse used for the chassis level KVM. The third port is a Micro-AB port that supports USB OTG. To use Chassis Direct, connect the USB OTG port to a laptop. The processor on the management module emulates a USB network interface and provides a network bridge into the management VLAN. The network is same that Quick Sync 2 bridges for OpenManage Mobile Wi-Fi access.

When network time protocol setting is not enabled, RCP replacement does not restore system time. The real-time clock on the new RCP is used as system time of the lead chassis and the same gets synced to all member chassis. This action may result in member OME-Modular reboot and MM redundancy loss for some time. Redundancy should be restored successfully after few minutes.

Remove the USB cable that is connected to the front panel and perform complete AC or DC power cycle the chassis.

With the system that is connected to the USB OTG port on the chassis, you can access the MM user interface and iDRAC user interface or KVM. You can get access by launching a browser on the laptop and entering the URL, `https://ome-m.local`. A chassis phonebook page which contains a list of entries to the available devices on the chassis, is displayed. This option provides a better experience than the front panel KVM, which provides access only the command-line prompt access for OME-Modular.

Select the check box to enable accessing the MX7000 chassis from a host such as a laptop or server, using a USB On-The-Go (OTG) cable. Connect the USB OTG cable from the host to the micro USB port on the front panel (right control panel) of the MX7000 chassis. On successful connection, LED under the micro-USB on the right control panel of MX7000 chassis turns green and USB Ethernet adapter is displayed on the host. The chassis is automatically configured with an IPV4 and IPV6 address. After ensuring that the addresses are configured, open a web browser and enter the URL, `https://ome-m.local` in the address bar.

On laptops running Windows, if the IPV6 traffic is blocked, check the Remote Network Driver Interface Specification (RNDIS) interface for IPv6 address. You may be able to access chassis phonebook page through IPv4, but iDRAC and OME-Modular web consoles are inaccessible. In that case, enable IPv6 traffic flow on the system.

When you enable or disable the Chassis Direct feature in OME-Modular, the following error codes are displayed:

The Chassis Direct feature in OME-Modular has a mutual exclusivity with the Quick Sync feature. Before downgrading the management module firmware from 1.10.00 version to an earlier version, remove the USB cable that is connected to the front panel of chassis. If USB cable is not removed and 1.10.00 firmware is downgraded, the Quick Sync feature may be degraded. Perform complete AC or DC power cycle of chassis to restore Quick Sync back to health.

Table 13. Chassis Direct—LED blink status and description

Error code	Chassis Direct LED blink status	Description and resolution
1	Amber	The USB network link is down as the Chassis Direct feature is disabled. **Resolution**—Enable the Chassis Direct and reattach the USB cable to access the chassis phonebook.
2	Amber	The USB network link does not come up as the chassis internal USB operation failed. **Resolution**—If the issue persists, reattach the USB cable to the laptop or perform complete AC or DC power cycle of the chassis.
3	Amber	The USB network link fails to come up owing to an issue on the host laptop. **Resolution**—If the issue persists, reattach the USB cable.

Table 13. Chassis Direct—LED blink status and description (continued)

Error code	Chassis Direct LED blink status	Description and resolution
4	Turned off	The USB network link is down as the USB cable is disconnected. **Resolution**—Reattach the USB cable for the link to come up.

If the Chassis Direct feature is disabled and the USB cable is inserted, the Chassis Direct LED turns amber and the alert, USR0197, is displayed on the OME-Modular web interface. You can see the alert only if you have logged in to OME-Modular using the public network. If you repeat the action within a short interval, the alert is not displayed. However, the Chassis Direct LED remains amber as the MM suppresses consecutive duplicate alerts.

NOTE: While using Internet Explorer to access the phonebook page, a custom certificate larger than 46 Kb results in TLS error. Change the certificate or use a different browser.

NOTE: If you have a custom certificate that is uploaded on 1.40.xx and you downgrade the OME-Modular to earlier version, downgraded chassis restores the self-signed certificate. Manually upload a custom certificate in the chassis.

Diagnose Chassis Direct connection

If you are unable to establish a secure connection with `ome-m.local` from your web browser using Chassis Direct, it may be because of your web browser safety features. For example, macOS integrated security settings prevents you from accessing a website that it does not consider it as secured. The error messages can vary depending on the browser, it may display "can't establish a secure connection to the server" on Safari, and "Revoked Certificate" on Google Chrome. You can resolve this issue either by uploading a trusted SSL web certificate to the Management Module UI or accepting the SSL certificate of the `ome-m.local`.

Obtaining the SSL certificate of the `ome-m.local`.

- Go to the `ome-m.local` and click lock icon on the address bar.
- Select **View/Show Certificate** and then click **Details**.
- Verify and save the certificate on your device.

Installing SSL certificate of the `ome-m.local` to Keychain Access application on the macOS.

- Go to the **Keychain Access** application on the macOS and click **Certificates**.
- Drag and drop the downloaded certificate into the **Keychain Access Certificates** screen.

Setting preference on the **Keychain Access** application to accept the SSL certificate of the `ome-m.local` .

- Double-click the downloaded certificate to set the system preference.
- Expand the **Trust** option and select **Always Trust** preference for the certificate.

Configure chassis location

To configure the location of the chassis:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Location**.
   The **Location** configuration section is expanded.
2. Enter the location names for the **Data Center**, **Room**, **Aisle**, and **Rack**.
   The **Data Center**, **Room**, **Aisle**, and **Rack** support up to 128 characters.
3. Enter the number of the **Rack Slot** and the name of the **Location** where the rack is located.
   The **Rack Slot** supports 1-255 numeric characters.
   The **Location** supports up to 128 characters. It is supported for backward compatibility. The Data Center, Aisle, Rack, and Rack Slot properties replace this property. Use these properties to describe the physical location of the chassis.
4. Click **Apply** to save the location settings.

Configure Quick Deploy settings

The **Quick Deploy** feature enables you to configure the password to access the iDRAC user interface, IOMs, and IPv4 and IPv6 settings. These settings can be applied to existing compute sleds or IOM devices immediately. You can apply the **Quick Deploy** settings to compute sleds when they are inserted into the chassis, later. However, you cannot apply the **Quick Deploy** settings to IOMs that are inserted later.

When you insert a new sled into an empty slot with only quick deploy settings that are configured, it only creates an audit log instead of deployment and configuration job.

Quick deploy settings are validated when the job is run. If an invalid parameter is used, the quick deploy job fails. The **Quick Deploy** job parameters are not evaluated, as they can contain any value, which is delegated while running the job.

Enabling and disabling quick deploy is a web interface feature to determine if the controls are enabled to configure **Quick Deploy** settings. The back-end only processes requests from the web interface.

NOTE: After the quick deploy settings are applied to the compute sled, the IP configuration is displayed in the OME–Modular web interface, when the inventory is refreshed.

NOTE: When IPv4 for IPv6 is disabled for MXG610s IOMs, the Device IPv4 address or Device IPv6 address is blank on the **Quick Deploy** page for IOMs. However, for network IOMs, the IPv4 and IPv6 device addresses are **::** and **0.0.0.0**.

To configure the **Quick Deploy** settings:

1. Click **Devices** > **Chassis** > **View Details** > **Settings** > **Quick Deploy**.
   The **Quick Deploy** configuration section is expanded.
2. Enter and confirm the password to access the iDRAC user interface.
   The password can be up to 20 characters in length.
   NOTE: If any iDRAC IP configuration is modified, the SSO for the SLEDs is functional from the OME-Modular console only after the default inventory task or manual inventory refresh is complete.
3. In the **Management IP** section, select **IPv4 Enabled** to enable the IPv4 network settings and select the **IPv4 Network Type**.
   The available options are:
   - Static
   - DHCP
4. Enter the **IPv4 Subnet Mask** and **IPv4 Gateway**.
   NOTE: The **IPv4 Subnet Mask** and **IPv4 Gateway** options are displayed only if the **IPv4 Network Type** is "Static" .
5. Select **IPv6 Enabled** to enable the IPv6 network settings and select the **IPv6 Network Type**.
   The available options are:
   - Static
   - DHCP
6. If the **IPv6 Network Type** is Static, select the **IPv6 Prefix Length** and enter the **IPv6 Gateway**.
7. From the list of slots that is displayed, select the check box next to the slot number to which you want to apply the **Quick Deploy** settings.
8. In the **Network IOM Settings** section, enter and confirm the password to log in to the IOM interface.
9. Select **IPv4 Enabled** to enable the IPv4 network settings and select the **IPv4 Network Type**.
   The available options are:
   - Static
   - DHCP
10. Enter the **IPv4 Subnet Mask** and **IPv4 Gateway**.
    NOTE: The **IPv4 Subnet Mask** and **IPv4 Gateway** options are displayed only if the **IPv4 Network Type** is "Static".
11. Select **IPv6 Enabled** to enable the IPv6 network settings and select the **IPv6 Network Type**.
    The available options are:
    - Static
    - DHCP
12. If the **IPv6 Network Type** is Static, select the **IPv6 Prefix Length** and enter the **IPv6 Gateway**.

13. Click **Apply** to save the **Quick Deploy** settings.

Managing chassis

You can view the list of chassis and the chassis details on the **Chassis** page. The details are—health, power state, name, IP address, service tag, and model of the chassis. You can also select a chassis to view the graphical representation and summary of the chassis, on the right side of the **Chassis** page.

You can also perform the following tasks on the **Chassis** page:

- Control chassis power
- Update firmware
- Blink LED
- Refresh chassis inventory
- Filter the chassis list

NOTE: When a chassis is power cycled, the inventory of the compute sleds and IOMs may be displayed in the OME–Modular web interface after three to five minutes.

NOTE: Maintain a minimum interval of two minutes between removing and inserting each device.

NOTE: After a chassis power off, the compute SLEDs are polled based on the event from the chassis. Each event from the chassis triggers a health-poll. You may see multiple connection loss events from compute SLEDs.

Creating chassis filters

You can sort the list of chassis that are displayed on the **Devices** > **Chassis** page, using filters.

To create filters:

On the **Chassis** page, click **Advanced Filters** to view the filter options.
The following options are displayed:

- **Health**
- **State**
- **Name Contains**
- **IP Address Contains**
- **Service Tag Contains**
- **Model**

Viewing chassis overview

On the chassis **Overview** page, you can click **View Slot Information** to view the compute sled slot details. A graphical representation of the chassis is displayed on the left side. Information about the chassis is displayed below the graphical representation. The information includes FIPS status of the chassis, name, model, service tag, asset tag, express service code, management IP, firmware version, power state, and faceplate power of the chassis. Click **View Devices** to view the list of all devices on the **All Devices** page.

You can also see information under the following sections:

- **Chassis Subsystems**—Displays the health status of the chassis components such as battery, fan, IOMs, and power supply.

  Fabric Consistency Check (FCC) information and health change is displayed under **Chassis Subsystems**. But the FCC details of the compute sled are not displayed in the chassis graphical representation and the compute **Overview** page.

- **Environment**—Displays the power consumption units and temperature of the chassis. Click **View Power Statistics** to view the chassis power consumption details such as current redundancy state, peak headroom, and system energy consumption. Click **Reset** to reset the power statistics and start monitoring period. Click **Power Usage** to view the chassis power supply information about the **Chassis** > **Hardware** > **Chassis Power Supplies** page. If a failover or management module reboot is performed, the last reset power statistics timestamp is updated based on the failover or management module reboot timestamp.

Click **View Temperature Statistics** to view information such as the duration, date, and time when temperature details recording began, peak temperature, timestamp, minimum temperature, and timestamp. Click **Reset** to reset the temperature statistics and start monitoring period.

NOTE: The power consumption value for compute sled device is rounded off and may display lesser than minimum power.

NOTE: The temperature statistics timestamp remains unchanged after a failover or management module reboot.

- **Recent Alerts**—Displays the number and details of the tasks that are performed in the chassis. Click **View All** to view the list of all alerts that are related to the compute sled on the **Chassis** > **Alerts** page.
- **Recent Activity**—Displays the status of the jobs that are performed in the compute sled.
- **Server Subsystems**—Displays a summary of information about the server sub systems. The information includes the health status of the components such as battery, memory, processor, and voltage.

If you have the Chassis Administrator privileges, you can perform the following tasks in this tab:

- **Power Control** tasks:
  - **Power Off (Non-graceful)**—Turns off the chassis power, which is equivalent to pressing the forceful power button when the chassis is turned on. This option is disabled if the chassis is already turned off. It does not notify the server operating system.
  - **Power Cycle System (Cold Boot)**—Turns off and then restarts the chassis forcefully (cold boot). This option is disabled if the chassis is already turned off.

    In the command-line interface, the power cycle action results in a graceful restart of the chassis.

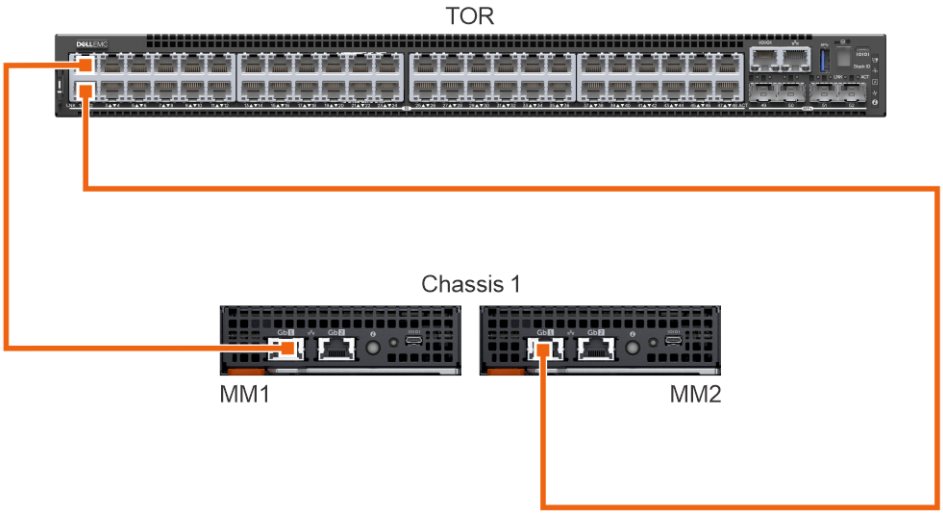
    NOTE: When the chassis is power cycled all devices in the chassis are also powered cycled. The management module does not get power cycled. However, the alerts logged may report that the connectivity was lost due to a power cycle operation.
  - **Power Off (Graceful)**—Notifies the server operating system to turn off the chassis. This option is disabled if the chassis is already turned off.
- Configuration tasks:
  - **Create Chassis Group**
  - **Join Chassis Group**
  - **Initial Configuration**
- Troubleshooting tasks:
  - Extract Log
  - Diagnostic Commands
  - Reset management module
  - Terminate serial connection
- Turn-on or turn off LEDs using **Blink LED**.
- Back up, restore, export chassis profile, and perform failover.

NOTE: After a chassis power off, the compute SLEDs are polled based on the event from the chassis. Each event from the chassis triggers a health-poll. You may see multiple connection loss events from compute SLEDs.

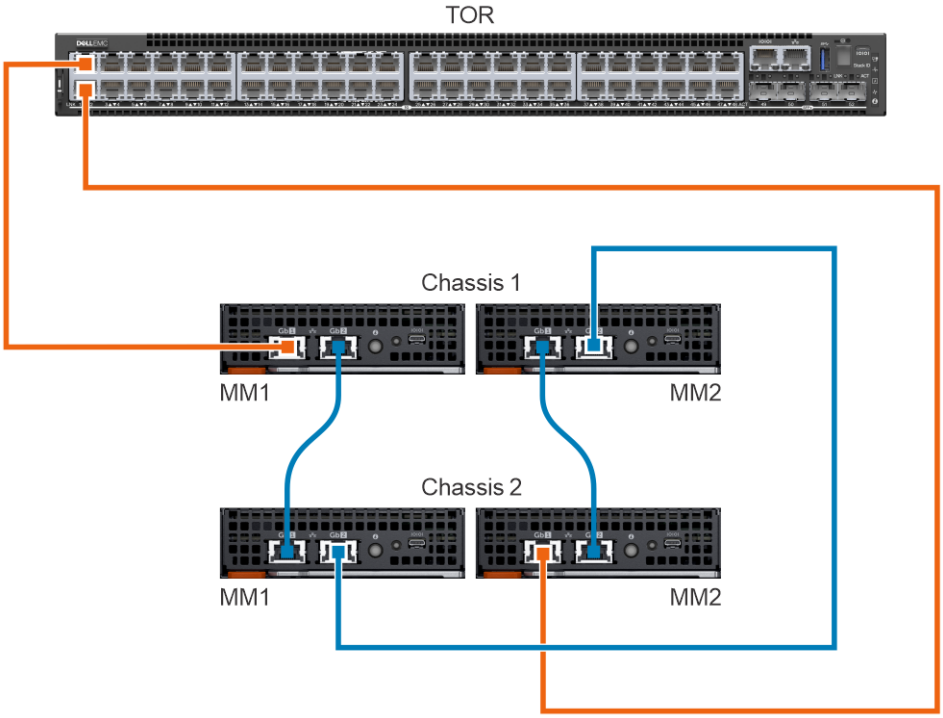
Wiring chassis

The automatic uplink detection and network loop prevention features in OME-Modular facilitate connection of multiple chassis with cables. The wiring saves port usage in the data center switches and access each chassis in the network. The cabling or wiring of chassis in this way is called stack.

While wiring a chassis, connect one network cable from each management module to the Top of Rack (ToR) switch of the data center. Ensure that both the ports on the ToR are enabled and are in the same network and VLAN. The following image is a representation of the individual chassis wiring:



The following image is a representation of the two-chassis wiring:



Chassis groups

You can group many chassis to form a multichassis management (MCM) group. An MCM group can have one lead chassis and 19 member chassis. You can use any management module to create an MCM group. The management module that is used for creating the MCM is the leader of the group, by default. The MCM group is of wired type, where the chassis is daisy-chained or wired through a redundant port on the management module. The chassis that you select for creating the group must be daisy-chained to at least one chassis. You can view a list of wired chassis and select all or the required number of chassis for creating the MCM group.

NOTE: You must have the chassis administrator privilege to create an MCM group.

You can perform the following tasks using an MCM group:

- View the health of the MCM group and the member chassis.
- Automatically apply settings of the leader chassis to member chassis.
- Perform any chassis operation on the MCM group.

You can add member chassis to an MCM group in two ways:

- Automatic—Enables automatic inclusion of the member to the chassis group. The automatic inclusion process does not require approval from the chassis administrator.
- Manual—Mandates approval by the chassis administrator to include the member chassis to the chassis group.

NOTE: PowerEdge MX740c, PowerEdge MX750c, PowerEdge MX760c, and PowerEdge MX840c platforms provides the Group Manager functionality through the OpenManage Enterprise Modular console. For these platforms, it is not recommended to use Group Manager feature as it may cause delayed response from iDRAC and failures during iDRAC firmware update.

Prerequisites for creating a wired group

Following are the prerequisites to create a wired or daisy-chained chassis group:

- List of wired daisy-chained chassis—All the chassis must be on the private stack. You need not enter a password as the machine to machine authentication trust is used.
- Ensure that you have added member chassis to the group using the automatic or manual method.
- Ensure that the chassis settings are selected for applying to the other chassis—Power, user authentication, alert destination, time, proxy, security, network services, local access.
- Ensure that Auto Negotiation is set to true in all the chassis that are connected to form an MCM group. For more information, see Configuring chassis network.
- Before stacking the chassis for creating a group or adding new members to the existing group, ensure that all the chassis have the same OME-Modular firmware version.

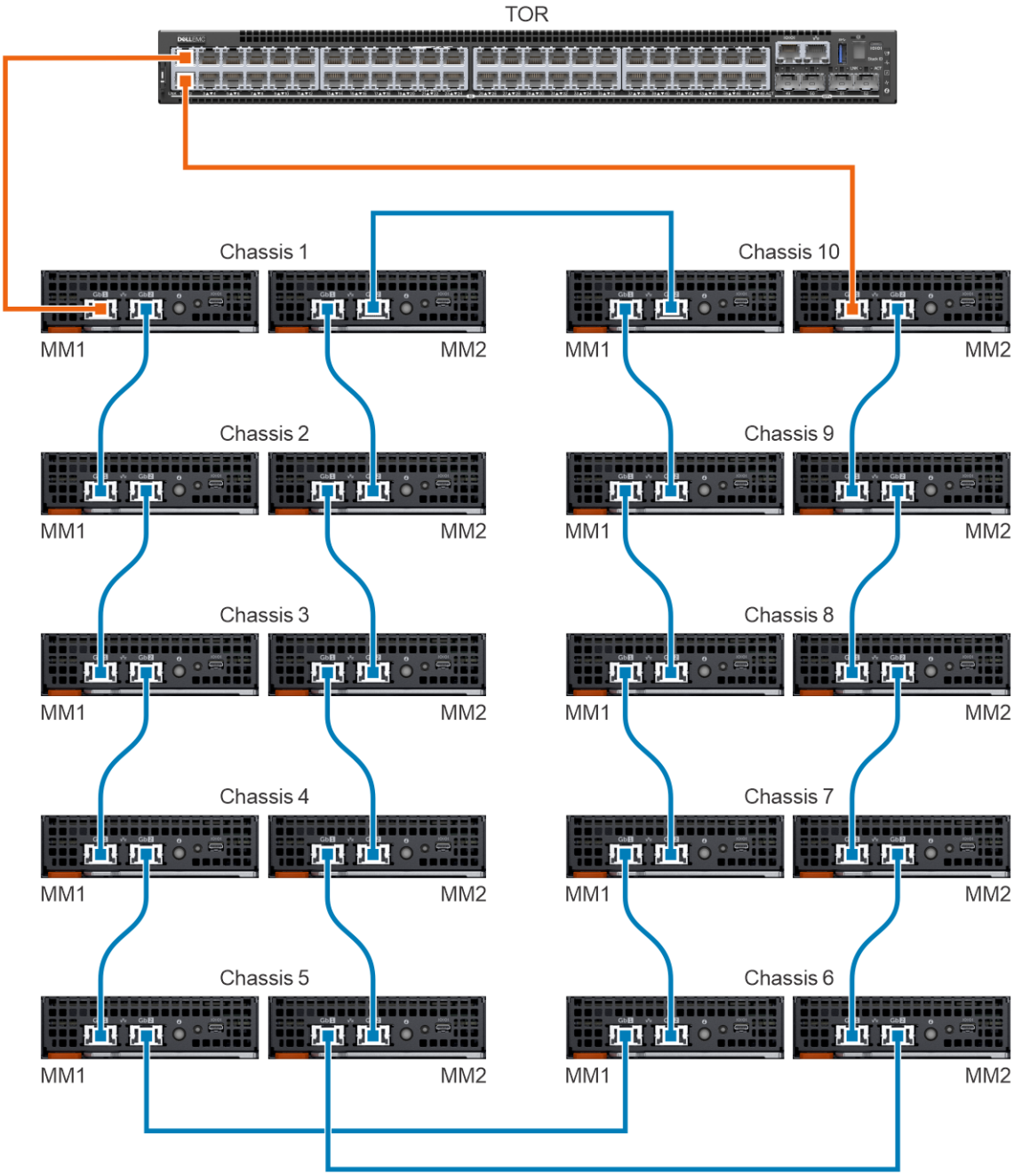
Before creating an MCM group, ensure that the MX7000 management networks are wired together in a stacked configuration. The stacked configuration helps in surviving:

- A single network cable failure
- A single management module failure
- Power loss owing to any chassis in the stack
- Failover of a chassis in the stack

NOTE: If any of the issues that are listed above occur, the management network access to all components in the daisy-chained group may be interrupted for up to 10 minutes. The OME - Modular web interface recovers automatically.

The wired chassis are displayed as under **Available Chassis** in the **Group Deployment Wizard**.

The following image is a representation of the recommended MCM wiring:



Creating chassis groups

To create a chassis group:

1. On the chassis dashboard, click **Overview** > **Configure** > **Create Chassis Group**.
   The **Create a Group and Configure Lead Chassis** wizard is displayed.
2. Enter a name and description for the chassis group you want to create.
   The group names can contain letters and numbers and must be fewer than 48 characters. However, the group names cannot contain spaces and special characters.
3. Select the onboarding permission type.
4. Select the configuration settings that you want to propagate to the member chassis.
   The settings are:
   - All—Applies all settings of the lead chassis to the member chassis
   - Power—Cap, redundancy, compute sled priority
   - User Authentication—Directory services, local users

- Alert Destination—Email, SNMP trap, system log
- Proxy Settings—All settings
- Security Settings—Login IP range, log on lockout policy
- Network Services—SNMP, SSH, remote RACADM, web server
- Local Access Configuration—Chassis power button, Quick Sync, KVM, LCD, serial access
- Session Inactivity Timeout Configuration—Session Inactivity Timeout

  NOTE: Time settings from the lead chassis are synced automatically to all the member chassis in the stack.

5. Click **Next** to view the summary of the group.

   The dashboard of a leader chassis displays a summary of the health information, recent activity, and recent alerts of the member chassis. You can select a member chassis to view its details.

   The current membership ID of the chassis is displayed on the left side.

Adding member chassis to groups

You can add members to the chassis groups from:

- **Overview** page of the lead chassis or from the member chassis.
- **Group Configuration** option from the MCM dashboard.

Adding member chassis from lead chassis

To add a member chassis to the group from the lead chassis:

1. On the lead chassis **Overview** page, click **Configure** > **Add member**.
   The **Modify Group Members** window is displayed. The discovered chassis are displayed under **Available chassis**.
2. Select the number of chassis that you want to add to the chassis group and click **Add**.
   The list of added chassis is displayed at the bottom of the window.
3. Click **Finish**.

Adding individual chassis to chassis groups

To add an individual chassis to the chassis group:

1. On the chassis **Overview** page, click **Configure** > **Join Chassis Group**.

   NOTE: **Join Chassis Group** job fails when the Management Module firmware is downgraded to an earlier version.

   The **Join Group** window with all the existing MCM groups in the stack is displayed.
2. Select the chassis or MCM group to which to want to add the member, from the **Select a Group** drop-down.
3. Click **Finish**.

   If the MCM group is created with manual on boarding policy, the join request is displayed in the pending list. The lead chassis must confirm the addition of the member chassis. The lead chassis can approve or reject the request.

   If the MCM group is created with automatic on boarding policy, no approval is required from the lead chassis. The individual chassis is automatically added to the MCM group to become a member chassis.

4. Log in to the lead chassis and approve the request of the member chassis to join the chassis group.

Removing chassis from the chassis groups

To add an individual chassis to the chassis group:

1. On the chassis **Overview** page, click **Configure** > **Add member**.
   The **Modify Group Members** window is displayed. The discovered chassis are displayed under **Available chassis**.
2. Select the chassis from the **Current Members** list.
3. Click **Remove Chassis**.
4. Click **Finish**.

NOTE: When a chassis has MX9116n or MX5108n IOM installed and its role changes from standalone to member or member to standalone, the IOM reboots, irrespective of the IOM operating mode. However, if the role of the chassis changes from lead to standalone or standalone to lead, the IOM does not reboot.

Assigning backup lead

In a multichassis environment, the lead chassis may sometimes fail temporarily or retire. In such situations, it is necessary to nominate a member chassis in the MCM group as a backup to the lead chassis. The backup lead chassis can be promoted as a lead chassis when the existing lead chassis fails or retires. In an MCM group with network IOMs, it is recommended to designate the chassis which contains network IOMs as lead chassis and a backup lead. For more information, see Promoting backup chassis as lead section.

1. On the MCM dashboard, click **Actions** > **Designate Backup Lead**.
   The **Edit Backup Lead Settings** window is displayed.

   If a backup is already assigned, the name of the backup chassis is displayed in the **Current backup** field.
2. From the **Assign backup** drop-down, select the name of the member chassis that you want to select as the backup lead chassis.
3. Select the **Backup Sync Failure Alert Timeout** from the drop-down.

   The available options are:
   - 5 Minutes
   - 10 Minutes
   - 15 Minutes
   - 30 Minutes
   - 60 Minutes
4. Click the **Lead Virtual IP Configuration (Optional)** and **Additional Information** to view details about enabling the virtual IP. The details are:
   - **Modifying the network settings may impact the virtual IP configuration**
   - **Disabling the NIC will also disable the virtual IP**
   - **Disabling IPv4 will not disable the virtual IP**
   - **Enabling VLAN will leave the virtual IP accessible only within the specified VLAN**
   - **Enabling/disabling DHCP for IPv4 will reconfigure the virtual IP to match the new subnet mask and gateway**

   Also, see the section, Use case scenarios.

   When a job for assigning a member chassis as the backup lead is stopped, the status of the job on the **Jobs** page is displayed as **Stopped**. However, the member chassis is assigned as the backup lead of the group.
5. Select the **Enable Virtual IP** check box and enter the **Static IPv4 address**.

   The virtual IP, if configured, facilitates consistency in the IP when the lead chassis role is transferred from one chassis to another.

Promoting backup chassis as lead

You can promote the backup chassis as the new lead chassis when the existing lead chassis fails. If the initial lead chassis is available, you can also assign it as a member chassis. To promote the backup chassis as the lead chassis, you must log in to the backup chassis.

After promoting a backup lead as lead chassis:

- Refresh all the compliance reports for baselines that are created for all devices.
- Detach and reattach any profiles that are attached to a slot containing a compute sled, in the new lead. Detaching and reattaching the profiles ensures that the assignment is persistent. The "promote" task does not affect profiles that are assigned to empty slots. Also, see the section, Use case scenarios.

1. On home page of the backup chassis, click **Configure** > **Promote As Lead Chassis**.
   The **Promote As Lead Chassis** window is displayed.
2. Click **Promote**.

After promoting the backup lead as the new lead of the chassis group, if you have the chassis administrator privileges, perform the following steps before putting the old lead chassis back into the production environment:

1. From the new lead chassis, remove the old lead chassis from the group to remove all references to the old lead chassis.
2. Remove the old lead chassis from the stacking network.
3. Run a forced reset configuration action by using the REST API, `URI:/api/ApplicationService/Actions/ApplicationService.ResetApplication` For details, see the *OpenManage Enterprise and OpenManage Enterprise - Modular Edition RESTful API Guide*.

   The reset configuration task transitions the old chassis to a stand-alone chassis and ready to be part of the production environment.

When a backup lead is promoted as the lead chassis, join requests from other member chassis sent to the earlier lead chassis, are not displayed on the MCM dashboard of the new lead. As a result, the particular member chassis cannot send joining requests to other groups in the stack. To unblock the pending requests, run the following API from the member chassis from which the joining requests were sent and resend the requests:

URI—`/api/ManagementDomainService/Actions/ManagementDomainService.DeletePendingDomains`

Method—`POST`

Payload—`empty`

Retiring lead chassis

You can use the retirement process of the existing lead chassis to make it a member chassis of the existing group or a stand-alone chassis.

1. On the MCM dashboard, click **Configure** > **Retire Lead Chassis**.
   The **Retire Lead Chassis** window is displayed.
2. Select one of the following options:
   - Make it a member of the current group.
   - Make it a stand-alone chassis.
3. Click **Retire**.

   Also, see the section, Use case scenarios.

   Any existing firmware baselines on the old lead chassis are imported to the new lead during retire, and a firmware compliance check job is initiated. The old lead is on-boarded after the compliance check for imported firmware baselines is completed owing to rediscovery ordering of chassis during retire. The ordering excludes the devices in the old lead chassis from the baseline report. To resolve this limitation, rerun the compliance check on the promoted lead after the retire job is completed so that the old lead devices are listed in the compliance or baseline report.

   After the retire lead task is completed, the system runs some internal tasks to complete the association of the groups that may take some time. Discrepancies, if any, occur for the devices information after the retire lead task is completed, they are reconciled automatically after the internal tasks are complete.

   After you retire a lead chassis, refresh all the compliance reports for baselines that are created for all devices.

Edit chassis groups

To edit a chassis group:

1. On the chassis dashboard, click **Overview** > **Configure** > **Edit Group**.
   The **Edit Chassis Group** wizard is displayed.
2. In the **Define Group** pane, edit group name and description for the chassis group you want to edit.

   The group names can contain letters and numbers and must be fewer than 48 characters. However, the group names cannot contain spaces and special characters.
3. Select the configuration settings that you want to propagate to the member chassis and click **Next**.

   The settings are:
   - All—Applies all settings of the lead chassis to the member chassis
   - User Authentication—Directory services, local users
   - Network Services—SNMP, SSH, remote RACADM, web server
   - Alert Destination—Email, SNMP trap, system log
   - Local Access Configuration—Chassis power button, Quick Sync, KVM, LCD, serial access
   - Power—Cap, redundancy, compute sled priority

- Proxy Settings—All settings
- Security Settings—Login IP range, log on lockout policy
- Session Inactivity Timeout Configuration—Session Inactivity Timeout

The **Add Members** pane is displayed.

4. You can add or remove the chassis as required. Select the chassis from the available chassis list and click **Add Chassis**.
5. Click **Finish**.

Delete groups

To delete a chassis group:

1. On the chassis dashboard, click **Overview** > **Configure** > **Delete Group**.
   The **Delete Group** wizard is displayed.
2. Click **Confirm** to delete the group.

MCM dashboard

The MCM dashboard is displayed only when a multichassis management (MCM) group is created. You can view the name of MCM group on the left side of the dashboard. Below the group name, you can view the names, IPs, and service tags of the lead and member chassis. The lead chassis is indicated as the "LEAD" on the right side of the chassis name, and the backup chassis is indicated as "BACKUP".

Click **Actions** to perform group-related actions.

You can perform the following actions:

- View Topology
- Take Chassis Group Backup
- Add/Remove Member
- Designate Backup Lead
- Edit Group
- Delete Group

The mid section of the MCM dashboard displays the health summary of all chassis, compute, networking, and storage devices in the MCM group. You can view the list of all the devices in the group by clicking **All Devices** at the upper right corner of the dashboard.

Below the health summary, you can view the alerts that are based on criticality of the alert and device type. Click **All Alerts** to view the list of the alerts that are related to all events in the MCM group.

You can view the details of the recent activities that are related to the group on the right side of the dashboard. The details consist of the name and status of the activity, and timestamp of the activity. Click **All User Initiated Activity** to view a list of all the activities that are related to the group, on the **Jobs** page.

Controlling chassis power

You can turn on and turn off the chassis power supply from the OME–Modular home page.

If you turn off the chassis manually or a power grid failure results in turning off multiple chassis, IOMs, and compute sleds, then, turning on all the chassis and compute sleds may result in failed inventory jobs for two to three hours. However, the inventory jobs recover with no impact to the chassis and related components.

To control the chassis power:

1. On the home page, click **Power Control** and select the required option.
   The available options are:
   - Power Off (Non-graceful)
   - Power Cycle System (Cold Boot)
   - Power Off (Graceful)

     NOTE: After login, wait for 7 minutes, if the IP is unavailable, then check if:
     - The cable is connected.

- DHCP is configured, ensure that the cable is connected to a Top of Rack (TOR) switch that has connectivity to the DHCP server.

A message is displayed prompting you to confirm your action.

2. Click **Confirm** to proceed.

Backing up chassis

The chassis backup feature allows you to take backup of the chassis configuration for later use. You must have administrator access with the device configuration privilege to take chassis backup. The chassis configuration contains the following settings:

- Application settings
  - Setup configuration
  - Power configuration
  - Chassis network configuration
  - Local access configuration
  - Location configuration
  - Slot configuration
  - OME-Modular network settings
  - Users settings
  - Security settings
  - Alert settings
- System configuration
  - Templates
  - Profiles
  - Identity pools and VLANs
- Catalogs and baselines
- Alert policies
- SmartFabric
- MCM configuration
- SSL certificates

You can restore the backed-up configuration in the same or other chassis. Backup and restore operation is not supported for the member chassis. You can only take backup of the lead chassis or the stand-alone chassis.

Create a backup file whenever a significant change is made to the chassis group. The changes include adding a chassis, removing a chassis, retiring a lead, adding a backup lead, or removing a backup lead. Failure in taking a new backup may result in the restore process not completing. Also, a complete tear down of the chassis may be required to proceed.

NOTE: **Backup Chassis** and **Restore Chassis** operations are supported in FIPS enabled configuration. The FIPS attribute is not part of backup files by default, you must switch to the required FIPS mode before initiating the restore operation.

NOTE: The backup lead configuration and virtual lead IP are not restored as they are not part of the backup file.

To create a chassis backup:

1. On the chassis **Overview** page, click **More Actions** > **Backup**.
   The **Chassis Backup** window is displayed.
2. On the **Introduction** section, read the process and click **Next**.
   The **Backup File Settings** section is displayed.
3. In **Backup File Location**, select the **Share Type** where you want to store the chassis backup file.
   The available options are:
   - CIFS
   - NFS
   - HTTPS
4. Enter the **Network Share Address** and **Network Share Filepath**.
5. Enter a name for the **Backup File**.
   The backup file name should not contain file extension. It can contain alphanumeric characters and the special characters, hyphen (-), period (.), and underscore (_).
6. If the **Share Type** is CIFS, enter the **Domain**, **User Name**, and **Password**. Else, go to step 9.

7. Click **Test Now**, if the network connection is not tested.
8. If the **Share Type** is HTTPS, **Certificate Verification** option is displayed. Select the checkbox to check the web server certificate authentication.
9. In the **Sensitive Data**, select the **Include Passwords** check box to include passwords while taking the backup. These passwords are encrypted and are applied when the backup file is restored on the same chassis. For more information, see Sensitive data section.
10. Select the **Include SSL Certificates** checkbox to include the certificate information.
11. In the **Backup File Password**, enter the **Encryption Password** and **Confirm Encryption Password**.

    The backup file is encrypted and cannot be edited.

    NOTE: The password must be 8 to 32 characters long and a combination of an uppercase, a lowercase, a special character (+, &, ?, >, -, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l) , and a number.

12. In the **Backup Schedule**, select the **Backup Frequency**.

    The available options are:

    - Automatic
    - Manual

    If you select the backup frequency as **Automatic** , select the intervals and time for backup process.
13. In the **Ethernet Switch Backup Instructions**, select the check box to confirm the backup settings. For more information about IOM backup, see Ethernet switch backup instructions section.

    NOTE: Chassis backup is not supported on some Ethernet switch settings. The settings include Hostname, Password, Management network, Spanning tree configurations, IOMs that are in full switch mode, and some CLI configurations. For the list of CLI configurations that are not supported, see CLI commands not part of chassis backup section.

    NOTE: Ensure to take backup of the IOM Startup.xml from all the IOMs before you perform chassis backup.

    ```
    OS10# copy config://startup.xml scp://username:password@hostip/<IOM_SERVICETAG>.xml
    ```

14. Click **Finish**. Click **Learn More** to see more information about the Ethernet switch backup instructions.

    NOTE: Backup and Restore operation cannot be performed when you have initiated any job and the job status is in-progress.

    A message is displayed indicating that the backup is successful, and the chassis **Overview** page is displayed.

    You can check the status and details of the backup process on the **Montitoring** > **Jobs** page.

Sensitive data

This option allows you to include passwords while taking the backup.

If you do not select the **Include Password** option, passwords for the following components are not included.

Table 14. Sensitive data

Category	Description
Network	Proxy password
Alerts	Email username and password
Alerts	SNMP Destination V3 user credentials
Network Services	SNMP Agent V3 user credentials
Local Access: Power Button	Disabled button LCD override PIN
Catalogs	CIFS or HTTPS username and password
Templates*	All user created templates
Users	AD or LDAP password and bind password
Users	OIDC registration username and password

NOTE: When you reenter the SNMP agent v3 user credentials to complete the restore task, reenter the other network services settings too.

*The secured attributes for templates include the following:

iDRAC Config

- USB Management
  - USB 1 Password for zip file on USB
- RAC Remote Hosts
  - RemoteHosts 1 SMTP Password
- Auto Update
  - AutoUpdate 1 Password
  - AutoUpdate 1 ProxyPassword
- Remote File Share
  - RFS 1 Remote File Share Password
- RAC VNC Server
  - VNCServer 1 Password
- SupportAssist
  - SupportAssist 1 Default Password
- LDAP
  - LDAP 1 LDAP Bind Password

Restoring chassis

You can restore the configuration of a chassis using a backup file. You must have the chassis administrator role with device configuration privilege to restore the chassis.

Catalogs and associated baselines cannot be restored when the **downloads.dell.com** is not reachable. Catalogs with proxy settings cannot be restored on a different chassis as the proxy password is not restored on a different chassis. This action causes **downloads.dell.com** not reachable. Configure proxy password manually and then rerun all catalog and baseline jobs to complete the restore process. If the source of a catalog is a validated firmware, re-create the catalog and all baselines that are associated with the catalog manually to complete the restoration.

Based on the HTTPS network share configuration, the catalogs for HTTPs are restored with or without password after the backup file excluding sensitive data is restored. If entering the username and password for the HTTPS share is not mandatory, the catalog is restored, else the catalog is restored with job status "failed". Enter the username and password manually after the restore task for the status to display as "completed".

The restore process is not supported if chassis role during backup does not match with the chassis role while restoring. The following table displays the chassis role prerequisites for the restore process.

NOTE: The chassis backup and restore feature is supported only if the OME-Modular firmware version in the backup file and the chassis during the restore process are identical. The restore functionality is not supported if the OME-Modular versions do not match.

Table 15. Chassis role prerequisites for restore process

During backup	Before restore	After restore	Action required
Standalone	Standalone	Standalone	Chassis restore is supported.
Standalone	Member (Group A)	Not supported	Transition the chassis to a Standalone state before initiating the restore process.
Standalone	Lead (Group A)	Not supported	Transition the chassis to a Standalone state before initiating the restore process.
Lead (Group A)	Lead (Group A)	Lead (Group A)	Chassis restore is supported. Onboard all the available chassis that were originally present in the group.

Table 15. Chassis role prerequisites for restore process (continued)

During backup	Before restore	After restore	Action required
Lead (Group A)	Standalone	Lead (Group A)	Chassis restore is supported. Standalone chassis is converted to a Lead and Onboard all the available chassis that were originally present in the group.
Lead (Group A)	Lead (Group B)	Not supported	Transition the chassis to a Standalone or Lead of the same group before initiating the restore process.
Lead (Group A)	Member (Group A)	Not supported	Transition the chassis to a Standalone or Lead of the same group before initiating the restore process.
Lead (Group A)	Member (Group B)	Not supported	Transition the chassis to a Standalone or Lead of the same group before initiating the restore process.

Use case scenarios

You can perform restore chassis operation in the following scenarios.

Restoring on the same chassis is supported:

- If management data is corrupt after a successful configuration and deployment of a chassis.
- If you run into a downgrade situation resulting in loss of management configuration.

  NOTE: OME-Modular does not support configuration restore on firmware downgrade scenarios.
- If you run into an issue where OME-Modular has to reset to default.

Restoring on a different chassis is supported:

- In disaster recovery situations, where the chassis and all its components are damaged or lost due to a catastrophic event.
- If you purchase a new chassis with the same hardware configuration.

Important notes

- When you take backup on a lead chassis with the backup lead assigned, you must assign the backup lead after the restore process, manually.
- During the restore process, you must not perform any management configurations using remote or local interfaces. Backup or restore process cannot be initiated if there are any other tasks running simultaneously.
- The member chassis that was not part of backup is automatically off-boarded from the lead chassis.
- The member chassis that was part of the lead chassis while taking backup, and later moved to another group is not restored.
- The backup and restore feature is not intended for cloning purposes as there are system-specific attributes.
- Catalogs that are created using CIFS or HTTPS network share are not restored if the backup is taken with password and restored after any of the following operations:
  - `racadm racresetcfg`
  - `racadm racresetcfg -f`
  - Change FIPS mode on the web interface.

  The tasks that are mentioned above regenerate the encryption key that is used for password encryption in the backup file. When the encryption key changes, these passwords cannot be decrypted with the changed key. Hence, the passwords cannot be restored automatically.
- Templates, profiles, I/O identities or VLANs restore can cause data path disruptions if there is a collision in VLANs between the pre-restore and backup VLANs. Manually fix dependent fabrics, if any, to address the VLAN issues.
- Catalogs and associated baselines cannot be restored when **downloads.dell.com** is unreachable as OME-Modular cannot get the catalog file name and path. Hence, the catalogs are not created.

- If the backup is taken including password and is restored on different chassis after all settings are restored successfully, you must enter the password manually for configurations that require passwords for the feature to function. Examples for configurations that require password include SMTP and proxy with authentication.
- When you reenter the SNMP agent v3 user credentials to complete the restore task, reenter the other network services settings too.

To restore a chassis:

1. On the chassis **Overview** page, click **More Actions** > **Restore**.
   The **Restore Chassis** window is displayed.
2. On the **Introduction** section, read the process and click **Next**.

   NOTE: Click **Learn More** to see more information about the Ethernet switch restore.

   SmartFabric restore operation is not supported if:
   - It is restored on a different chassis.
   - There is any difference between the current setup of the IOM hardware and the backup file.

   The maximum time to complete the chassis restore with Smart Fabric is five hours approximately.

   NOTE: Ethernet switch settings that are part of `Startup.xml` should be restored on all the IOMs before starting appliance restore task on the OME-M.

   ```
   OS10# copy scp://username:password@hostip/<IOM_SERVICETAG>.xml config://
   startup.xml
   ```

   NOTE: All the IOMs reload during SmartFabric restore.

   The **Upload File** section is displayed.
3. Under **Restore File Location**, select the **Share Type** where the configuration backup file is located.

   NOTE: If the current MM link configuration setup is different from the backup file, you must match the Top of Rack (TOR) connection to the MM link configuration before the restore operation.

   NOTE: During the SmartFabric restore, all the IOMs are converted in to the operating mode as in the backup file.

   NOTE: All the IOMs which go through the fabric restore are reloaded. The IOMs are reloaded twice if there is any difference in the mode of backup file and the current IOM.

4. Enter the **Network Share Address**, and **Network Share Filepath** where the backup file is stored.
5. Enter the name of the **Backup File and Extension**.
6. If the **Share Type** is CIFS, enter the **Domain**, **Username**, and **Password** to access shared location. Else, go to step 9.
7. Click **Test Now**, if the network connection is not tested.
8. If the **Share Type** is HTTPS, **Certificate Verification** option is displayed. Select the checkbox to check the web server certificate authentication.
9. In the **Restore File Password** section, enter the **Encryption Password** to open the encrypted backup file.

   NOTE: The password must be 8 to 32 characters long and must be a combination of an uppercase, a lowercase, a special character (+, &, ?, >, -, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l) , and a number.

   NOTE: If the restore operation is done excluding passwords or on a different chassis with proxy settings, the proxy dependent tasks, such as repository task, try to connect to the external share. Rerun the tasks after configuring the proxy password.

10. Click **Validate** to upload and validate the chassis configuration.
    The **Optional Component** section is displayed.
11. From the **Optional components**, you can choose to restore files on the selected components .
    - **Restore File Validation Status**—Displays the validation status of the restore files.

      NOTE: The ✅ indicates that the restore file validation status is successful. If the validation is not successful, an error message is displayed with the recommended action.
    - **Optional Components**—Displays the components that you can select for the restore operation. The possible options are:

- Templates, Profiles, Identity Pools, and VLAN Configurations
- Application and Chassis Settings
- Certificates

  NOTE: The chassis certificate restore fails if you perform racresetcfg in the chassis and try to restore the backup file.
- Catalogs and Baselines

  NOTE: You can restore only the latest validated catalog. If you want to restore the earlier validated catalogs, you must delete the previous catalogs and re-create them manually.
- Alert Policies
- SmartFabric Settings

  NOTE: Restoring fabrics may impact the data path.

NOTE: The list of **Optional Components** is based on the backup chassis settings. The components that are not part of chassis backup is listed under **Unavailable Components** section below.

- **Mandatory Components**—Displays the mandatory components for the restore operation.
- **Unavailable Components**—Displays the components that are unavailable for the restore operation.

12. Click **Restore** to restore the chassis.
    A message is displayed indicating that the chassis restore job is initiated successfully. You can check the status and details of the restore process on the **Montitoring** > **Jobs** page.

Impact on restore function

A chassis may have updated or additional configuration for profiles, templates, I/O identities, alert policies, firmware baselines, VLANs, or fabrics before the restore job. The restore job impacts these configurations in the following manner:

- Profiles—All profiles present in the chassis before the restore job, are replaced with profiles from the backup.
- Templates—Templates that do not overlap with the templates in the backup file are unaffected. Templates that overlap with the backup are renamed with a new template name in the format: `<Templatename_timestamp_at_restore>`.
- I/O-Identities—I/O-Identities that are not in the backup file are transferred to the Identity pool as available. Similar to templates, I/O pools names that do not overlap with the names in the backup file are unaffected. If the names overlap, the backup I/O pool is renamed as `<I/OPool_timestamp>`.
- Alert policies—Alert policies that do not overlap with the policies in the backup file are unaffected.
- Firmware baselines or catalogs—All baselines or catalogs present in the chassis before the restore job, are replaced with baselines or catalogs from the backup.
- VLANs—VLANs that do not overlap with the VLANs in the backup file are unaffected. Any VLANs that overlap with the backup are replaced with VLANs from the backup.
- Fabrics—All fabrics present in the chassis before the restore job, are replaced with fabrics from the backup.

Impact on restore when existing devices and devices in chassis backup mismatch

The following table describes the impact on the restore job when the existing devices and devices available in the chassis backup do not match.

Configuration description	Notes	Existing or new devices
Appliance settings	All these settings are device compatible and are restored in the OME-Modular database and file system.	N/A
Templates/Profile/Identities/VLANs	It is possible that the chassis is missing a server that existed at the time of backup. For example: any profile deployed to compute is restored in the database as unassigned profile. The profile and its associated data such as Identities, are restored in the database with appropriate states (profile: unassigned, identities: reserved).	Configuration is restored in the database only. No deployment jobs run during restore. If there is disaster recovery, you can edit the restored unassigned profile and associate it with a new device and deploy it.

Configuration description	Notes	Existing or new devices
Alert Policies/Firmware Baselines	It is possible that the chassis is missing a server that existed at the time of backup. For example: policies and firmware baselines are restored without any device associations.	New devices—Edit the policies and baselines to add new devices.
Fabrics	It is possible that the chassis has all the switches participating in the fabrics or some switches are missing, or all switches are missing that existed at the time of backup of fabrics.	Fabric restoration is not supported if : 1. It is restored on different chassis. 2. There is a mismatch between current set of IOMs and backup file.

Ethernet switch backup instructions

Backing up IOM

You can backup IOM configuration settings using the IOM CLI followed by the backup procedure on the OME-M.

NOTE: You must backup each IOM before performing the backup operation on the OME-M interface.

To create IOM backup:

- Log in to each IOM using SSH from a terminal `ssh username@<IOM Mgmt IP>`
- At the OS10 CLI prompt, use the write memory command for each IOM in the cluster to save the current configuration.
- Enter the `copy config://startup.xml scp://userid:password@hostip/<SERVICETAG>.xml` command to create a backup for each IOM.

  NOTE: SCP protocol is used as an example, the copy command can use other protocols such as FTP, SFTP, TFTP, HTTP, or HTTPS to perform this activity. For detailed instructions, see the Dell SmartFabric OS10 User Guide.

  NOTE: The name of the backup file should be unique. The above example uses the service tag of the IOM. In OS10, the configuration settings are saved in the startup configuration file called startup.xml. This file is stored in the config system folder. To create a backup of all the configuration settings saved in the startup file, copy the startup configuration file to a remote server or the local `config:, home:, or usb:`directories. The above example command shows the startup configuration file that is saved on a remote server.
- Perform backup procedure on the OME-M interface.

Restoring IOM

You can restore IOM configuration settings using the IOM CLI from the backup file that is stored on a remote server or in the local directory of the IOM. After this step, follow the backup procedure on the OME-M.

To restore a chassis:

- Log in to each IOM using SSH from a terminal `ssh username@<IOM Mgmt IP>`.
- Enter the `copy scp://userid:password@hostip/<SERVICETAG>.xml config://startup.xml` command to restore the backup configuration for each IOM.

  NOTE: The name of the file should be the same as the backup file that was saved earlier.

  CAUTION: Reload the IOM after you have copied the file.
- Perform restore procedure on the OME-M interface.

  After running the copy command, reload the node. Reload one VLT fabric node at a time to avoid data path impact. The links might flap and pass traffic for a short time till the SmartFabric restore is complete from OME-Modular.

Exporting chassis profiles

You can export chassis profiles for cloning the settings to other chassis.

To export the chassis profile:

1. On the OME–Modular home page, click **More Actions** > **Export Profile**.
   The **Export Profile** window is displayed.
2. Select the **Share Type**.
3. Enter the network share address and path.
4. If the **Share Type** is CIFS, enter the **Domain**, **User Name**, and **Password** to access the shared location.
5. Click **Export**.

Managing chassis failover

Failover is applicable in dual management module configuration and is the process of transferring the active role to the standby management module. Reboot the active management module and reinitialize the stand-by management module to assume the active role. The failover operation takes up to 10 minutes for completion. OME–Modular is unavailable during this process. You must have the chassis administrator privilege to start a failover.

The OME-Modular IP is online in about five minutes after performing a chassis failover task.

NOTE: After a failover, the chassis management performance returns to normal in a few minutes.

NOTE: During a failover, the chassis power state on the OME–Modular user interface is displayed as **off**. The original power state is displayed after the inventory is refreshed.

To start a failover:

On the chassis **Overview** page, click **More Actions** > **Failover**.
A message is displayed stating that the system cannot be accessed during a failover.

Troubleshooting in chassis

The Troubleshoot option on the OME–Modular home page enables you to use the following options to resolve issues that occur in the chassis:

- Extract Log—Use this option to extract application logs and save them to the NFS or CIFS locations on the network.
- Diagnostic Commands—Use this option to run diagnostic commands and parameters to troubleshoot the chassis network.
- Reset Management Module—Use this option to reboot the management module (MM) in a single management module configuration, and perform a failover in a dual MM configuration.

  NOTE: During a factory reset process, the synchronization takes about 5 to 8 minutes. During this period, the serial, KVM, and Quick Sync interfaces do not accept the factory password and the login attempt fails.

  NOTE: Reset Management Module causes the MM to reboot in a single MM configuration, and a failover in a dual MM configuration. This operation may take up to 10 minutes for completion, and the OME-M is unavailable during this process.
- Terminate Serial Connection—Use this option to end the existing serial sessions.

Extracting logs

You can extract the application logs and save them to a local device or, to the NFS or CIFS location on the network. You cannot extract logs and update firmware simultaneously.

To extract application logs:

1. On the **Devices** > **All Devices** page, click **Extract Logs** .
   The **Extract Logs** wizard is displayed.
2. On the **Extract New Log** section, click **Edit Selection**.
   The **Select Devices** wizard is displayed.

3. Select the device or chassis and click **Finish**.
   You can see the device that is selected under the **Selected Devices** section.
4. On the **Download Details** section, select the **Saved File Location** where you want to extract the logs.
   The available options are:
   - CIFS
   - NFS
   - Locally to device—Downloads the application logs to a location on your local system.
     - Supported devices are:
       - MX7000
       - MX740c, MX840c, MX760c, and MX750c
       - MX5000s IOM
     - Unsupported devices are:
       - MX9116N, MX7116N, and MX5108N
       - 10G PTM and 25G PTM

   NOTE: The "Locally to device" option is available only when you are directly logged in to lead, member, or stand-alone chassis.
5. Enter the **Network Share Address** and **Network Share Filepath**.
6. If the **Share Type** is CIFS, enter the **Domain**, **User Name**, and **Password**. Else, go to step 7.
7. Select the **Mask Sensitive Logs** checkbox to exclude the sensitive data. For more information, see Sensitive data section.
8. Click **Test Connection**, and then click **Save**.

Blinking LEDs

You can use the **Blink LED** option on the OME–Modular home page to turn off or turn on the chassis LED.

Interfaces to access OME-Modular

After configuring the network settings in OME–Modular, you can remotely access OME-Modular using various interfaces. The following table lists the interfaces that you can use to remotely access OME–Modular.

Table 16. Management module Interfaces

Interface	Description
Web interface	Provides remote access to OME–Modular using a graphical user interface. The web interface is built into the OME–Modular firmware and is accessed through the NIC interface from a supported web browser on the management station. The number of user sessions that are allowed for each interface is: ● Web interface – 6 ● RESTful API – 32 ● SSH – 4 For a list of supported web browsers, see the Supported browsers section in the *Dell OpenManage Enterprise-Modular for PowerEdge MX7000 Chassis Release Notes* available at https://www.dell.com/openmanagemanuals.
Remote RACADM command-line interface	Use this command-line utility to manage OME–Modular and its components. You can use remote or firmware RACADM: ● Remote RACADM is a client utility that runs on a management station. It uses the out-of-band network interface to run RACADM commands on the managed system and uses the HTTPs channel. The `-r` option runs the RACADM command over a network. ● Firmware RACADM is accessible by logging in to OME–Modular using SSH or telnet. You can run the firmware RACADM commands without specifying the OME–Modular IP, user name, or password. After you enter the RACADM prompt, you can directly run the commands without the RACADM prefix.

Table 16. Management module Interfaces (continued)

Interface	Description
	NOTE: A log for remote RACADM session (login or logout) is displayed in the **Audit Logs** page, irrespective of the remote RACADM status. However, the feature does not work if the remote RACADM option is disabled.
LCD	Use the LCD on the front panel to: ● View alerts, OME–Modular IP or MAC address. ● Set DHCP ● Configure OME–Modular static IP settings. ● View OME–Modular MAC address for the active MM. ● View the OME–Modular VLAN ID appended to the end of MM IP, if the VLAN is already configured. ● At-the-box management—Create a group, join group, leave group, or delete group. ● At-the-box storage mapping resolution on compute sled replacement condition. **NOTE:** The data refresh can take several seconds depending on OME-Modular response. This is typically 1-5 seconds, but can be longer if the OME-Modular is busy. If it takes longer than 30 seconds, check OME-Modular response using GUI or RACADM. For more information about the LCD touch panel, see the Dell PowerEdge MX7000 Enclosure Installation and Service Manual.
SSH	Use SSH to connect to the MX7000 chassis and run RACADM commands locally.
RESTful API and Redfish	The Redfish Scalable Platforms Management API is a standard that the Distributed Management Task Force (DMTF) has defined. Redfish is a next-generation systems management interface standard, which enables scalable, secure, and open server management. It is a new interface that uses RESTful interface semantics to access data that is defined in model format to perform out-of-band systems management. It is suitable for a wide range of servers ranging from stand-alone servers to rack mount and bladed environments and for large-scale cloud environments. Redfish provides the following benefits over existing server management methods: ● Increased simplicity and usability ● High data security ● Programmable interface that can be easily scripted ● Follows widely used standards For more information, see the *OpenManage Enterprise-Modular RESTful API Guide* available at https://www.dell.com/openmanagemanuals.
SNMP	Use SNMP to: 1. Download the OME-Modular MIB file from the https://www.dell.com/support. 2. Use MIB walker tool to get supported information using OIDs. **NOTE:** SNMP SET is not supported.
Serial	You can use the serial interface to access OME–Modular by connecting the micro USB port on the rear of the management module to a laptop and opening a terminal emulator. The user interface that is displayed enables you to log in to the management module, networking IOMs, or servers (iDRAC). You can have a maximum of one serial session open at a time.
Quick Sync	You can have a maximum of one Quick Sync session open at a time.
KVM	You can have a maximum of one KVM session open at a time.
Chassis Direct	The Chassis Direct feature enables you to access management consoles such as iDRAC and management module of devices on the MX7000 chassis.

Viewing chassis hardware

On the OME–Modular home page, click **Hardware** to view details of the hardware components that are installed in the chassis. You can also view the chassis hardware details by clicking **Devices** > **Chassis** > **View Details** > **Hardware**. The hardware components consist of chassis power supplies, chassis slots, management module, fans, temperature, FRU, device management information, installed software, and management ports.

The upper warning threshold changes based on the user and dynamic configurations. Manually configured values take a priority over system calculated threshold. Hence, reset the manually configured threshold for the thermal feature to function properly. To reset the threshold:

- In the iDRAC CLI, run the command, `racadm racresetcfg`.
- In the iDRAC user interface, go to **Maintenance** > **Diagnostics** and click **Reset iDRAC to Factory Defaults**.

Points to remember:

- If the Power Supply Unit (PSU) is absent, the health state and power status for the PSU are not displayed on the **Chassis** > **Hardware** > **Chassis Power Supplies** page.
- Maintain a minimum interval of two minutes while removing and inserting any device.

Chassis slot details

The **Chassis Slots** page displays details of the slots that are inserted in the chassis. The details are—number, type, and name of the slot, name of the device, model, unique identification code of the slot, and, the number of VLAN IDs associated with the slot. The page also indicates if a server profile is associated with the slot.

You can perform the following tasks on the **Chassis Slots** page:

- System Reseat—Virtually reseats the compute or storage sleds, and IOMs. This operation causes the devices to behave as if they were physically removed and reinserted.
- iDRAC Reset—Performs hard reset of the slot-based compute sled. You can use this option to troubleshoot an unresponsive iDRAC.

Viewing chassis alerts

On the OME–Modular home page, click **Alerts** to view details of the alerts triggered for the events that occurred in the chassis. You can also view the chassis hardware details by clicking **Devices** > **Chassis** > **View Details** > **Alerts**.

You can sort the list of alerts based on the following advanced filters:

- Severity
- Acknowledge
- Start Date
- End Date
- Source Name
- Category
- Subcategory
- Message

Select an alert to view the summary of the alert.

You can also perform the following activities on the **Alerts** page.

- **Acknowledge**
- **Unacknowledge**
- **Ignore**
- **Export**
- **Delete**

Viewing chassis hardware logs

The logs of activities performed on the hardware components associated with the chassis are displayed on the OME–Modular **Hardware Logs** page. The log details that are displayed include severity, message ID, category, timestamp, and description. You can also view the chassis hardware logs by clicking **Devices** > **Chassis** > **View Details** > **Hardware Logs**.

You can perform the following tasks on the **Hardware Logs** page:

- Click **Advanced Filter** to filter the logs based on severity, message ID, start date, end date, or category.
- Click **Export** > **Export Current Page** to export all the displayed logs.
- Select a specific log and click **Export**.

NOTE: If a `racrestcfg` is performed, the message, "CMC8709 and CMC8710 logs are appearing 2 times each, one for slot 1 and other for slot 2", is displayed on the **Hardware Logs** page.

Configuring OME–Modular

The **Application Settings** menu on the home page enables you to configure various settings for OME–Modular. The settings include the following:

- Network
- Users
- Security
- Alerts

Viewing current configuration

Click **Application Settings** > **Network** > **Current Settings**.
The current network, IPv4, and IPv6 settings are displayed.

If all three DNS servers that are available for use are IPv4 or IPv6, then only two of them are displayed. The third server could be in use but is not displayed on the OME-Modular or RESTful interface.

NOTE: If the MX7000 Management Module is receiving router advertisements from more than one router, the current gateway address may be displayed as blank in the User interface, REST, and RACADM interfaces.

Configuring OME–Modular IP address

1. Click **Application Settings** > **Network** > **Address Configuration**.
2. Ensure that the **Enable NIC** option is selected.
3. Enable the required IP version-IPv4 or IPv6.

   NOTE: The IOM and OME–Modular must be registered in the DNS. Else, the message, `Warning: Unit file of rsyslog.service changed on disk, 'systemctl daemon-reload' recommended.`, is displayed.

   NOTE: After rebooting OME–Modular, the public interface with the OME–Modular IP is available after 12 minutes approximately.

4. Enable the DHCP option, and enter the IP address and other details.

Configuring OME–Modular web server

1. Click **Application Settings** > **Network** > **Web Server Configuration**.
2. Ensure that the **Enable Web Server** option is selected.
3. Enter the timeout value in minutes.
4. Enter the port number for the web server.
   You can enter a port number in the 10 to 65535 range. The default port number is 443.

When the web server https port settings from the lead chassis are applied to member chassis as part of the add or join member task, refresh the inventory for the lead chassis manually to see the correct https port for the member chassis on the **Hardware** > **Device Management Info** page. Launch the member chassis from the lead chassis to see the port number.

If you customize the https port, OME-Modular tries to redirect to the new port automatically. However, the redirection may not work owing to security limitations of the browser. In such cases, open a new window or tab of the browser and enter the OME-Modular URL using the customized port. For example, `https://10.0.0.1:1443`

NOTE: Disabling the OME-Modular web server does not affect the launching of OME-Modular UI on the phonebook page while using Chassis USB Direct.

NOTE: To update the webservice timeout and session configuration timeout, use the same chassis profile. Using the same chassis profile ensures that the webservice timeout and the session configuration timeout are synchronized. Else, when the webservice timeout is updated and the session configuration is processed, the session configuration overwrites the web service settings.

5. Select the TLS protocol version from the drop-down.

   The available options are:
   - **TLS 1.1 and Higher**
   - **TLS 1.2 and Higher**
   - **TLS 1.3 only**

   NOTE: Set the TLS protocol settings to **TLS 1.2 and Higher** before:
   - Downgrading OME-Modular from version 2.00.00 to earlier versions.
   - Performing MM part replacement and MM synchronization with modules earlier than 2.00.00.

6. The default cipher string is displayed. Click **Edit Cipher String** to edit the existing string or replace it with another string. The **Set Cipher String** window is displayed.

Configuring session inactivity timeout

1. In the **Universal Timeout** section, select the **Enable** check box and enter the time in minutes after which all the sessions must end. The duration can be in 1 to 1440 minutes.

   If you enter the universal inactivity timeout duration, the inactivity options for the API, web interface, SSH, and Serial sessions are disabled.

2. In the **API**, **Web Interface**, **SSH**, and **Serial** sections, enter the time in minutes after the sessions must end and the maximum number of sessions you want to enable.

   The timeout duration can be 1 to 1440 minutes, and the maximum number of sessions can be between one and 100. The inactivity timeout duration can be 1 to 1440 minutes for API and Serial sessions, 1 to 120 minutes for web interface sessions, and 1 to 180 minutes for SSH sessions.

   The maximum number of sessions for the interfaces are as follows:

   - API—1-100
   - Web interface—1-6
   - SSH—1-4
   - Serial—1

   When you downgrade from the current version of OME-Modular to an earlier version, maximum number of API sessions supported is 32. However, if you upgrade OME-Modular to the latest version that supports 100 sessions, but the API Session attribute value that is displayed is 32. You can manually set the attribute value to 100 sessions.

Configuring OME–Modular date and time settings

1. Click **Application Settings** > **Network** > **Time Configuration**.
2. Select the **Use NTP** check box, if required, and enter the NTP server details.
3. Select the required time zone.

   NOTE: Any change in the attribute settings leads to IP drop or unavailability of the OME–Modular web interface for some time. However, the OME–Modular web interface recovers automatically.

NOTE: Some time zones which are supported in OME-M might not be supported on MXG610s IOMs.

Configuring OME–Modular proxy settings

1. Click **Application Settings** > **Network** > **Proxy Configuration**.
2. Select **Enable HTTP Proxy Settings**.
3. Enter the proxy address and the port number.
4. Select **Enable Proxy Authentication** and enter the proxy user credentials.
   You can enable proxy authentication only if the **Enable HTTP Proxy Settings** option is selected.
5. Select **Ignore Certificate Validation**,
6. Enter the **Proxy Exclusion List** to exclude proxy addresses from the configuration.
7. Click **Apply**.

Configuring IOM synchronization

You can replicate the time and alert destination configuration of the lead chassis in the network and MXG610s IOMs.

To configure the time and alert destination:

1. Click **Application Settings** > **Network** > **IOM Synchronization Configuration**.
2. Select the **Replicate Time Configuration from Chassis** and **Replicate Alert Destination Configuration from Chassis** check boxes.
   - MXG610s supports only three SNMP destination unlike OS10 which supports four SNMP destinations.
     - Using SNMP, IPV4 and IPV6 replication is supported from OME-Modular to IOM.
     - Using SNMP, FQND and Host Name is supported only if DNS Address for MXG610s (Pre-requisite for DNS configuration) is Static management IP Address configuration.
     - Using SNMP, SNMPv2 replication is supported for OS10 and SNMPV1 and SNMPv3 replication is supported for MXG610s.
   - MXG610s supports four Syslog destinations same as OME-Modular.
     - Using Syslog, only 514-port number is supported from OME-Modular to Network IOM.
     - Using Syslog, 10 to 65535-port number is supported from OME-Modular to MXG610s. Port number is configured as a secure port.

   NOTE: For MXG610s, the SNMP v3 alert destination replication is skipped, if the authentication or privacy type options on the **Application Settings** > **Alerts** > **SNMP Alert Forwarding** page are set to **None**.
3. Click **Apply** to save the changes.
   In MCM environment, the IOM network synchronization configuration is propagated from the lead to the member chassis only if the alert destination option is selected while creating the chassis group or adding members to the group.

Configuring device name preference

1. Click **Application Settings** > **Network** > **Device Name Preference**.
2. Select the naming preference.

Ports and protocols supported in OME-Modular

The table below lists the protocols and ports that are supported in OME-Modular.

Table 17. Ports and protocols that are supported in OME-Modular

Port number	Protocol	Port type	Maximum encryption level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	External application	In	OME-Modular	Required for incoming only

Table 17. Ports and protocols that are supported in OME-Modular (continued)

Port number	Protocol	Port type	Maximum encryption level	Source	Direction	Destination	Usage
							if FSD is used. OME-Modular administrator must enable this port only while interacting with Dell.
25	SMTP	TCP	None	OME-Modular	Out	External Application	To receive email alerts from OpenManage Enterprise.
53	DNS	UDP or TCP	None	OME-Modular	Out	External Application	For DNS Queries
80	HTTP	TCP	None	External Application	In	OpenManage Enterprise Modular	The Web interface landing page. Will redirect a user to HTTPS.
123	NTP	UDP	None	OME-Modular	Out	NTP Server	Time synchronizati on (if enabled).
137, 138, 139, 445	CIFS	UDP or TCP	None	OME-Modular	Out	CIFS Share	To import firmware catalogs from CIFS share.
161*	SNMP	UDP	None	External Application	In	OpenManage Enterprise Modular	For SNMP queries.
162	SNMP	UDP	None	External Application	In or Out	OpenManage Enterprise Modular	Send SNMP traps and receive Informed Request.
443	HTTPS	TCP	128-bit SSL	External Application	In or Out	OpenManage Enterprise Modular	Web interface. To download updates and warranty information from dell.com. The 256-bit encryption is enabled while communicatin g with OME-Modular by using the HTTPS protocol for

Table 17. Ports and protocols that are supported in OME-Modular (continued)

Port number	Protocol	Port type	Maximum encryption level	Source	Direction	Destination	Usage
							the web interface.
514**	Syslog	TCP	None	OME-Modular	Out	Syslog Server	To send alert and audit log information to Syslog server
546	DHCP	TCP	None	OME-Modular	Out		Network configuration
636***	LDAPS	TCP	None	OME-Modular	Out	External Application	AD/ LDAP login for Global Catalog.
3269***	LDAPS	TCP	None	OME-Modular	Out	External Application	AD/ LDAP login for Global Catalog.

Legend:

- *—You can configure up to 65535 ports excluding the port number that is already allocated.
- **—Configurable ports
- ***— OME-Modular is configured by default to use only LDAPS to communicate AD or LDAP servers.

Configuring users and user settings

In OME–Modular, you can create up to 64 local users and assign them specific roles and privileges. Using the options available under **Application Settings** > **Users**, you can add and edit users, import a directory group, and view and terminate active user sessions.

NOTE: You can create, delete, enable, or disable users only if you have the security setup privilege.

Viewing and editing user accounts

1. Click **Application Settings** > **Users**
   On this page, you can view a list of user accounts and their roles, the user types, and whether the account is enabled or not.
2. Hover over and click to select the user row that you want to edit and click **Edit** on the right side of the page.
   The **Edit User** wizard is displayed.
3. Enter the **Username**.
   The default username is "root", and you cannot edit it. You cannot disable the default account or edit the role that is associated with the default account. The length of the username can be 1 to16 characters long and contain white spaces and alphanumeric characters. The special characters - §, ", /, :, @, and ` are not supported.

   NOTE: For the OME–Modular serial interface, ensure that the length of the local or remote username does not exceed 35 characters.

   NOTE: Do not use "system" as a username.
4. Enter the **Password** and **Confirm Password**.
   The password can be 8 to 32 characters long and contain at least one of the following:
   - Number
   - Special character—The supported special characters are - **+**, **&**, **?**, **>**, **-**, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, %, =, <, :, {, l
   - Uppercase letter
   - Lowercase letter

NOTE: You can change only the password of the default "root" account.

5. Select **User Role**. The available options are:
   - Chassis Administrator
   - Compute Manager
   - Fabric Manager
   - Storage Manager
   - Viewer
6. Select **Enabled** to enable the account immediately after you create it.

   NOTE: For more information about the fields, see the integrated help in the OME–Modular web interface.

7. From the **RSA SecurID**, select the option, **Disable** or **Enable**. The default option is **Disable.**
   Click **RSA SecurID Configuration** link if you want to edit the configuration.

Adding users

1. Click **Application Settings** > **Users**
2. Click **Add**.
   The **Add New User** wizard is displayed.
3. Enter the **Username**.
   The default username is "root", and you cannot edit it. You cannot disable the default account or edit the role that is associated with the default account. The length of the username can be 1 to16 characters long and contain white spaces and alphanumeric characters. The special characters - §, ", /, :, @, and ` are not supported.

   NOTE: For the OME–Modular serial interface, ensure that the length of the local or remote username does not exceed 35 characters.

   NOTE: Do not use "system" as a username.

4. Enter the **Password** and **Confirm Password**.
   The password can be 8 to 32 characters long and contain at least one of the following:
   - Number
   - Special character—The supported special characters are - **+**, **&**, **?**, **>**, **-**, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, %, =, <, :, {, |
   - Uppercase letter
   - Lowercase letter
5. Select **User Role**. The available options are:
   - Chassis Administrator
   - Compute Manager
   - Fabric Manager
   - Storage Manager
   - Viewer
6. Select **Enabled** to enable the account immediately after you create it.

   NOTE: For more information about the fields, see the integrated help in the OME–Modular web interface.

7. From the **RSA SecurID**, select the option, **Disable** or **Enable**. The default option is **Disable.**
   Click **RSA SecurID Configuration** link if you want to edit the configuration.

Enabling, disabling, and deleting users

1. Click **Application Settings** > **Users**.
   A list of user account is displayed.
2. Select the account, and then click the required option above the list of accounts.

Recovering passwords

You must have physical access to the chassis to reset the login credentials to defaults.

Recovering passwords in single OME-Modular controller

1. From the chassis, remove the single OME–Modular controller.
2. Locate the Jumper, see the board location—P57 RESET PASSWORD, and then insert the Jumper.
3. Reinsert the controller into the chassis.
4. When OME–Modular is available, login with the user name as "root" and password as "calvin".
5. After the root user authentication, change the password for the root user on the **Application Settings** > **Users** page.
6. Log out and log in again using the modified password to ensure that the login is successful.
7. Remove the jumper and reinsert it into the default positions—2 and 3.

Recovering passwords in dual OME-Modular controllers

1. From the chassis, remove both the OME-Modular controllers.
2. On one of the modules, locate the Jumper, see the board location—P57 RESET PASSWORD, and then insert the Jumper.
3. Reinsert only the controller, where the Jumper is installed, into the chassis.
4. When OME–Modular is available, login with the user name as "root" and password as "calvin".
5. After the root user authentication, modify the password for the root user on the **Application Settings** > **Users** page.
6. Remove the controller where the Jumper is inserted, locate the Jumper.
7. Set the Jumper to the default position and insert the controller back into the chassis.
8. When OME-Modular is available, login with the modified password.
9. Insert the second controller to restore the MM redundancy.

User roles and privileges

Table 18. User roles and privileges

User Role	Chassis Administrator	Compute Manager	Storage Manager	Fabric Manager	Viewer
Privilege					
Viewing application information	Yes	Yes	Yes	Yes	Yes
Setting up applications such as network, NTP, and proxy	Yes	No	No	No	No
Setting up users, security login policies, and certificates	Yes	No	No	No	No
Monitoring alert policies and alert destinations	Yes	No	No	No	No
Device power control	Yes	Yes	Yes	Yes	No
Device configuration actions	Yes	Yes	Yes	Yes	No

Table 18. User roles and privileges (continued)

User Role	Chassis Administrator	Compute Manager	Storage Manager	Fabric Manager	Viewer
Example—Applying templates, migrating profiles, and managing storage mappings					
Updating device firmware	Yes	Yes	Yes	Yes	No
Creating and managing device templates, identity pools, and logical networks	Yes	Yes	Yes	Yes	No
Managing firmware catalogs and baseline policies	Yes	Yes	Yes	Yes	No
Power budget configuration and management	Yes	No	No	No	No

Managing user sessions

You can view and terminate existing user sessions using the **User Sessions** page, if you have the chassis administrator privilege.

Viewing user sessions

On the **Users** page, click **User Sessions**.
You can view the list and details of the users who are logged in.

Terminating user sessions

1. On the **Users** page, click **User Sessions**.
   You can view the details of the users who are logged in.
2. Select the user from the list and click **Terminate**.
   A message is displayed prompting you to confirm the termination.

Configuring login security settings

OME–Modular supports IP range-based access restriction. You can restrict access to only a specified range of IP addresses. You can also configure lockout policies that enforce delays after certain number of failed login attempts.

Configuring login IP range

1. Click **Application Settings** > **Security** > **Settings** > **Restrict Allowed IP Ranges**.
2. Select **Enable IP Range**.
3. Enter the IP range in the CIDR format.
   For IPv4, enter the IP address in the format—192.168.100.14/24. For IPv6, enter the IP address in the format—2001:db8::/24.
   NOTE:

- OME-Modular supports single or multiple IP ranges. Ensure that the multiple IP ranges are comma-separated using CIDR notation. For example: 100.101.10.24/16,192.168.137.1/8
- IPv4 and IPv6 are not supported together.

4. Click **Apply**.

Configuring login lockout policy

1. Click **Application Settings** > **Security** > **Login Lockout Policy**.
2. Select **By User Name** to enable user account-based lockout. Select **By IP Address** to enable IP address-based lockout.
3. Enter the lockout details:
   a. Lockout Fail Count: The number of failed login attempts. Valid values are between 2 and 16.
   b. Lockout Fail Window: The time within which subsequent failed logins are registered. Valid time is between 2 seconds and 65,535 seconds.
   c. Lockout Penalty Time: Time for which the logins are restricted. Valid time is between 2 seconds and 65,535 seconds.

If the IP is still unavailable, ensure that:
- The network cable is connected.
- If DHCP is configured, ensure that the cable is connected to a ToR switch that has connectivity to the DHCP server.

Enabling FIPS mode

The United States government agencies and contractors use the FIPS standards. FIPS Mode is intended to meet the requirements of FIPS 140-2 level 1.

To enable FIPS mode, click **Application Settings** > **Security** > **Federal Information Processing Standards (FIPS)**.

NOTE: After enabling the FIPS mode or reset configuration operation, wait for sometime for the application to become stable.

To view FIPS version, click **Application Settings** > **Security** > **Federal Information Processing Standards (FIPS)**.

Configuring RSA SecurID

This option allows you to configure Multifactor Authentication(MFA) using RSA SecurID. Select both security settings and user authentication settings in the propagation section. This action enables you to use RSA passcode when you try logging into the member chassis. You should add required license to use the RSA SecurID feature. The **Time Configuration** should be configured manually after RCP replacement to use the RSA feature.

The **RSA SecurID** feature is available only when the OME-Modular Advanced license is installed.

NOTE: You cannot enable the RSA SecurID option for root users.

1. Enter the **RSA SecurID Authentication Server URL**, **RSA SecurID Client ID**, and **RSA SecurID Client Access Key**.
2. Click **Test Connection** to check the network connection.
3. Select the **Upload RSA Server Certificate** check box and click **Select a file** to upload and validate the certificate.
4. Click **Apply** to complete the configuration.

Managing certificates

You can view details of the SSL certificates on the **Certificates** page. The information includes:
- Validity of the certificate
- Name of the organization
- Name of the issuing authority
- Alternative name of the organization

If you have the security setup privilege, you can perform the following tasks:
- View the SSL certificate that is deployed.
- Generate a new certificate signing request (CSR).

- Upload the server certificate that is based on the CSR generated, to replace the default or deployed certificate.

NOTE: If you have a custom certificate that is uploaded on 1.40.xx and you downgrade the OME-M to earlier version, downgraded chassis restores the self-signed certificate. Manually upload a custom certificate in the chassis.

NOTE: The OME-Modular SSL certificate is not generated with a valid expiry date after the chassis local time is set to leap year and the `racresetcfg` task is performed. This is because the SSL certificate uses the system build system date, which is also stored in the file, `msm_build_date.dat`.

Adding new certificate

You can replace existing SSL certificate with a new certificate. The options perform certificate enrollment are:

- Manual Certificate
- Automatic Certificate
- Custom PKCS Certificate

To add a certificate:

1. Click **Application Settings** > **Security** > **Certificates** > **Replace**.
   The New Certificate window is displayed.
2. Select the required option to enroll the certificate. The available options are:
   - Manual Certificate
   - Automatic Certificate
   - Custom PKCS #12 Certificate

Manual certificate enrollment

To enroll the certificate manually:

1. Click **Application Settings** > **Security** > **Certificates** > **Replace**.
   The **New Certificate** window is displayed.
2. Select **Manual Certificate** option.
3. On the **Manual Certificate Enrollment** section, click **Add**.
   The **New Certificate Information** window is displayed.
4. Add the required details and click **Finish**.
5. Click **Generate CSR**.
   The **Certificate Signing Request** window is displayed.
6. Click **Download Certificate Signing Request** to download the content in .txt format to a local drive. Submit the content to a certifying authority to obtain a valid SSL certificate.
7. Click **Upload** to navigate and upload the signed CSR file.
8. Click **Finish** to create the certificate.

Automatic certificate enrollment

The **Automatic Certificate** enrollment feature is available only when the OME-Modular Advanced license is installed.

To enroll the certificate automatically:

1. Click **Application Settings** > **Security** > **Certificates** > **Replace**.
   The **New Certificate** window is displayed.
2. Select **Automatic Certificate** option.
3. On the Automatic Certificate Enrollment section, click **Add** or **Replace** as applicable.
   The **New Certificate Information** window is displayed.
4. Add the required details and click **Finish**.
5. Enter the following information and click **Apply**.
   - Enrollment Actions—Select the applicable enrollment actions. The available options are:
     - Halt—Stops or pauses monitoring the certificate which is already enrolled on the server.
     - Enroll—Registers the certificate on the server.
     - Monitor—Monitors the certificate which is already enrolled on the server. If the certificate is expired, it triggers reenrolled certificate automatically.

- CA URL—Enter the URL of the CA Server.
- Challenge Password—Displays the password of the CA server. This field is optional.

  NOTE: If server is set up without challenge password, the server ignores user provided challenge password and provides the certificate.

6. Click **Upload** to navigate and upload the signed CSR file.
7. Click **Finish** to create the certificate.

Custom PKCS #12 certificate enrollment

To enroll the certificate using Custom PKCS #12:

1. Click **Application Settings** > **Security** > **Certificates** > **Replace**.
   The New Certificate window is displayed.
2. Select **Custom PKCS #12 Certificate** option.
3. Enter the autogenerated password from the server for certificate enrollment. Password complexity depends on the server.
4. Click **Upload** to navigate and upload the signed CSR file.
5. Click **Finish** to create the certificate.
   - OME–Modular does not create an SSL certificate on time change or on every boot or time change and boot simultaneously.
   - OME–Modular generates a new SSL certificate with validity from build_time until (build_time +10 years) only during first boot scenarios such as firmware update, `racresetcfg`, and FIPS mode changes.
   - Upload the original PKCS certificate on the UI. For Rest API Interface, the PKCS certificate should be encrypted and pass encrypted string in Rest payload.

   NOTE: Only the users with the chassis administrator privileges can generate certificate signing requests.

Configuring alerts

This section allows you to configure the email, SNMP, and the syslog settings to trigger alerts.

NOTE: Reset Management Module causes the MM to reboot in a single MM configuration, and a failover in a dual MM configuration. This operation may take up to 10 minutes for completion, and the OME-M is unavailable during this process. Alerts are not forwarded to some of the external destinations in this duration.

Configuring email alerts

1. Click **Application Settings** > **Alerts**.
2. Click **Email Configuration**.
3. Enter the **SMTP Server Network Address**.

   NOTE: The SMTP server network address can have a maximum length of 255 characters.

4. Select **Enable Authentication** if the server requires authentication.

   NOTE: If **Enable Authentication** is selected, you must provide the username and password to access the SMTP server.

5. Enter the **SMTP Port Number**.
6. Select the **Use SSL** option if the SMTP server is configured to use SSL.
7. Select the **Email Content-Type**. The possible options are:
   - HTML
   - Plain Text
8. Click **Apply**.

Configuring SNMP alerts

The SNMP alerts contain the service tag of the chassis as one of the parameters in the trap. Third-party consoles can use this information to correlate the traps with the system.

For network IOMs and compute sleds, OME–Modular subscribes to alerts through internal private VLANs—SNMP or REST. For MXG610s fiber channel switching modules, only SNMP V1 and SNMP V3 are supported and you can configure only three SNMP alert destinations.

You can configure the SNMP alert destination for IOMs from the **Application Settings** > **Alerts** > **SNMP Configuration** page. After configuring the SNMP destination, go to **I/O Settings** > **Replicate Alert Destinations**.

NOTE: When there are multiple alert policies or destinations that are configured, there might be a delay in receiving alerts in the SNMP destination.

To configure SNMP alerts, perform the following steps:

1. From the main menu, select **Application Settings** > **Alerts**.
2. Click **SNMP Configuration**.
3. Select **Enable** to enable the configuration.
4. Enter the **Destination Address**.

   You can configure up to four SNMP destinations.
5. Select the **SNMP Version**.

   The possible SNMP versions are:
   - SNMP V1
   - SNMP V2
   - SNMP V3

   NOTE: For MX9116n or MX5108n IOMs, SNMP V2, is supported. SNMP V1 only supports MXG610s IOM.

   NOTE: The MX7000 chassis facilitates configuration of four SNMP destinations. However, the MXG610s IOM switches support only three SNMP destinations. If the fourth SNMP destination is configured, the IOM ignores it.
6. Enter the **Community String**.

   When you configure the community string for SNMP V1, by default, the community string is appended with `|common|FibreChannel11`.
7. Select the destination **Port Number** for the SNMP. The port number can be 10 to 65535.
8. Enter the **Username**, select the **Authentication Type**.

   The possible options are:
   - SHA
   - MD_5
   - None
9. Enter the **Authentication Passphrase**. Passphrase must be 8 to 32 characters long and must be a combination of an uppercase, a lowercase, a special character, and a number.
10. Select the privacy type of the user.

    The possible options are:
    - DES
    - AES_128
    - None
11. Enter the **Privacy Passphrase** for the user. Passphrase must be 8 to 32 characters long and must be a combination of an uppercase, a lowercase, a special character, and a number.
12. Click **Send** to test the SNMP trap.

    NOTE: When you select SNMP v3, the engine ID is displayed with the version number in the SNMP test trap.

Configuring sys log alerts

You can configure up to four sys log destinations.

To configure system log alerts, perform the following steps:

1. Click **Application Settings** > **Alerts** > **Syslog Configuration**.
2. Select the **Enabled** check box corresponding to the required server.
3. Enter the destination address or the hostname.
4. Enter the port number.

5

Managing compute sleds

OME–Modular enables you to allocate and manage compute sleds to balance workload demands.

You can view the list and details of compute sleds on the **Compute** page. The details are—health, power state, name, IP address, service tag, and model of the chassis. You can also select a compute sled to view the graphical representation and summary of the compute sled, on the right side of the **Compute** page.

Select a compute sled from the list to view a summary of the sled on the right side. The summary includes links to launch the iDRAC and virtual consoles, name of the compute sled, device type, service tag, management IP, model, and health.

If you have the Compute Manager privileges, you can perform the following tasks in this tab:

- **Power Control** tasks:
  - **Power Off (Non-graceful)**
  - **Power Cycle System (Cold Boot)**
  - **System Reset (Warm Boot)**
  - **Power Off (Graceful)**
  - **System Reseat**
  - **Power On**
- Turn-on or turn off LEDs using **Blink LED**.
- Refresh Inventory.

  NOTE: When a compute sled is inserted into a chassis, sometimes the message, "No device image found", is displayed. To resolve the issue, manually refresh the inventory of the compute sled.

After performing a power operation on compute sleds, some sleds do not transition to the intended state immediately. In such cases, actual state of the compute sled is updated during the next health or inventory refresh.

NOTE: If the compute sled and fabric IOM mismatch, the health status of the compute or IOM is displayed as "Warning" in the chassis subsystem health. However, the health status is not displayed in the chassis graphical representation on the **Chassis** page, I/O Modules, and **Compute** pages.

NOTE: Occasionally, you may see messages stating the device is offline. The messages are logged when the status poll for the device indicates that the device transitioned to "off" from "on".

Topics:

Viewing compute overview

On the compute **Overview** page, you can view a graphical representation of the compute on the left side. The compute information is displayed below the graphical representation. The information includes details such as iDRAC DNS name, device name preference, model, service tag, asset tag, express service code, management IP, system up time, power state, connection state, total system memory, populated DIMM slots, total number of DIMM slots, and the processor summary of the compute. You can also see the operating system and location information details.

The midsection of the **Overview** page displays the number of different **Recent Alerts** triggered in the compute. The details of the alerts are displayed below.

Below the **Recent Alerts** is the **Recent Activity** section, which displays the list of recent activities that are associated with the compute. The status and timestamp of completion of the activities are also displayed. Click **View All** to view the list of all activities in the **Jobs** page.

NOTE: The time that is displayed is based on the time zone of the system from where OME-Modular is accessed.

A graphical representation of the remote console is displayed on the right-side of the page. Below the remote console image, you can use the following links:

- **Launch iDRAC**—Displays the iDRAC user interface.
- **Launch Virtual Console**—Opens the virtual console.

The **Launch iDRAC** or **Launch Virtual Console** options are disabled based on the:

- Readiness of iDRAC
- **Power off** state of the compute sled
- Availability of express license in iDRAC
- Status of firmware update in iDRAC
- Status of the virtual console

Also, Internet Explorer and Safari have certain limitations that restrict the reuse of OME–Modular sessions. Hence, you are prompted to enter the OME–Modular user credentials to access iDRAC.

NOTE: The virtual console preview is unavailable for users with the "Viewer" **User Role** type.

A summary of information about the **Server Subsystems** is displayed below the remote console image. The information includes the health status of the components such as battery, current, fan, memory, processor, SEL/Misc, storage, temperature, and voltage.

When there is any mismatch of the storage-mapping in the compute sled, the compute health status is displayed as healthy. It is considered healthy even if the OME-Modular receives a warning alert for the compute mismatch.

NOTE: The **REASON** for **SEL/Misc** may be empty if the health of the **SEL/Misc** sub system is not ok. There are **SEL** events that do not have an associated fault that is displayed under **REASON**. In such cases, look for the hardware log for details about the **SEL** event.

The **Environment** section at the right-side bottom of the **Overview** page displays the temperature and power supply information of the compute. You can also view the power and temperature statistics for the compute.

In the **Power Statistics** window, click **Reset** to reset the power statistics and start monitoring period.

The temperature statistics may not be displayed if the server is turned off. Wait for at least 24 hours after the server is turned on for the temperature statistics to appear.

NOTE: The temperature statistics timestamp remains unchanged after a failover or management module reboot.

NOTE: The **Peak Power** value that is displayed is the last peak value irrespective of the power state of the device or component.

If you have the Compute Manager privileges, you can perform the following tasks in this tab:

- **Power Control** tasks:
  - **Power Off (Non-graceful)**—Turns off the server power, which is equivalent to pressing the forceful power button when the server is turned on. This option is disabled if the server is already turned off. It does not notify the server operating system.
  - **Power Cycle System (Cold Boot)**—Turns off and then restarts the server (cold boot). This option is disabled if the server is already turned off.
  - **System Reset (Warm Boot)**—Restarts (resets) the server without turning off (warm boot).
  - **Power Off (Graceful)**—Notifies the server operating system to turn off the server. This option is disabled if the server is already turned off.

    NOTE: For Linux operating system—Configure power settings as power off for the successful graceful shutdown operation and to avoid watchdog reboot errors. For more information, see https://topics-cdn.dell.com/pdf/red-hat-entps-lx-v70_release-notes_en-us.pdf.
  - **System Reseat**—Removes the compute sled virtually.
  - **Power On**—Turns on the server power, which is equivalent to pressing the power button when the server is turned off. This option is disabled if the server is already turned on.
- **Troubleshoot**

- **Extract SupportAssist Collection**- Allows you to extract the SupportAssist Collection logs like hardware, operating system, and RAID controller logs and store the logs in the Local, NFS, or CIFS share location.

  NOTE: Sensitive information that is captured as part of audit logs and Lifecycle Controller logs are not masked or filtered.
- **Reset iDRAC**— Helps in troubleshooting when iDRAC is noncommunicative.

- Turn-on or turn off LEDs using **Blink LED**. The available options are:
  - **1 Minute**
  - **10 Minutes**
  - **30 Minutes**
  - **1 Hour**
  - **Indefinitely**

Configuring compute settings

You can configure the following compute settings:

- Network
- Management

Configuring compute network settings

Once Quick Deploy settings are applied to a compute sled, the settings may be reported after some time due to data refresh in OME-Modular.

To configure the compute network settings:

1. Click **Devices** > **Compute** > **View Details** > **Settings** > **Network**.
2. In the **General Settings** section, select the LAN Enablement check box to configure the network settings.
3. Configure the IPv4, IPv6, and management VLAN settings.

Configuring compute management settings

To configure the compute management settings:

1. Click **Devices** > **Compute** > **View Details** > **Settings** > **Management**.
2. Configure the password to access the iDRAC console and select **IPMI over LAN** to enable access from OME–Modular to iDRAC, through BIOS.

Replacing compute sleds

The rip-and-replace feature of OME-Modular enables you to replace a failed compute sled, storage sled, or IOM, and apply the configuration automatically.

NOTE: While replacing compute sleds, ensure that the:

- Compute sled is turned off and the compute nodes in the chassis contain PERC or HBA controllers.
- SAS IOMs and storage sleds are installed in the chassis.

- When you replace a compute sled, with a service tag, with a compute sled of another service tag, and the storage sleds are mapped to the compute node slot, the power on the particular compute sled is turned off. An option to unblock power is displayed on the **Devices** > **Compute** > **Overview** page for the compute sled.
- When you remove a compute sled, containing an HBA 330 controller with shared mappings, and replace it with a compute sled containing a PERC controller, the sled is checked to ensure that no shared mappings exist. If shared mappings exist, a message is displayed on the **Devices** > **Compute** > **Overview** page for the compute sled, prompting you to clear the mapping. The compute sled is turned off.
- When you remove a compute sled containing a PERC controller with mappings, and replace it with a new compute sled having an HBA 330 controller with a different service tag, a message is displayed on the **Devices** > **Compute** > **Overview** page for the compute sled, prompting you to clear or accept the mapping. However, the compute sled is turned on in this scenario.

The following flowchart and table illustrate the behavior of OME-Modular and the LCD panel on the chassis when the compute sled is replaced:

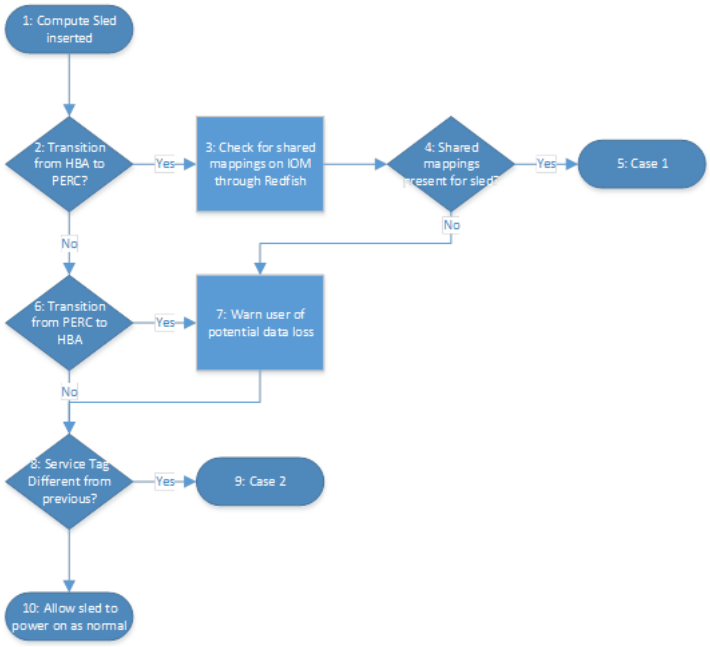


Figure 1. Compute sled replacement—flowchart

Table 19. Compute sled replacement - Behavior of OME-Modular and LCD panel

	OME-Modular behavior	LCD behavior
Case 1	Enables users to clear all mappings to the compute sled.	Enables users to clear all mappings to the compute sled.
Case 2	Enables users to clear or retain all mappings to the compute sled.	Enables users to clear or retain all mappings to the compute sled.

Viewing compute hardware

You can view the details of the hardware components that are installed in the compute sled, on the compute **Hardware** page. The hardware components include processor, storage controller, and FRU.

The deployment and configuration jobs on the compute sled are performed only for the first time, if the profile and sled device ID are unchanged. If the sled is removed and reinserted, the deployment and configuration job is not performed. This condition is applicable to the **Edit Profile** task too.

NOTE: If the storage controller cards are absent in iDRAC, the storage enclosure details are not displayed on the **Compute** > **View Details** > **Hardware** > **Storage Enclosure** page.

Viewing compute firmware

You can view the firmware list for the compute in the compute **Firmware** page. Click **Devices** > **Compute** > **View Details** > **Firmware**.

The details include name of the device or component, impact assessment, current version, and baseline version.

You can perform the following tasks on the Firmware page:

- Select a baseline from the **Baseline** drop-down to view the list of components and their current and baseline firmware versions. You can select the component for which you want to update the firmware.
- Update the existing firmware on the compute using **Update Firmware**.
- Downgrade the updated firmware version to the previous version using **Rollback Firmware**.

- Export the firmware baseline report in a `.csv` format using **Export**.

Viewing compute hardware logs

The logs of activities performed on the hardware components associated with the compute sled are displayed on the compute **Hardware Logs** page. The log details that are displayed include severity, message ID, category, timestamp, and description.

To view the hardware logs, click **Devices** > **Compute** > **View Details** > **Hardware Logs**.

You can also perform the following tasks on the **Hardware Logs** page:

- Filter the logs using **Advanced Filter**—You can filter the logs based on severity, message ID, start date, end date, or category.
- Select logs and include comments for them using **Add Comment**.
- Export logs displayed on the current page or export specific logs using **Export**.

Viewing compute alerts

You can view the list of alerts and warnings for compute sleds on the **Alerts** page.

To view the compute alerts, click **Devices** > **Compute** > **View Details** > **Alerts**.

You can sort the list of alerts based on the following advanced filters:

- Severity
- Acknowledge
- Start Date
- End Date
- Category
- Subcategory
- Message

Select an alert to view the summary on the right side of the **Alerts**.

You can also perform the following activities on the **Alerts** page.

- **Acknowledge**
- **Unacknowledge**
- **Ignore**
- **Export**
- **Delete**

6

Managing Profiles

OME–Modular allows you to create server profiles and apply them to compute sled or slot.

If a slot profile is assigned in MCM and you perform a system erase, the profile may be reapplied. If you do not want the profile to be reapplied, then unassign the profile before performing system erase.

- You can perform the following **Profile** specific operations:
  - **Create Profile**
  - **View Profile**
  - **Edit Profile**
  - **Assign Profile**
  - **Unassign Profile**
  - **Redeploy Profile**
  - **Migrate Profile**
  - **Delete Profile**

Topics:

Creating Profile

You can create profiles based on the server templates.

To create a profile:

1. On the **Profiles** page, select a profile and click **Create**.
   The **Create Profiles** wizard is displayed.
2. On the **Template** tab, **Select Template** and click **Next**.
   The **Details** tab is displayed.
3. On the **Details** tab, enter **Name Prefix**, **Description**, and **Profile Count** of the profile and click **Next**.

   NOTE: You can create a maximum of 100 profiles at a time.

   The **Boot to Network ISO** tab is displayed.
4. Select **Boot to Network ISO** and enter the following file share information and click **Next**.
   - **Share Type**—Select CIFS or NFS as required
   - **ISO Information**—Enter the ISO path
   - **Share Information**—Enter the Share IP Address, Workgroup, Username, and Password
   - **Time to Attach ISO**—Select the time duration to attach ISO from the dropdown
   - **Test Connection**—Displays the test connection status

   The **iDRAC Management IP** tab is displayed.
5. Click **Finish**.

Viewing Profile

This feature allows you to only view profile and network details of the selected profile.

- **View Profile**—You can view Boot to Network ISO, iDRAC Management IP, Target Attribute, and Virtual Identities information that is related to the profile.
- **View Network**—You can view Bandwidth and VLANs information that is related to the profile.

On the **Profiles** page, select a profile and click **View** and select **View Profile**.
The **View Profile** wizard is displayed.

Editing Profile

You can Rename and Edit the profile to change the existing settings.

Rename Profile

The **Rename Profile** wizard allows you to change the name of the profile.

1. On the **Profiles** page, select a profile and click **Edit** and select **Rename**.
   The **Rename Profile** wizard is displayed.
2. Change the name of the profile and click **Finish**.

Edit Profile

The **Edit Profile** feature allows you to change the profile name, network options, iDRAC management IP, target attributes, and unassigned virtual identities. You can edit the profile characteristics that are unique to the device or slot.

1. On the **Profiles** page, select a profile and click **Edit** and select **Edit Profile**.
   The **Edit Profile** wizard is displayed.
2. On the **Details** tab, edit name and description of the profile and click **Next**.
   The **Boot to Network ISO** tab is displayed.
3. Select **Boot to Network ISO** and enter the following file share information and click **Next**.
   - **Share Type**—Select CIFS or NFS as required
   - **ISO Information**—Enter the ISO path
   - **Share Information**—Enter the Share IP Address, Workgroup, Username, and Password
   - **Time to Attach ISO**—Select the time duration to attach ISO from the dropdown
   - **Test Connection**—Displays the test connection status

   The **iDRAC Management IP** tab is displayed.
4. Select **Target IP setiings** and click **Next**. The available options are:
   - **Don't change IP settings**—No changes are made
   - **Set as DHCP**—Select **Enable IPv4** or **Enable IPv6**
   - **Set as static IP**—Select **Enable IPv4** or **Enable IPv6** and enter the corresponding details

   The **Target Attributes** tab is displayed.
5. Select **Target Attributes** components and click **Next**. The available options are:
   - **BIOS**
   - **FC**
   - **System**
   - **NIC**
   - **iDRAC**

   The **Virtual Identities** tab is displayed.
6. View **Virtual Identity Pool** information and click **Next**.
7. Click **Finish**.

Assigning Profile

You can assign and deploy profile to a target device. The source identities displayed in the **Job Details** can be either server assigned or remote assigned which depends on the adapter behavior.

To assign a profile:

1. On the **Profiles** page, select a profile and click **Assign**.
   The **Deploy Profile** wizard is displayed.
2. On the **Details** tab, verify the details and click **Next**.
   The **Target** tab is displayed.
3. Select **Attach to Slots** or **Deploy to Devices** and click **Select Slots**.
   The **Select Device** wizard is displayed.
4. Select the device from **All Devices**, click **Finish** and then click **Next**.
   The **Boot to Network ISO** tab is displayed.
5. Select **Boot to Network ISO** and enter the following file share information and click **Next**.
   - **Share Type**—Select CIFS or NFS as required.
   - **ISO Information**—Enter the ISO path.
   - **Share Information**—Enter the Share IP Address, Workgroup, Username, and Password.
   - **Time to Attach ISO**—Select the time duration to attach ISO from the dropdown.
   - **Test Connection**—Displays the test connection status.

   The **iDRAC Management IP** tab is displayed.
6. Select **Target IP setiings** and click **Next**. The available options are:
   - **Don't change IP settings**—No changes are made.
   - **Set as DHCP**—Select **Enable IPv4** or **Enable IPv6**.
   - **Set as static IP**—Select **Enable IPv4** or **Enable IPv6** and enter the corresponding details.

   The **Target Attributes** tab is displayed.
7. Select **Target Attributes** components and click **Next**. The available options are:
   - **BIOS**
   - **FC**
   - **System**
   - **NIC**
   - **iDRAC**

   The **Virtual Identities** tab is displayed.
8. View **Virtual Identity Pool** information and click **Next**.
   The **Schedule** tab is displayed.
9. Select **Schedule** option from the following:
   - **Run Now**—Select this option to deploy the profile to the server immediately.
   - **Enable Schedule**—Select this option to select the date and time for the profile deployment.

   NOTE: The **Enable Schedule** option is disabled for slot-based profile deployment.

   NOTE: When you select **Enable Schedule**, the profile deployment runs at the scheduled time, even if you have already performed **Run Now** before the schedule. The Deploy Profile job fails when it is run at the scheduled time and an error message is displayed.
10. Click **Finish**.

Unassigning Profile

You can **Unassign** the profile from the selected targets and disassociate the profiles from the targets. You can select only the profiles that are in assigned or deployed state. To unassign the profile:

1. Select the profile that you want to unassign.
2. Click **Unassign** from the actions menu. The **Unassign Profile** window is displayed.
3. On the **Unassign** profile wizard, **Force Reclaim Identities** is checked by default. This action reclaims the identities from this device, and the server is forcefully rebooted. All the VLANs configured on the server are removed.

4. Click **Finish**.

   NOTE: The **Unassign profile** job is not created when the action is performed on the assigned profile that has the Last Action Status as **Scheduled** for device-based deployment.

Redeploying Profile

You can redeploy profiles which are in the deployed profile state.

When **Quick Deploy** and **Profile** settings are enabled for the slot, a deployment and configuration job is created every time that a sled inserted. If the profile contains RAID attributes, the RAID settings are reconfigured. Disable **Quick Deploy** when RAID configuration exists in the profile.

NOTE: After performing a `racresetcfg -all` task, reboot the system fully before redeploying a profile.

To redeploy the profile:

1. On the **Profiles** page, select a deployed profile that you want to redeploy and click **Redeploy**.
   The confirmation request wizard is displayed.
2. Click **Yes** to confirm the redeploy profile action.
   The Redeploy wizard is displayed.
3. On the **Attribute Deploy Options** tab, select **Modified attributes only** or **All attributes**. If the reboot is required, select the **Do not forcefully reboot the host OS if the graceful reboot fails** option and click **Next**.
   The Schedule tab is displayed.
4. Select the schedule option to redeploy the profile. The available options are **Run Now** and **Enable Schedule**.
5. Click **Finish**.

Migrating Profile

You can migrate a profile from one server to another. The system unassigns the identity from the first server before the migration. If the unassignment fails, the system displays a critical error. You can override the error and force the migration to a new server.

NOTE: If identities are not part of the source template, the associated source device is not turned off after migrating profiles.

To migrate profile settings:

1. On the **Profiles** page, select a profile and click **Migrate**.
   The **Migrate Profile** wizard is displayed.
2. On the **Selection** pane, click **Select Target**.
   The **Select Devices** wizard is displayed.
3. Select the device or chassis to which you want to migrate the profile. Click **Finish** and click **Next**.
   The **Schedule** tab is displayed.
4. Select the schedule option to migrate the profile settings. The available options are **Run Now** and **Enable Schedule** .
5. Click **Finish**.

Deleting Profile

You can delete profiles which are not running any profile actions and is in the unassigned profile state.

To delete the profile:

1. On the **Profiles** page, select profiles that you want to delete and click **Delete**.
   The confirmation request wizard is displayed.
2. Click **Yes** to confirm the deletion.

7

Managing storage

This chapter describes the Storage and IOM features of OME–Modular. It also provides details about performing various storage-related tasks. The SAS IOMs manage the storage enclosures. SAS IOMs facilitate communication between storage and compute sled and also help in assigning the storage to the compute sleds. You can assign storage devices as:

- Specific drive bays storage to compute sleds
- Entire storage enclosure to compute sleds

You can use the options available on the storage page to perform power operations, update firmware, manage hardware settings, and configure alerts for the storage devices.

For more information about SAS Storage, see Managing SAS IOMs.

Topics:

Storage overview

On the **Storage Overview** page, you can view all the storage enclosures that are installed in the chassis. You can also perform a virtual reseat of the storage enclosure and blink the LEDs to identify the storage enclosures.

To view the available storage enclosures or sleds:

1. From the **Devices** drop-down menu, select **Storage**.
2. Select the storage sled from the list of the storage devices.
3. Click **View Details**.

The storage **Overview** page is displayed.

Performing a storage system reseat

You can perform a system reseat remotely using the OME–Modular. The system reseat option simulates a physical sled removal and reinstallation.

To perform storage system reseat:

1. From the **Devices** drop-down menu, select **Storage**.
2. Select the storage sled you want to reseat.
3. Click **Power Control** and click **System Reseat**.
4. Click **Confirm**.

NOTE: The storage sled, if assigned to compute sleds that are powered on, causes input/output disruption.

Blinking LED

You can locate a storage sled within a chassis by making the sled LED blink. This is helpful in identifying a system. To turn on the LED blinking:

1. From the **Devices** drop-down menu, select **Storage**.
2. Select the storage sled.
3. Click **Blink LED** and click **Turn On**.

To turn off the LED blinking:

1. From the **Devices** drop-down menu, select **Storage**.
2. Select the storage sled.
3. Click **Blink LED** and click **Turn Off**.

You can pull out the storage sled trays from the chassis to access the storage sled drives. When a tray is opened, the storage sled drive is away from the chassis and does have cooling support causing the temperature of the drive to reach a critical level. When the tray is opened, the LCD displays count down timer starting from five minutes. Close the tray within five minutes for cooling the storage drive. Also, if another tray containing a storage sled drive is opened, the current warning display is not affected. You can dismiss the LCD warning display.

NOTE: The LCD display for storage-mapping owing to server replacement takes priority over opening of the storage tray. If LCD has completed displaying storage-mapping menus and a storage tray is still open, a warning, stating the storage tray is open, is displayed.

Editing storage sled assignments

You can change the assignments of the device using **Edit Assignments** option. To edit assignments:

- On the storage **Overview** page, click **Edit Assignments**.

  The **Hardware** page is displayed.

- Select the hardware component, and change the assignment. For more information, see Assigning drives to a compute sled.

Other information

On the **Hardware** page, you can view more information about the device as follows:

- **Storage Enclosure Information**—Provides the information of an enclosure, such as **Name**, **FQDD**, **Model**, **Service Tag**, **Asset Tag**, **Power State**, **Firmware Version**, **Drive Slot Count**, and **Assignment Mode**
- **Chassis Information**—Provides the information of a chassis, such as **Chassis**, **Slot Name**, and **Slot**
- **Connected I/O Module Information**—Provides the information of an I/O module such as **I/O Module Name** and **Multipath**
- **Recent Alerts**—Provides the list of the recent alerts
- **Recent Activity**—Provides the list of recent activities
- **Storage Subsystems**—Provides the list of storage subsystem
- **Environment**—Provides the information of the power usage

Viewing hardware details

The hardware components of a storage sled consist of hard drives, enclosure management modules (EMMs), Field Replaceable Unit (FRUs), and installed software. To view the details of hardware components in the storage sled:

1. From the **Devices** drop-down, select **Storage**.
2. Select a storage from the list of the storage devices.
3. On the right side, click **View Details**.
4. To view the hardware details, click **Hardware**. The hardware components in the storage sled are displayed at the top of the **Hardware** page.

Viewing drive details

To view the list of drives in the storage sled, click **Hardware** > **Hard Drives**. You can assign a hard drive to a compute sleds.

NOTE: Use the iDRAC web interface to update the firmware for a drive.

Current Mode—Indicates if the hard drive is assigned to an enclosure or to a single compute node slot.

- **Enclosure-Assigned**—In this mode, you can assign an entire storage sled to one or more compute node slot.

  NOTE: You cannot assign storage when a redundant SAS IOM setup is temporarily degraded to nonredundant state.

  NOTE: The storage enclosure is assigned to the slots of the compute slots and not to the sled itself. If a compute sled is replaced with another sled on the same slot, then the storage enclosure gets assigned to the new sled automatically. However, if you move the compute sled from one slot to another, you must remap the storage to that sled.
- **Drive-Assigned**—In this mode, you can select a hard drive slot and assign it to a compute node slot.

  CAUTION: Assigning a hard drive to a compute node slot may result in loss of data.

  NOTE: If the SAS IOM is unavailable, the **Current Mode** is displayed as Unknown. This indicates that there is a communication failure and no assignments can be done.
- The **Current Slot Assignment(s)**—In this mode, you can view the number of storage-compute sled mappings.

  NOTE: When a SAS IOM is power that is cycled, the storage-IOM mapping information is displayed after five minutes.

  NOTE: The storage assignment times vary, based on the number of compute slots that are selected.

  NOTE: Replace the storage sleds one at a time, to retain the storage mapping after replacing a sled with empty service tag.

Assigning drives to a compute sled

Using the **Drive-Assigned** mode, you can map the drives in a storage enclosure to a compute sled slot. If the compute sled fails, the drive remains assigned to the slot. If the sled is moved to another slot on the chassis, reassign the drives to the new slot. To configure RAID on the drives, use the iDRAC web interface, a server configuration profile, or an operating system deployment script, after the drive assignment is complete.

CAUTION: Before you assign a drive to a slot, ensure that the data from the drive is backed up.

NOTE: The HBA330 controller card does not set a status for the hard drives when the hard drives are removed from the storage sleds after the hard drives are assigned to compute sleds.

To assign a drive:

1. From the **Devices** drop-down, select **Storage**.
2. Select the storage sled from the list of the storage devices.
3. Click **View Details**.
   The storage **Overview** page is displayed.
4. Click **Hardware**.
   The drive list is displayed.

   NOTE: Ensure that the **Drive-Assigned** mode is selected.
5. Select one or more drives and click **Assign Drive to Slot**.
   The **Assign Hard Drive to Compute** page is displayed.
6. Select the slot and click **Assign**.

   When a drive is reassigned from one compute sled to another, the enclosure status and spin-up state of the drive is the same. If a drive is in power-savings mode, the status of the drive is displayed as "starting".

Assigning storage enclosure to a compute sled

Using the **Enclosure-Assigned** mode, you can assign a storage enclosure to one or more compute sleds with HBA330 minimezzanine adapter. Using this mode, you can also assign a storage enclosure to an empty slot. If the sled is removed and installed to another slot the assignment must be performed again.

CAUTION: Before you assign an enclosure to a slot, ensure that the data from the drive is backed up.

NOTE: Systems with H745P MX controller only support a single storage enclosure mapping.

To assign an enclosure:

1. From the **Devices** drop-down list, select **Storage**.
2. Select the storage sled from the list of the storage devices.
3. Click **View Details**.
   The storage **Overview** page is displayed.
4. Click **Hardware** and select **Enclosure-Assigned**.
   A warning message about loss of data while selecting this mode is displayed.
5. Select **I understand that reseting this assignment could result in data loss** and click **Ok**.
6. Select the compute sled slots and click **Assign**.
   After replacing PERC card, wait for some time for OME–Modular to get the new inventory details from iDRAC before performing the assignment operation. Else, refresh the inventory on the **Compute** page, manually.

Replacing storage sleds

When you remove a storage sled from one slot and insert it into another slot on the chassis, the mapping on the new slot is used for the storage sled. If you replace the storage sled with a new sled which does not have a service tag, the service tag and the mapping of the sled that was present in the slot earlier, are applied. However, the storage sled firmware is not replaced automatically.

Updating enclosure firmware

You can update or rollback the storage enclosure firmware using the OME–Modular. Use the following methods to update the firmware:

1. Dell Update Package (DUP)
2. Catalog-based compliance method

NOTE: The OME–Modular is inaccessible during the update process.

Updating the firmware using DUP

1. Download the DUP from www.dell.com/support/drivers.
2. On the OME–Modular web interface, go to **Devices** > **Storage**.
3. Select the storage sled on which you want to update the firmware.
4. Click **Update Firmware**.
5. Select the **Individual package** option and click **Browse** to go to the location where you have downloaded the DUP.
   Wait for the comparison report, the supported components are displayed.
6. Select the required components and click **Update** to start the firmware update.
7. Go to the **Monitoring** > **Jobs** page to view the job status.

Updating the firmware using catalog-based compliance

1. On the OME–Modular web interface, go to **Devices** > **Storage**.
2. Select the storage sled on which you want to update the firmware.
3. Click **Update Firmware**.
4. Select the baseline and click **Next**.
   The Schedule Update page is displayed.
5. Select the **Schedule Update** options as required.
   - **Update Now**—apply the firmware updates immediately.
   - **Schedule Later**—schedule the firmware updates for a later date. Select the required date and time.
   - **Server Options**—choose to apply the update as required.

- **Reboot server immediately**—Select this check box to send the update and reboot the server immediately. You can select the reboot options from the drop-down, the available options are:
  - Graceful Reboot with Forced Shutdown
  - Graceful Reboot without Forced Shutdown
  - Power Cycle
- **Stage for next server reboot**—Select this check box to send the update to the server. However, the update is installed only the next time the server is rebooted.

Downgrading storage enclosure firmware

Follow these steps to roll back the firmware for a storage enclosure:

1. On the OME–Modular web interface, go to **Devices** > **Storage**.
2. Select the system and click **View Details**.
3. Click **Rollback Firmware**.
4. Select the available version of the firmware and click **Confirm** to continue.

Managing SAS IOMs

The internal connection of the storage subsystem is called "Fabric C", which serves as a communication mode between compute sleds and storage enclosures. The "Fabric C" is used for SAS of FC storage connectivity and includes a midplane. SAS IOMs allow creating storage assignments in which you can map storage enclosure drives or whole storage enclosures to compute sleds. SAS IOMs provide multi-path input out access for compute sleds to drive elements. The active module manages the SAS IOM and is responsible for all inventory and storage assignments on the fabric.

A single width compute sled can support one Fab-C mezzanine card that connects to each IOM through a x4 link. Each lane in the link supports 12Gbps SAS for a total of 48Gbps link to each SAS IOM. In SAS IOMs, the Fab-C IOMs are used to provide SAS switching between compute sleds and internal storage sleds such as PowerEdge MX5016s.

For information on the tasks that you can perform on the I/O Modules page for SAS, see Managing IOMs.

SAS IOM Overview

The SAS IOM **Overview** page displays details of the IOM, chassis, the list of recent alerts, and recent activities. The IOM information consists of the model, power state, firmware version, fabric type, and management role of the IOM. The management roles can be of three types:

- Active
- Passive
- Degraded

A healthy system has one "Active" and one "Passive" SAS IOM.

The chassis information consists of the name of the chassis, slot name, and slot number.

Information about the SAS IOM storage subsystems is also displayed on the right side of the **Overview** page. The storage subsystem information consists of the name of the subsystem and health status. Click **View Details** to view the alerts and alert details. The details consist of the message ID, message, timestamp when the alert was triggered, and recommended action.

To view the IOM overview:

1. From the menu bar, click **Devices** > **I/O Modules**. The **I/O Modules** list page is displayed.
2. Select the IOM whose details you want to view. A summary of the selected IOM is displayed on the right side. The summary consists of the name of the IOM, device type, management IP, model, health status, and availability.
3. Click **View Details**. The **Overview** page is displayed.

On the **IOM Overview** page, you can perform the following tasks:

- Power Control—Turn on, turn off, power cycle, or system reseat operations.
  - Turn on or turn off—When you turn off the IOM, the status of the IOM is "Offline". As a result, status of the peer IOM may be "Active". When you power cycle the IOM, it causes a warm reboot of the IOM.
  - Power Cycle—The Power Cycle option initiates a warm reboot of the IOM. In this instance, the power is not removed from the IOM and the core systems of the IOM reboot.

- System Reseat—The System Reseat option removes the IOM virtually. In this instance, the power is removed from the IOM and the IOM reboots.

  NOTE: After the power reseat of the SAS IOM, the IOM turns on within a minute. Any mismatch in the power status of the IOM is corrected through refreshing the inventory or is corrected automatically with the default inventory task.

- Blink LED—Turn on or turn off to identify the IOM LEDs.
- Clear Configuration—Delete the storage IOM configuration.
- Extract Log—Extract the IOM activities log to a CIFS or NFS share location.
- View a list of the latest alerts and the date and time when the alerts were generated, in the **Recent Alerts** section. To view a list of all alerts click **View All**. The **Alerts** page with all alerts that are related to the IOM is displayed.
- View a list of all activities that are related to the IOM, the rate of completion of the activity, and the date of time when the activity began, in the **Recent Activity** section. To view a list of all activities that are related to the IOM, click **View All**. The **Jobs** page with a list of all the jobs that are related to the IOM is displayed.
- View the power statistics of the IOM by clicking **View Power Statistics** in the **Environment** section. The statistics comprise peak power timestamp, minimum power timestamp, date, and time from when the statistics is recorded. Click **Reset** to reset the power statistics data.

NOTE: If you perform the **Clear** operation on a SAS IOM, the IOM becomes active, if it is not already active and, the storage configuration on both the SAS IOMs is cleared.

NOTE: Resolve any suboptimal health of the IOM, other than firmware mismatch, before updating the firmware. This action ensures that the firmware is updated without downgrading the health of the SAS IOM.

Force active

You can use **More Actions** > **Force Active** to perform a failover on a "Passive" or "Degraded" switch. Performing a "Force Active" operation on the SAS IOM is considered a disruptive operation and must only be used if necessary. When you perform a "Force Active" operation, the SAS IOM becomes "Active" and the associated storage configuration is applied to the chassis.

You can use the **Force Active** option to resolve mismatches that occur when:

- The switches were configured earlier but are inserted in a chassis that did not have SAS IOMs earlier.
- Two switches from two different chassis are inserted into a third chassis.

You can also use **Force Active** as a preemptive action for servicing a switch. Ensure that the remaining switch is "Active" before removing the switch that must be serviced. This in turn, prevents any disruption to the fabric that might occur if the switch is removed when the other switch is "Passive".

Clearing configuration

You can clear the storage configuration of the SAS IOMs using **More Actions** > **Clear**. When you click **Clear**, the SAS IOM becomes "Active" and the storage configuration is cleared from the chassis.

You can use the **Clear** option to:

- Reset a chassis configuration in one step.
- Resolve a mismatch, where two switches from two different chassis are inserted into a third chassis. In this scenario, it is unlikely that the two switches have a correct configuration. Use the **Clear** option to wipe the existing configuration and create a correct configuration.

Use the **Force Active** and **Clear** options to act upon some critical and warning messages that are displayed in the OME–Modular web interface, particularly, for a configuration mismatch.

Extracting IOM logs

You can collect a log bundle for support by selecting **Extract Log**. The log bundle collected from the SAS IOM also contains the associated logs from all storage enclosures that are discovered by the IOM even if they are not currently present in the chassis.

8

Managing templates

OME–Modular allows you to configure servers based on templates. A server template is a consolidation of configuration parameters that are extracted from a server and used for replicating the configuration to multiple servers quickly. A server profile is a combination of template and identity settings that are applied to a specific or multiple servers, or saved for later use.

You must have the template management privilege to create templates. A server template consists of the following categories:

- BIOS
- SupportAssist
- NIC
- System
- EventFilters
- LifecycleController
- iDRAC

To view the list of existing templates, click **Configuration** > **Template**. The **Deploy** page is displayed.

You can sort the list of templates that are based on the name and status of the template.

On this page, you can perform the following tasks:

- Create Template
- Edit Template
- Clone Template
- Export Template
- Delete Template
- Edit Network
- Deploy Template

Following are the list of secured attributes for restored templates:

Attribute Header	Attribute
iDRAC config	
USB Management	USB 1 Password for .zip file on USB
RAC Remote Hosts	RemoteHosts 1 SMTP Password
Auto Update	• AutoUpdate 1 Password • AutoUpdate 1 ProxyPassword
Remote File Share	RFS 1 Remote File Share Password
RAC VNC Server	VNCServer 1 Password
SupportAssist	SupportAssist 1 Default Password
LDAP	LDAP 1 LDAP Bind Password

Topics:

- Deploying templates

Viewing template details

To view the template details.

1. On the **Template** page, select the template of which you want to view the details.
   A summary of the template is displayed on right side.
2. Click **View Details**.
   The **Template Details** page is displayed.

   The details that are displayed are—name and description of the template, reference device, timestamp when the template was last updated, and the name of the user who last updated it. You can also view the configuration details such as BIOS, SupportAssist, NIC, System EventFilters, LifecycleController, and iDRAC information.

   You can perform the following tasks on the **Template Details** page:

   - Deploy Template
   - Edit

Creating templates

You can create templates in the following ways:

- Clone from an existing server—**Reference Device**
- Import from an external source—**Import from File**

To create a template from a reference device:

1. On the **Templates** page, click **Create Template** and select **From Reference Device**.
   The **Create Template** wizard is displayed.
2. Enter the name and description for the template and click **Next**.
   The **Reference Device** tab is displayed.
3. Click **Select Device** to view the **Select Devices** window where you can select the device or chassis based on which you want to create the template.

   To deploy virtual identities for NIC, select NIC and iDRAC.

   To deploy virtual identities for fibre channel, you must select iDRAC, NIC, and Fibre Channel.

4. Select the configuration elements that you want to clone.

Importing templates

To import an existing template:

1. On the **Templates** page, click **Create Template** and select **Import from File**.
   The **Import Template** window is displayed.
2. Enter a name for the template and **Select a file** to go to the location where the template that you want to import is stored.

Editing templates

The **Edit Template** feature allows you to change the name and description of the template.

1. On the **Templates** page, select a template and click **Edit**.
   The **Edit Template** wizard is displayed.
2. On the **Template Information** tab, enter the name and description of the template and click **Next**.
   The **Edit Components** tab is displayed.
3. On the **Edit Components** tab, click **Guided View**. You can edit the following components.
   - **BIOS**—Select the configuration method for the BIOS settings.

     NOTE: The **Deploy Template** job fails when you select **DenseCfgOptimized** and **PerfPerWattOptimizedOs** attributes. These are predefined attributes which are not displayed in the system profile list.

- **Boot**—Select the Boot mode for the Boot settings
- **Networking**—Select the NIC Teaming and click edit icon to modify the template. On the **Edit Template** wizard, modify the following components and click **Finish**.
  - Untagged Network
  - Tagged Network
  - Min Bandwidth (%)
  - Max Bandwidth (%)

4. Click **Advanced View** to select the following components or attributes to include in the template and click **Next**.
   - BIOS
   - FC
   - SupportAssist
   - NIC
   - System
   - EventFilters
   - Lifecycle Controller
   - iDRAC
   - RAID

   The **Summary** tab is displayed.
5. Verify the selected components and their configurations in the **Summary** tab.
6. Click **Finish**.

Refreshing templates

The **Refresh Template** feature allows you to update the existing template. You can update the template from the Reference device or Local file (xml). During template refresh, ensure that the FQDD components selected are the same. Else, the refresh template task fails. If a refresh template task fails, the original template and its associated attributes are retained.

1. On the **Templates** page, select a template and click **Edit** > **Refresh Template**.
   The **Refresh Template** wizard is displayed.
2. On the **New Template Association** section, select **New Reference Device** option to update the template using a new reference device.
3. On the **Local File** section, click **Select File** to go to the location where the external file is located.
4. On the **Current Reference Device** verify the reference device that is selected.
5. Click **Finish** to create template association.

Cloning templates

To create a copy of a template:

On the **Templates** page, select the template of which you want to create a copy, and click **Clone**.

Exporting templates

You can export a template to a network share or a local drive on your system.

To export a template:

On the **Templates** page, select the template that you want to export and click **Export**.
A message is displayed to confirm the export action. The template is exported in `.xml` format to a local drive on your system or a network share.

Deleting templates

To delete templates:

1. On the **Templates** page, select templates that you want to delete and click **Delete**.

A message is displayed prompting you to confirm the deletion.

2. Click **Yes** to proceed.

   When a template is deleted, the unassigned identity pools in the template are restored to the identity pool.

   NOTE: You cannot delete a template, if there are profiles that are created using the template.

Editing template networks

To edit template network details:

1. On the **Templates** page, select the template whose network details you want to modify and click **Edit Network**. The **Edit Network** window is displayed.
2. Modify the **Identity Pool**, if necessary.
3. Select the NIC teaming option for the port.

   NIC teaming is suggested for redundancy, though it is not required. NIC Partitioning (NPAR) can impact how NIC teaming operates. Based on restrictions that are related to NIC partitioning, which NIC vendors implement, certain configurations prevent certain types of teaming. The following restrictions are applicable to both Full Switch and SmartFabric modes:

   - If NPAR is not used, both Switch-dependent (LACP) and Other (Switch-independent) teaming methods are supported.
   - If NPAR is used, only Other (Switch-independent) teaming methods are supported. Switch-dependent teaming is not supported.

   The NIC teaming feature is applicable to IOM versions 10.5.0 and later.

   Refer to the network adapter or operating system documentation for detailed NIC teaming instructions.

   The available NIC teaming options are:

   - No Teaming—NICs are not bonded and provide no load balancing or redundancy.
   - LACP—Also referred to as Switch Dependent, 802.3ad or Dynamic Link Aggregation. The LACP teaming method uses the LACP protocol to understand the teaming topology. It provides Active-Active teaming with load balancing and redundancy. With this option, only the native VLAN is programmed on non-LAG interfaces. All tagged VLANS wait until the LACP LAG is enabled on the NICs. The following restrictions are applicable to LACP teaming:
     - The IDRAC shared LOM feature can only be used if “Failover” option on IDRAC is enabled.
     - If the host operating system is Windows, the LACP timer must be set to “slow” (also referred to as “normal”).
   - Other—Refers to a NIC teaming method where the switch is unaware of the teaming technology that is used. The "other" option involves using the operating system and NIC device drivers on the server to team the NICs. Each NIC vendor may provide slightly different implementations with different pros and cons.

4. Select or clear the **Propagate VLAN Settings**. Selecting this option will propagate any changes to VLAN settings to sleds which were previously targeted by this template.

Deploying templates

You can deploy templates from the **Deploy Template** and **Template Details** pages.

After a template is deployed on one or more servers along with VLAN configurations, if you make a mistake or decide to change the existing VLAN configurations on the Fabric Manager, perform the deployment workflow again. In the deployment workflow, the server is deployed after the VLAN is configured on the Fabric Manager.

The system-specific attributes that are defined in the template are not deployed automatically. Redefine the attributes for the target system that is selected for the deployment. Use **Quick Deploy** to set the VLAN ID for the system.

If the `OneTimeBootMode` attribute is disabled, then you cannot set the `OneTimeUefiBootSeq` or `OneTimeHddSeq` attributes.

Before applying the server templates, ensure that:

- The number of ports in the profile matches that of the server on which you want to deploy the template.
- All the server ports on the servers that are connected through the MX7116n Fabric Expander Module are connected to the IOMs properly.

When you deploy an imported template where NPAR is enabled, it does not configure the bandwidth settings on fabric mode IOMs.

NOTE: Templates that are created on the earlier versions of iDRAC may fail during deployment, when tried on the latest versions of iDRAC.

NOTE: Deployment Configuration job is created automatically, if the profile is already attached to the slots when the **SystemErase** task is performed on the sled.

NOTE: The **Workgroup** option in the **Boot to Network ISO** tab is available only if the **Share Type** is CIFS.

The source identities that are displayed in the **Job Details** can be either server that is assigned or remote assigned which depends on the adapter behavior.

To deploy a template from the **Templates** page:

1. Select the required template, and click **Deploy Template**.
   If the template has identity attributes, but is not associated with a virtual identity pool, an error message is displayed. Else, the **Deploy Template** wizard is displayed.
2. On the Target tab, select the target devices or slot on which you want to deploy the template. Select the **Do not forcefully reboot the host OS if the graceful reboot fails** option if the reboot is required.

   If you select an occupied slot, the **Immediately Apply Template to Compute Sleds** check box is enabled. Select the check box to reseat the compute sled immediately and deploy the template on it.

   Selecting the **Do not forcefully reboot the host OS if the graceful reboot fails** option prevents a nongraceful reboot of the compute sled.

   NOTE: OME-Modular Deployment Boot to network ISO may fail when iDRAC and ISO Share are in different unreachable networks. The TEST CONNECTION may be successful if OME-Modular and ISO Share are in reachable networks. But, iDRAC can be in an unreachable network. The failure could be due to network protocol restrictions.

   NOTE: Rack Slot and Rack Name are not populated automatically, as they are target-specific attributes which are different for each device. You can select and add rack details to include iDRAC attributes to the selected device. This may be applicable to other target-specific attributes too.

3. Select **Boot to Network ISO** and enter the following file share information and click **Next**.
   - **Share Type**—Select CIFS or NFS as required.
   - **ISO Information**—Enter the ISO path.
   - **Share Information**—Enter the Share IP Address, Workgroup, Username, and Password.
   - **Time to Attach ISO**—Select the time duration to attach ISO from the dropdown.
   - **Test Connection**—Displays the test connection status.

   Boot to network ISO operation is not initiated when deploy template job results in attribute failure.

   The **iDRAC Management IP** tab is displayed.
4. Select **Target IP setiings** and click **Next**. The available options are:
   - **Don't change IP settings**—No changes are made.
   - **Set as DHCP**—Select **Enable IPv4** or **Enable IPv6**.
   - **Set as static IP**—Select **Enable IPv4** or **Enable IPv6** and enter the corresponding details.

   The **Target Attributes** tab is displayed.
5. Select **Target Attributes** components and click **Next**. The available options are:
   - **BIOS**
   - **FC**
   - **System**
   - **NIC**
   - **iDRAC**

   The **Schedule** tab is displayed.
6. Select **Schedule** option from the following:
   - **Run Now**—Select this option to deploy the template immediately.
   - **Enable Schedule**—Select this option to select the date and time for the template deployment.
7. Click **Finish**.

9

Managing identity pools

Identity pools are used in template-based deployment of servers. They facilitate virtualization of network identities that are required for accessing systems using Ethernet, iSCSI, FCoE, or Fibre Channel (FC). You can enter the information that is required for managing the I/O identities. The identities, in turn, are managed by chassis management applications such as OME–Modular.

When you start a server deployment process, the next available identity is fetched from the pool and used for provisioning a server from the template description. You can migrate the server profile from one server to another without losing access to the network or storage resources.

You can also associate server profiles with slots. The server profile uses the reserved identity from the pool to provision a server.

To view the list of identity pools, click **Configuration** > **Identity Pools**.

The **Identity Pools** page is displayed with the list of available identity pools and their key attributes. You can perform the following tasks on the **Identity Pools** page:

- Create identity pools
- View identity pools
- Edit identity pools
- Delete identity pools
- Export identity pools

For Intel NICs, all partitions on a port share the same IQN. Hence, a duplicate iSCSI IQN is displayed on the **Identity Pools** > **Usage** page when the **View By** option is iSCSI.

You can also use the RESTful API commands to create and edit identity pools.

NOTE: The **Identity Pools** page displays the MAC association even if the deployed template for the destination device is deleted.

Topics:

Creating identity pools

You can create up to 4096 MAC addresses in an identity pool. An error message is displayed when:

- There are errors such as overlap in identity values with an existing pool.
- Syntax errors while entering the MAC, IQN, or network addresses.

Each identity pool provides information about the state of each identity in the pool. The states could be:

- Assigned
- Reserved

If the identity is assigned, the information about the assigned server and NIC Identifier is displayed. If the identity is reserved, the information about the assigned slot in the chassis is displayed.

You can create an identity pool with only the name and description and configure the details later.

NOTE: You can clear identities by disabling the **I/O Identity Optimization** option in iDRAC.

To create identity pools:

1. Click **Configuration** > **Identity Pools**.

The **Identity Pools** page is displayed with the list of available identity pools and their key attributes.

2. Click **Create**.
   The **Create Identity Pool** wizard is displayed.
3. Enter a name and description for the identity pool and click **Next**.
   The **Ethernet** tab is displayed.
4. Select **Include Ethernet virtual MAC Addresses** to enter the **Starting virtual MAC Address**, select the **Number of Virtual MAC Identities** you want, and click **Next**.

   The MAC addresses can be in the following formats:

   - `AA:BB:CC:DD:EE:FF`
   - `AA-BB-CC-DD-EE-FF`
   - `AABB.CCDD.EEFF`

   You can choose to create the identity pools from iSCSI, FCoE, or FC.

   The **iSCSI** tab is displayed.
5. Select the **Include virtual iSCSI MAC Addresses** to enter the **Starting virtual MAC Address** and select the **Number of iSCSI MAC addresses** or IQN addresses you want.
6. Select the **Configure iSCSI Initiator** to enter the **IQN Prefix**.

   The pool of IQN addresses is generated automatically by appending the generated number to the prefix in the format—`<IQN Prefix>.<number>`
7. Select the **Enable iSCSI Initiator IP Pool** to enter the **IP Address Range**, **Subnet Mask**, **Gateway**, **Primary DNS Server**, and **Secondary DNS Server**.

   The iSCSI Initiator IP settings are used only when the iSCSI is configured for booting, and when the iSCSI Initiator configuration through DHCP is disabled. When iSCSI Initiator configuration through DHCP is enabled, all these values are obtained from a designated DHCP server.

   The IP Address Range and Subnet Mask fields are used to specify a pool of IP addresses that OME–Modular can assign to a device. The device can use the IP in the iSCSI Initiator configuration. Unlike the MAC address pools, a count is not specified for the IP Address Range. The pool of IP addresses can also be used to generate the initiator IP. OME–Modular supports the IPv4 format of IP addresses range in the following formats:

   - `A.B.C.D - W.X.Y.Z`
   - `A.B.C.D-E, A.B.C.`
   - `A.B.C.D/E`—This format is a Classless Inter-Domain Routing (CIDR) notation for IPv4.

   A maximum of 64,000 IP addresses is allowed for a pool.

   OME–Modular uses the Gateway, Primary DNS, and Secondary DNS server values while deploying a template instead of using the values in the template.OME–Modular does not assign the Gateway, Primary DNS, and Secondary DNS server values from the IP address pool, if the values are within the specified IP address range. The Gateway, Primary DNS, and Secondary DNS server values serve as exclusions from the specified IP Address Range, when applicable.
8. You can select the **Include FCoE Identity** to enter the **FIP MAC Address** and select the number of **Number of FCoE Identities** you want.

   The WWPN/WWNN values are generated from the MAC address. The WWPN address is prefixed with `0x2001` while the WWNN address is prefixed with `0x2000`. This format is based on an algorithm similar to FlexAddresses.
9. Select the **Include FC Identity** to enter the **Postfix (6 octets)** and select the **Number of WWPN/WWNN Addresses**.

Viewing identity pools

You can view the details of the identity pool.

Select the required identity pool to view the summary and usage details of the identity pool.

- **Summary**—Displays the Date Created, Last Updated, and protocol details of the identity pools.
- **Usage**—Displays the following details of the selected identity pools.
  - Conflict
  - Virtual MAC Address
  - State
  - Profile name
  - Chassis name

- Slot
- Name
- Management IP
- NIC Identifier

You must have the template management privilege to manage identity pools. You can filter and view the usage details by:

- Ethernet
- iSCSI
- FCoE
- FC

NOTE: The identity state is displayed as **Used** for the identities that are assigned to the device from an external source. For example, identities deployed directly using iDRAC interface.

Editing identity pools

You can modify the number of entries in the identity pool. However, you cannot reduce the size of the identities that are already assigned or reserved. For example, in a pool of 100 MAC addresses, if 94 of the addresses are assigned or reserved, you cannot reduce the number of MAC addresses to less than 94.

To edit an identity pool:

1. On the **Identity Pools** page, select the identity pool and click **Edit**.
   The **Edit Identity Pool** window is displayed.
2. Make the required changes.

Exporting identity pools

You can export the identity pools in a `.csv` format to a network share or local drive on your system.

To export identity pools:

On the **Identity Pools** page, select the identity pools and click **Export**.

Deleting identity pools

You can delete identity pools that are not assigned or reserved. When you attempt deleting identity pools that are associated with templates, a warning message is displayed.

To delete identity pools:

On the **Identity Pools** page, select the identity pools that you want to delete and click **Delete**.

10

Ethernet IO Modules

The MX7000 supports the following Ethernet I/O Modules (IOMs):

- Managed Ethernet switches:
  - MX9116n Fabric Switching Engine
  - MX5108n Ethernet Switch
- Unmanaged devices:
  - MX7116n Fabric Expander Module
  - PowerEdge MX 25 Gb Ethernet Pass-Through Module
  - PowerEdge MX 10GBASE-T Ethernet Pass-Through Module

Ethernet IOMs are supported in Fabrics A and B. For details about the supported IOM slots, see Supported slot configurations for IOMs.

The Ethernet switches operate in two modes:

- Full Switch mode (default)
- SmartFabric Services mode or Fabric mode

By default, an Ethernet switch operates in Full Switch mode.

In Full Switch mode, the switch operates as a full L2/L3 switch with all functionality that is supported by the OS10 and the underlying hardware. The switch configuration is done through the CLI. For information about configuring a switch using the CLI, see the *OS10 Enterprise Edition User Guide.*

NOTE: While replacing IOMs in full switch mode, remove the IOM before removing the ISL cables to prevent possible split-brain situations.

You can use OME–Modular to perform the following tasks:

- Configure hostname, SNMP, and NTP settings.
- Configure port breakout modes.
- Set ports up or down.
- Monitor health, logs, alerts, and events.
- Update and manage firmware.
- View the physical topology.
- Perform power control operations.

It is recommended that you use the full switch mode when you require a feature or network architecture that is unavailable with SmartFabric Services.

For information about Fabric mode, see SmartFabric Services.

Managing Ethernet IOMs

The **I/O Modules** page displays the health and asset information of the IOMs. If you have the fabric manager role with device configuration and power control privileges, you can perform the following tasks on the **I/O Module** page:

- Power Cycle—Turn on, turn off, or perform a system reseat on the IOM
- Update firmware, if applicable
- Blink LED—Turn on or turn off the IOM Identification LED
- Refresh Inventory

You must have the device configuration privileges to set up network IOMs and perform configuration tasks on them.

NOTE: The perpetual license comes by default with the factory shipped IOMs. If you perform ONIE install on the IOM, the perpetual license is removed and replaced with the evaluation trail license. It is recommended to contact DELL support for the perpetual license installation after the ONIE install is complete.

NOTE: When a switch changes between Full Switch and Fabric modes, it reboots.

NOTE: If the compute sled and fabric IOM mismatch, the health status of the compute or IOM is displayed as "Warning" in the chassis subsystem health. However, the health status is not displayed in the chassis graphical representation on the **Chassis** page, I/O Modules, and **Compute** pages.

Topics:

Viewing hardware details

You can view information for the following IOM hardware:

- FRU
- Device Management Info
- Installed Software
- Port Information

NOTE: If the physical port is added as part of the port channel, it is listed under the port channel group instead of the physical port.

NOTE: The URL attribute is displayed as "N/A" on the **Hardware** > **Device Management Info** page for MXG610s IOMs, owing to device capability limitations.

NOTE: For Quad Port Ethernet adapters, the second uplink of the MX7116n has to be connected to the IOM. When the second uplink is connected, the number of ports in each virtual slot is increased from eight to sixteen ports.

Ensure that OME-Modular is updated to 1.20.10 before populating the Quad Port.

For **Port Information**, when you enable autonegotiation, peer devices exchange capabilities such as speed and settle on mutually acceptable configuration. However, when the autonegotiation is disabled, the peer devices may not exchange capabilities. Hence, Dell Technologies recommends that the configuration on both peer devices is identical.

The guidelines for autonegotiation process are as follows:

- MX9116n, MX7116n, and MX5108n IOMs support only 25G speeds on server facing ports.
- By default, autonegotiation is enabled on server facing 25G ports, as per the IEEE 802.3 Standard.
- Enabling or disabling autonegotiation is supported. However, configuring speed on server facing ports is not supported.
- When autonegotiation is enabled, Ethernet switches display speed capability of only 25G.

To view the hardware details:

Click **I/O Modules** > **View Details** > **Hardware**

Configuring IOM settings

If you have the IOM device configuration privilege, you can configure the following settings for the MX9116n FSE and MX5108n Ethernet Switch IOMs:

- Network
- Administrator password
- SNMP
- Time

You must have the network administrator privilege to configure the public management IP for the IOMs. The public IP facilitates use of the IOM Command Line Interface (CLI) to configure and troubleshoot the IOMs.

Configuring IOM network settings

The network settings for IOMs include configuring the public management IP for the selected management port.

To configure the networking settings:

1. Click **All Devices** > **I/O Modules** > **View Details** > **Settings** > **Network** or **Devices** > **I/O Modules** > **View Details** > **Settings** > **Network**.
2. In the **IPv4 Settings** section, select **Enable IPv4**.
3. Enter the **IP Address**, **Subnet Mask**, and **Gateway** for the management port.

   The **IP Address**, **Subnet Mask**, and **Gateway** options are enabled only if the **Enable DHCP** check box is cleared.

   For MXG610s FiberChannel Switch, if you configured the IPv6 address through DHCPV6 by selecting **IPv6 Settings** > **Enable Autoconfiguration**, the prefix length of 128 is assigned.

   NOTE: For MX5108n and MX9116n IOMs, the default prefix length of the DHCP IP is 128 bits, though the DHCP server is configured for 64 bits.

4. In the **IPv6 Settings** section, select **Enable IPv6**.
5. Enter the **IPv6 Address**, select the **Prefix Length**.

   The **IPv6 Address**, **Prefix Length**, and **Gateway** options are enabled only if the **Enable Autoconfiguration** check box is cleared.
6. Enter the **Gateway** for the management port.

   The **IPv6 Address**, **Prefix Length**, and **Gateway** options are enabled only if the **Enable Autoconfiguration** check box is cleared.

   NOTE: For tagged or untagged VLAN network, any IPv6 setting that is configured using OME-Modular may not have the default gateway. To get the default gateway, go to the respective OS10 CLI and disable the Stateless Address Autoconfiguration (SLAAC) on the respective tagged or untagged VLAN.
7. In the **DNS Server Settings** section, enter the **Preferred DNS Server**, **Alternate DNS Server 1**, and **Alternate DNS Server 2** addresses.

   For MXG610s IOMs, you can set the Preferred DNS and Alternate Server 1 and 2 addresses. However, the server address for **Alternate DNS Server 2** is not applied though the response is successful as, MXG610s IOMs support only two server addresses for DNS settings.
8. In the **Management VLAN** section, select **Enable VLAN** and enter the **VLAN ID**.

   For MXG610s IOMs, DHCP works only without VLAN while Static IP works with or without VLAN configuration. To change the IP configuration from DHCP IP to Static IP, perform the following steps:

   a. Disable DHCP, configure the static IP, and save the configuration.
   b. Enable VLAN, configure the VLAN ID, and save the configuration.

Configuring IOM management settings

The management settings for IOMs include configuring the hostname and password of the management system.

1. Click **All Devices** > **I/O Modules** > **View Details** > **Settings** > **Management** or **Devices** > **I/O Modules** > **View Details** > **Settings** > **Management**.
2. In the **Host Name** section, enter the name of the management system.
   If you modify the hostname settings in the OME-Modular web interface for Fibre Channel IOM, the modified hostname for Fibre Channel IOMs is displayed only in a new session. To see the modified hostname, log out and log in back to the session.
3. Enter the password to access the management system.

   NOTE: For Ethernet IOMs with OS10 version 10.5.0.7 and later and MXG610s, it sets the admin account password. For OS10 versions earlier than 10.5.0.7, it sets the linuxadmin account password.

   NOTE: The OS10 password length must be with minimum nine characters. It is recommended to have at least one upper case, one lower case, one numeric character, and one special character for stronger password. By default, the minimum number of different character settings are set as 0. You can use **password-attributes** command to configure wanted password strength.

   NOTE: The Ethernet IOMs with OS10 contain a Linux Admin User account for accessing the Linux shell. The username and default password for this account is **linuxadmin**. For instructions about changing the Linux Admin User account password, see the **Security** section of the *Dell SmartFabric OS10 User Guide*.

4. Click **Apply** to save the management settings or click **Discard** to clear the changes and go back to the previous settings.

Configuring IOM monitoring settings

The monitoring settings for IOMs include configuring the settings to monitor SNMP.

1. Click **All Devices** > **I/O Modules** > **View Details** > **Settings** > **Monitoring** or **Devices** > **I/O Modules** > **View Details** > **Settings** > **Monitoring**.
2. Select the **Enable SNMP** checkbox to enable of disable the SNMP.
3. From **SNMP Version**, select **SNMP v1** or **SNMP v2**.
4. Enter the **Read Community String** to fetch requests from the OME-Modular daemon directed at the IOM.
5. Click **Apply** to save the monitoring settings or click **Discard** to clear the changes and go back to the previous settings.

Configuring OS10 administrator password

The OS10 admin user account is the default administrator account that is used to configure OS10.

To configure the OS10 administrator account password:

1. Click **All Devices** > **I/O Modules** > **View Details** > **Settings** > **Management** or **Devices** > **I/O Modules** > **View Details** > **Settings** > **Management**.
   The **I/O Modules** page is displayed.
2. Enter the **Host Name** and **Root Password** for the IOM.

   NOTE: For OS10 versions 10.5.0.5 and earlier, the above procedure changed the password for the OS10 linuxadmin account. For OS10 versions later than 10.5.0.5, the above procedure changes the password for the OS10 admin user.

Configuring SNMP settings

To configure the SNMP settings:

1. Click **All Devices** > **I/O Modules** > **View Details** > **Settings** > **Monitoring** or **Devices** > **I/O Modules** > **View Details** > **Settings** > **Monitoring**.
2. Select **Enable SNMP** to configure the SNMP version and community string.

   NOTE: OME-Modular does not support disabling SNMP for OS10. You can only set the community string to blank. For MX9116n and MX5108n IOMs, only SNMP v2 is supported while for MXG610s, only SNMPv1 is supported. OME-Modular does not support SNMP v3 for IOMs.

Configuring advanced settings

To configure the advanced IOM settings:

1. Click **Application Settings** > **Network** > **IOM Synchronization Configuration**.
2. Select the options to replicate the chassis time and alert settings to the IOM. The settings are applied to all applicable IOMs in the chassis or chassis group.

Configuring ports

In SmartFabric mode, you can configure breakout and admin status, and MTU size for IOMs. You can configure port breakout only for port groups.

In Full Switch Mode, the **Port Information** page is read-only. Use the OS10 CLI to modify interface settings.

NOTE: Ensure that the peer FC port has a fixed speed and matches the speed of the IOM FC port for the link to come up.

NOTE: Interswitch link (ISL) port role is renamed as Interchassis link (ICL) port role from OME-M 1.40.00 onwards.

To configure breakout:

1. Click **Devices** > **I/O Modules** > **View Details** > **Hardware** > **Port Information**.
2. Select the port group and click **Configure Breakout**.
   The **Configure Breakout** window is displayed.
3. Select the **Breakout Type**.

Configuring admin status

You can switch the admin status for all ports, which is enabled by default. You can set the administrative status to enabled or disabled.

To switch the admin status:

Select the port and click **Toggle Admin State**.
The **Toggle Admin State** window is displayed.

Configuring Maximum Transmission Unit

You can configure the Maximum Transmission Unit (MTU) for full-switch and fabric mode IOMs.

SmartFabric Services do not support configuring MTU for the Fiber Channel Interfaces.

To configure MTU:

1. Click **Devices** > **I/O Modules** > **View Details** > **Hardware** > **Port Information**.
2. Select the Ethernet port and click **MTU**.
   The **Configure MTU** window is displayed.
3. Select the **MTU Size**.
   The default value for MTU is 9216 bytes.

Configuring auto negotiation

You can switch auto negotiation (AutoNeg) by performing **Toggle AutoNeg**.

The default configurations are:

- MX9116n/MX5108n—The auto negotiation is enabled for DAC cables and disabled for AOC and fiber optic transceivers.
- MX7116n Fabric Expander Module—The auto negotiation is enabled for DAC cables and disabled for AOC and fiber optic transceivers.
- Servers—(Smart auto negotiation)—The NIC cycles through the possible settings matches the configuration on the link partner.

For MX7116n, you cannot change the configuration. Hence, do not change the auto negotiation on the IOM manually, to avoid configuration mismatch. The smart auto negotiation is common for DAC and fibers. It is recommended not to set forced speed or enable the auto negotiation on the server for the different media that are supported. The following table describes the expected results when auto negotiation is enabled or disabled on the switch and servers.

Auto negotiation on servers	Auto negotiation on IOMs	Interface status	Expected results
Enable	Enable	Up	Auto negotiation is enabled on all three devices. Port is up. Expected.
Disable	Disable	Down	Auto negotiation is enabled on MX7116n Fabric Expander Module. Auto negotiation on IOM and server is disabled manually. Configuration mismatch. Port is down. Expected.

NOTE: Switch server ports have autoneg enabled by default in order to bring up the link with server NIC at 25 GbE. Disabling autoneg on the server port may force the server link to be operationally down.

To switch AutoNeg:

Select the port and click **Toggle AutoNeg**.
The **Toggle AutoNeg** window is displayed.

If Ethernet links are not displayed automatically, switch the auto negotiation setting.

Configuring Forward Error Correction

The Forward Error Correction (FEC) feature in OME-Modular helps mitigate errors in data transfers. FEC increases data reliability.

To configure FEC:

1. On the **Port Information** page, expand the physical port group, and select the Ethernet port .
2. Click Configure FEC.
   The **Configure Forward Error Correction** window is displayed.
3. Select the **FEC Type**.

   The available options are:
   - **Auto**—Applies FEC based on the cable or optic connected
   - **Off**—Disables FEC
   - **CL74-FC**— Configures CL74-RS FEC and supports 25G and 50G
   - **CL91-RS**—Configures CL91-RS FEC and supports 100G
   - **CL108-RS**—Configures CL108-RS FEC and supports 25G and 50G
4. Click Finish to save the changes and return to the **Port Information** page.

11

MX Scalable Fabric architecture

The scalable fabric architecture ties multiple MX7000 chassis into a single network domain to behave like a single logical chassis from a networking perspective. The MX scalable fabric architecture provides multichassis Ethernet with:

- Multiple 25 Gb Ethernet connections to each server sled
- No east-west oversubscription
- Low “any-any” latency
- Scale up to 10 MX7000 chassis
- Flexible uplink speeds
- Support for non-PowerEdge MX devices such as rack servers

For more information, see the *PowerEdge MX I/O Guide* available at www.dellemc.com.

Architectural Overview

A scalable fabric consists of two main components – a pair of MX9116n Fabric Switching Engines (FSE) and additional pairs of MX7116n Fabric Expander Modules (FEM) used to connect remote chassis to the FSEs. This is a hardware enabled architecture, and it applies irrespective of whether the switch is running in Full Switch or Fabric modes. A total of ten MX7000 chassis are supported in a scalable fabric.

Fabric Switching Engine

The FSE contains the switching ASIC and network operating system. Traffic that is received from a FEM is mapped to the correct switch interface automatically. Each NIC port has a dedicated 25 GbE lane from the NIC through the FEM and into the FSE so there is no port to port oversubscription.

Fabric Expander Module

An FEM takes Ethernet frames from a compute node and sends them to the FSE and from the FSE to the compute node. There is no switching ASIC or operating system running on the FEM, which allows for low latency. The FEM is invisible to the FSE and is not managed in any way.

When using dual-port NICs, only the first port on the FEM must be connected to the FSE. The second port is not used.

When connecting a FEM to an FSE, the general rules to remember are:

- FEM in Slot A1 connects to FSE in Slot A1 or Slot B1
- FEM in Slot A2 connects to FSE in Slot A2 or Slot B2
- FEM in Slot B1 connects to FSE in Slot A1 or Slot B1
- FEM in Slot B2 connects to FSE in Slot A2 or Slot B2

NOTE: For Quad Port NICs, you must connect two cables from the MX7116n FEM to the MX9116n FSE.

Topics:

Recommended physical topology

The recommended minimum design for a scalable fabric is two chassis with Fabric A populated with redundant IOMs. Ideally, the two chassis are located in separate racks on separate power circuits to provide the highest redundancy.

Additional chassis only have FEMs and the appear as the image below.

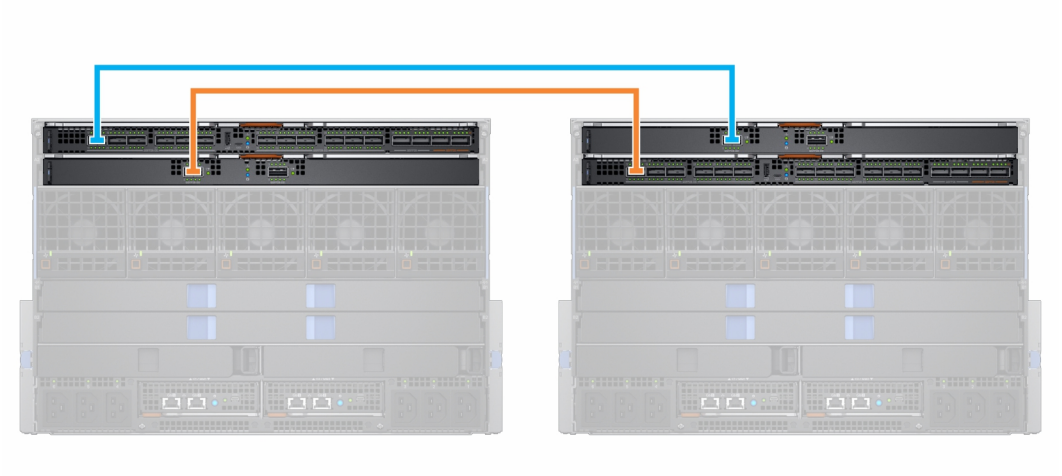


Table 20. Fabric topology

Chassis	Slot	Module
Chassis 1	A1	MX9116n FSE
	A2	MX7116n FEM
Chassis 2	A1	MX7116n FEM
	A2	MX9116n FSE
Chassis 3-10	A1	MX7116n FEM
	A2	MX7116n FEM

You can also use Fabric B to create a second scalable fabric:

NOTE: The OME-Modular firmware version 1.20.10 supports additional but complex topologies and also Quad Port Ethernet adapters. For more information, see the *PowerEdge MX Network Architecture Guide* available at https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

Restrictions and guidelines

The following restrictions and guidelines are applicable when building a scalable fabric:

- Mixing switch types in the same fabric is not supported. For example: MX9116n in slot A1 and MX5108n in slot A2
- Mixing switch types across fabrics is supported. For example: MX9116n in slots A1& A2 and MX5108n in slots B1 & B2
- All FSE and FEM IOMs in a scalable fabric must be in the same OME–Modular MCM group. FEMs in a chassis in MCM group 1 cannot be connected to FSEs in a chassis in MCM group 2.

The following restrictions are applicable when implementing a scalable fabric in both fabric slot A and fabric slot B:

- IOM placement for each scalable fabric must be the same within the same chassis. For example, if the FSE for the first scalable fabric is in Slot A1, then the second FSE must be in slot B1 in the same chassis, and so on.
- For chassis that only contain FEMs, all four FEMs must connect to the same chassis with the FSEs. The fabric B FEMs cannot be connected to FSEs in a different chassis as the fabric A FSEs.

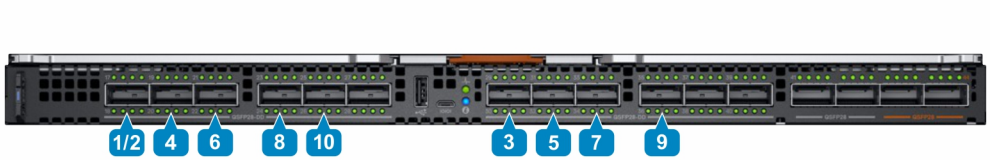
Recommended connection order

Any QSSFP28-DD port on the MX9116n can be used for any purpose. The table below describes the recommended port order for connecting chassis with Fabric Expander Modules (FEMs) to the FSE. The table contains references IOMs in fabric A, but the same guidelines apply to IOMs in fabric B.

Table 21. Recommended port order for connecting FEM to FSE

Chassis	FSE Port (Physical Port)
1 & 2	FSE Port 1 (17/18)
3	FSE Port 7 (29/30)
4	FSE Port 2 (19/20)
5	FSE Port 8 (31/32)
6	FSE Port 3 (21/22)
7	FSE Port 9 (33/34)
8	FSE Port 4 (23/24)
9*	FSE Port 10 (35/36)
10	FSE Port 5 (25/26)

*—By default, the port group 10 is not configured to support a FEM. If you want to connect a FEM to this port, use the OME - Modular interface to set the port mode to Fabric Expander.



NOTE: The port groups, 6, 11, and 12 (physical ports 27/28, 37/38, 39/40), can be used for additional uplinks, ISLs, rack servers, and so on.

12

SmartFabric Services

SmartFabric Services is a capability of Dell Networking OS10 Enterprise Edition running on Ethernet switches that are designed for the PowerEdge MX platform.

A SmartFabric is a logical entity containing a collection of physical resources such as servers and switches and logical resources —networks, templates, and uplinks. In the SmartFabric Services mode, the switches operate as a simple Layer 2 input output aggregation device, which enables complete interoperability with network equipment vendors.

A SmartFabric provides:

- Data center Modernization
  - I/O Aggregation
  - Plug-and-play fabric deployment
  - A single interface to manage all switches in the fabric like a single logical switch
- Lifecycle Management
  - Fabric-wide firmware upgrade scheduling
  - Automated or user enforced rollback to last well-known state
- Fabric Automation
  - Ensured compliance with selected physical topology
  - Policy-based Quality of Service (QoS) based on VLAN and Priority assignments
  - Automatic detection of fabric misconfigurations and link level failure conditions
  - Automated healing of the fabric on failure condition removal
- Failure Remediation
  - Dynamically adjusts bandwidth across all inter-switch links if a link fails

Unlike Full Switch mode, most fabric configuration settings are performed using the OME-Modular.

For information about automated QoS, see SmartFabric VLAN management and automated QoS

Changing operating modes

In both Full Switch and Fabric modes, all configuration changes you make using the OME–Modular interface are retained when you switch modes. It is recommended that you use the GUI for all switch configurations in Fabric mode and the OS10 CLI for configuring switches in Full Switch mode.

To switch an MX9116n Fabric Switching Engine or MX5108n Ethernet Switch between Full Switch and Fabric modes, use the OME–Modular GUI and create a fabric with that switch. When that switch is added to the fabric, it automatically changes to Fabric mode. When you change from Full Switch to Fabric mode, all Full Switch CLI configuration changes are deleted except for a subset of settings that are supported in Fabric mode.

To change a switch from Fabric to Full Switch mode, the fabric must be deleted. Then all Fabric GUI configuration settings are deleted. However, the configurations that are supported by the subset of Fabric CLI commands (hostname, SNMP settings, and so on) and the changes you make to port interfaces, MTU, speed, and auto-negotiation mode, are not deleted. The changes to port interfaces exclude the administrator state—shutdown/no shutdown.

During switch replacement of a fabric:

- If the fabric name and fabric description string contain the service tag of the old switch, the service tag is replaced with the service tag of the new switch during node replacement.
- If the switch being replaced has the VLT-MAC of the fabric, then VLT port-channel flaps are expected or unavoidable during switch replacement. This is because the VLT-MAC must be changed to one of the switches available in the fabric.

Topics:

- NIC teaming restrictions
- OS10 CLI commands available in SmartFabric mode
- Fabrics Overview
- Viewing topology details
- Viewing Multicast VLANs
- VLANs for SmartFabric and FCoE

Guidelines for operating in SmartFabric mode

The guidelines and restrictions while operating in SmartFabric mode are as follows:

- When operating with multiple chassis, ensure that the switches in A1/A2 or B1/B2 in one chassis are interconnected only with other A1/A2 or B1/B2 switches respectively. Connecting switches that are placed in slots A1/A2 in one chassis with switches in slots B1/B2 in another chassis is not supported.
- Uplinks must be symmetrical. If one switch in a SmartFabric has two uplinks, the other switch must have two uplinks of the same speed.
- Enable LACP on the uplink ports for switches being uplinked.
- You cannot have a pair of switches in SmartFabric mode uplink to another pair of switches in SmartFabric mode. You can only uplink a SmartFabric to a pair of switches in Full Switch mode.

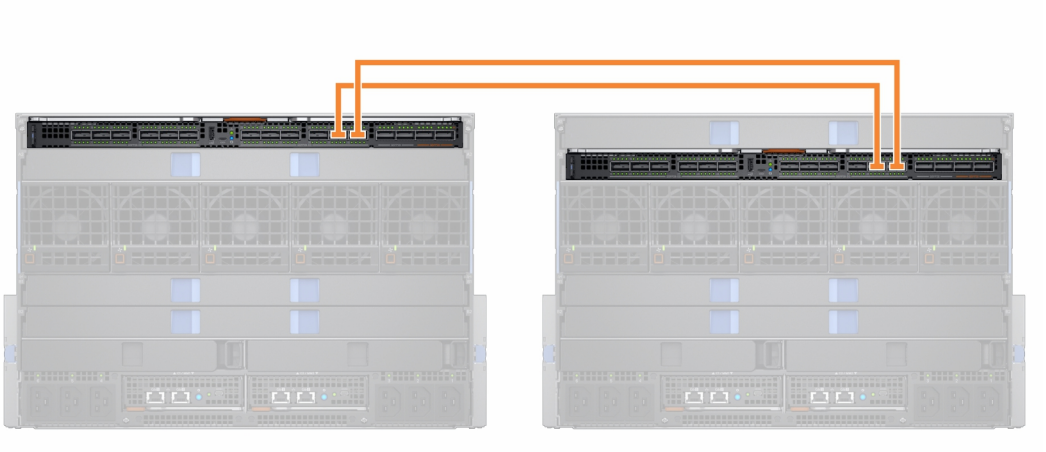
SmartFabric network topologies

The SmartFabric Services support three network topologies with specific IOM placement requirements.

- 2 x MX9116n Fabric Switching Engines in different chassis
- 2 x MX5108n Ethernet Switches in the same chassis
- 2 x MX9116n Fabric Switching Engines in the same chassis

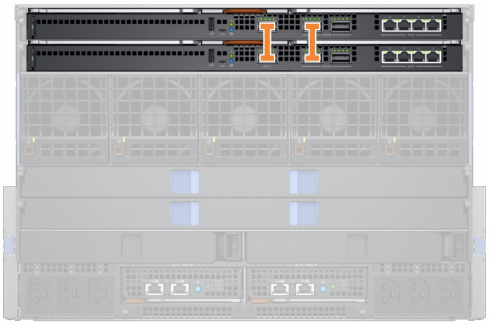
2 x MX9116n Fabric Switching Engines in separate chassis

This placement is recommended while creating a SmartFabric on top of a scalable fabric architecture. This configuration supports placement in Chassis1/A1 and Chassis 2/A2 or Chassis1/B1 and Chassis 2/B2. A SmartFabric cannot include a switch in Fab A and a switch in Fab B. If one of the chassis fails, placing the FSE modules in separate chassis provides redundancy. Both the chassis must be in the same MCM group.



2 x MX5108n Ethernet Switches in the same chassis

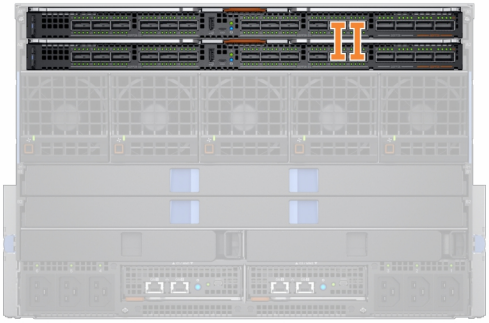
The MX5108n Ethernet Switch is supported only in single chassis configurations. The switches must be placed in slots A1/A2 or slots B1/B2. A SmartFabric cannot include a switch in Fab A and a switch in Fab B.



In SmartFabric mode, ports 9 and 10 are automatically configured in a VLT at 40GbE speed. For port 10, use a cable or optic that supports 40GbE and not 100GbE.

2 x MX9116n Fabric Switching Engines in the same chassis

Use this placement in environments with a single chassis. The switches must be placed in either slots A1/A2 or slots B1/B2. A SmartFabric cannot include a switch in Fab A and a switch in Fab B.

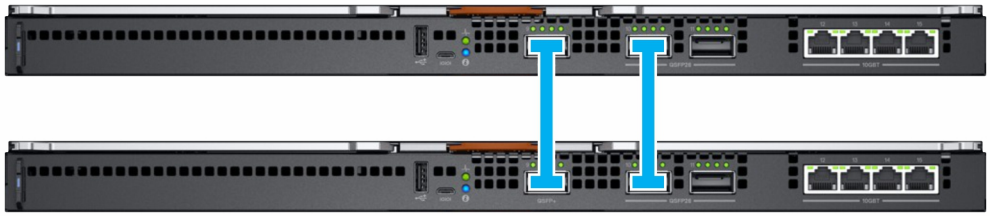


The fabric design, "2 x Mx9116n Fabric Switching Engines in the same chassis" is supported, but not recommended. Use of this design displays an error message on the **Fabric Topology** and **View Topology** pages of OME - Modular.

Switch to switch cabling

When operating in SmartFabric mode, each switch pair runs a Virtual Link Trunk (VLT) link between them. For the MX9116n, the port groups 11 and 12 are used.

For the MX5108n, ports 9 and 10 are used. Port 10 operates at 40GbE instead of 100GbE because all VLT links must run at the same speed. Ensure that you use a cable or optic fibre that supports 40GbE.



NOTE: You cannot select the ports, and the connection topology is enforced by SmartFabric Services.

NOTE: VLT is supported only on Ethernet and not on FCoE. Physically separate uplinks for LAN and FCoE traffic are required for MX5108n and MX9116n switches.

Upstream network switch requirements

It is recommended, but not required, that PowerEdge MX switches are connected to a pair of redundant upstream switches. When you are connecting a pair of switches in Fabric mode to an upstream switch pair, ensure that:

1. Both upstream switches must be connected to each other using technologies such as VLT or VPC.
2. The upstream switch ports must be in a port channel using LACP.

   NOTE: The LACP option is supported on Ethernet uplinks only.
3. A compatible Spanning Tree Protocol is configured. For more information, see the section, **Spanning Tree Protocol**.

Spanning Tree Protocol

OpenManage Modular v1.20.00 and OS10 versions later than 10.5.0.5 include a new Ethernet uplink type that does not require STP. The No STP Ethernet uplink is now the recommended uplink type for all SmartFabric installations. See the *Dell PowerEdge MX Networking Deployment Guide* for upstream switch configuration instructions.

The legacy Ethernet uplink type that does require STP is still supported. If you are creating a legacy Ethernet uplink, ensure that the correct STP type is selected.

OS10 defaults to RPVST+ as the Spanning Tree protocol. To change STP modes, use the spanning-tree mode command. Use the spanning-tree mode command to change STP modes. For steps, see the *OS10 Enterprise Edition User Guide*.

NOTE: During MX deployment, if the Spanning Tree is enabled, assign the Top of Rack (ToR) switch as root bridge to avoid traffic drop during convergence.

NOTE: If the upstream network is running RSTP, change from RPVST+ to RSTP before physically connecting the switches to the upstream network. Failure to do so may cause a network outage.

For more information about SmartFabric uplinks, see the *PowerEdge MX SmartFabric Configuration and Troubleshooting Guide*.

NIC teaming restrictions

NIC teaming is suggested for redundancy unless a particular implementation recommends against it. There are two main kinds of NIC teaming:

1. Switch Dependent—Also referred to as 802.3ad or Dynamic Link Aggregation. The switch-dependent teaming method uses the LACP protocol to understand the teaming topology. This teaming method provides Active-Active teaming and requires the switch to support LACP teaming.
2. Switch Independent—This method uses the operating system and NIC device drivers on the server to team the NICs. Each NIC vendor may provide slightly different implementations with different pros and cons.

NIC Partitioning (NPAR) can impact how NIC teaming operates. Based on restrictions that are implemented by NIC vendors that are related to NIC partitioning, certain configurations preclude certain types of teaming.

The following restrictions are applicable to both Full Switch and SmartFabric modes:

1. If NPAR is NOT in use, both Switch-Dependent (LACP) and Switch Independent teaming methods are supported.
2. If NPAR IS in use, only Switch Independent teaming methods are supported. Switch-Dependent teaming is NOT supported.

The following restrictions are applicable to Switch Dependent (LACP) teaming:

1. The IDRAC shared LOM feature can only be used if "Failover" option on IDRAC is enabled.
2. If the host operating system is Windows, the LACP timer MUST be set to "slow" (also referred to as "normal").

   For the list of supported operating systems, see Dell PowerEdge MX7000 Enclosure Installation and Service Manual.

NOTE: In a SmartFabric, if an LACP team is created with four ports and you want to delete two ports from the LACP team, you must delete the entire LACP team and create a new LACP team with two ports.

For detailed NIC teaming instructions, refer to the network adapter or operating system documentation.

OS10 CLI commands available in SmartFabric mode

When operating in SmartFabric mode, most of the switch configuration is managed through the OME-Modular GUI. Some OS10 functionality, such as Layer 3 routing, is disabled. A switch operating in Fabric mode supports all OS10 **show** commands, but only a subset of CLI configuration commands. For more information about supported CLI configuration commands, see the Dell SmartFabric OS10 User Guide.

Fabrics Overview

The MX7000 includes two general-purpose I/O fabrics, Fabric A and Fabric B. These fabrics are connected using a direct orthogonal connection between mezzanine cards. It is installed on the compute sleds in the front of the chassis and on I/O Fabric modules in the rear of the chassis. The absence of a midplane provides the end user a flexible option to choose their I/O fabric. It allows the adoption of new I/O technologies without upgrading the midplane which also reduces the failure points.

In the scaled VLAN environment, configuration update in the IOM console might be delayed even though the job status is **Completed** on the OME-Modular interface.

Viewing fabric details

To view details an existing fabric:

- From the **Devices** drop down, select **Fabric**.
- From the fabrics table, select the fabric and click **View Details**.

The **Fabric Details** page is displayed.

Editing fabric details

To edit the fabric details:

1. From the **Devices** drop down, select **Fabric**.
   The **Fabric** page is displayed.
2. From the fabrics table, select the fabric and click **Edit**.
   The **Edit Fabric** page is displayed.
3. Make the necessary changes to the **Name** and **Description** fields.

Replacing fabric switch

You can easily replace a faulty fabric switch in a SmartFabric. Click **Devices** > **Fabric** > **Replace Switch**.

To replace a fabric switch, perform the following steps:

- **Copy Current Configuration** —Copy the configurations from the switch to be replaced.
- **Replace Switch Hardware**—Remove the faulty switch from the chassis and replace it with the new switch.

- **Configure New Switch**—Apply the settings that were copied from the old switch to the new switch.
- **Update Fabric**—Enter the service tag of the old switch and the new replacement switch to complete the configuration of the SmartFabric.
- Click **Finish**.

Adding SmartFabric

To add a fabric:

1. Click **Devices** > **Fabric** .
   The **Fabric** page is displayed.
2. Click **Add Fabric**.
   The **Create Fabric** window is displayed.
3. Enter **Name** and **Description**, and then click **Next**.
4. Select the **Design Type** from the drop-down.
   The available options are:
   - 2xMX5108n Ethernet Switches in same chassis
   - 2xMX9116n Fabric Switching Engines in same chassis
   - 2xMX9116n Fabric Switching Engines in different chassis

   Based on the design type selected, the options to select the chassis and the switches—A and B, are displayed.
5. Select the chassis and switches.
   The cabling image is displayed.
6. Click **Next** to view the summary of the fabric.
   You can print to print a hard copy of the fabric details or save the details as a PDF on your system.
   After the fabric is created, the switch is placed in the SmartFabric mode and the IOM reboots.

   NOTE: After a fabric is created, the health status of the fabric is critical until uplinks are created.

   NOTE: The fabric health alerts are displayed on all chassis in the MCM group.

Adding uplinks

To add uplinks:

1. From the **Devices** drop-down, select **Fabric**.
   The **Fabric** page is displayed.
2. From the fabrics table, select the fabric and click **View Details**.
   The **Fabric Details** page is displayed.
3. From the **Uplinks** section, click **Add Uplink**.
   The **Add Uplink** window is displayed.
4. Enter **Name**, **Description**, select the **Uplink Type**.
   The available options are:
   - **Ethernet - No Spanning Tree**—This is the recommended uplink type. You can pick one or more Ethernet ports across IOMs to form a LAG to connect to the upstream network. This type of uplink will not have spanning tree enabled on it. This uplink type does not require Spanning Tree Protocol to be configured on the upstream Ethernet switch. For more information about how to configure the upstream Ethernet switch, see *Dell PowerEdge MX Networking Deployment Guide* at https://infohub.delltechnologies.com/. Before you can create an **Ethernet - No STP** uplink, all legacy Ethernet uplinks that use STP must be deleted. There are additional steps that must be completed before creating an **Ethernet - No STP** uplink on an existing fabric that was not running the RSTP protocol. For more information, see the *Dell PowerEdge MX Networking Deployment Guide* at https://infohub.delltechnologies.com/
   - **Ethernet**—This uplink type is no longer recommended. You can pick one or more Ethernet ports across switches to form a LAG. The network can be of any type. Also, you must configure **Spanning Tree** on the upstream network switch.
   - **FCoE**—You can pick one port from an IOM and associate a single network of FCoE type. This is for FCoE connectivity that connects to another switch that connects to the FC network. For single fabric, you can have two FCoE uplink, one from each IOM. Both IOMs must have different network that is, different FCoE VLANs.

     In FCoE mode, untagged VLAN on the server port and FCoE uplink must be the same. This condition ensures that the untagged FIP VLAN discovery (L2 frame) packets are switched to the untagged VLAN. The FCoE uplink is used to

identify FIP Snooping Bridge (FSB) mode at the switch. For the FCoE sessions to come up, configure the same untagged VLAN on FCoE uplinks and server ports.

NOTE: On the uplink FCoE switch, use the default fc-map (0efc00) only.

- **FC Gateway**—You can pick one or more ports from the same IOM and associate a single network of FCoE type. This type of uplink is for connectivity to a SAN switch. For single Fabric, you can have two FC gateway uplinks one from each IOM. Both IOMs must have different network that is, different FCoE VLANs. For a given fabric, you can have at least one uplink of type FC (either of FCoE, FCDirectAttach, FC Gateway).

  In Fabric mode, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN that has one or more FC Gateway uplinks. The FC Gateway uplink is used to identify NPG (N Port Proxy Gateway) mode at the switch.

- **FC Direct Attach**—You can pick one or more ports from same IOM and associate a single network of FCoE type. This type of uplink is for direct FC storage connectivity. For single fabric, user can have two FC DirectAttach uplink, one from each IOM. Both IOMs must have different networks that is, different FCoE VLANs.

  In Fabric mode, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN that has one or more FC Direct attach uplinks. The FC Direct attach uplink is used to identify F-Port mode at the switch.

5. Select **Include in Uplink Failure Detection Group** and click **Next**.

   Selecting the **Uplink Failure Detection(UFD)** detects loss of upstream connectivity and indicates this state to the servers connected to the switch. UFD associates downstream interfaces with the uplink interfaces. If the uplink fails, the switch operationally disables the corresponding downstream interfaces. This allows the downstream servers to select alternate paths for upstream connectivity available.
6. Choose the necessary **Switch Ports** and select any **Tagged Networks** .

   If you are required to configure new network other than the existing ones, click **Add Network** and enter the network details. For more details see, Adding Network.

Adding network

You can use the **Fabric** and **Configuration** > **VLANs** pages to add networks. For more information, see Defining networks.

To add new network from the **Fabric** page:

1. From the **Devices** drop-down, select **Fabric**.
   The **Fabric** page is displayed.
2. From the fabrics table, select the fabric, and click **View Details**.
   The **Fabric Details** page is displayed.
3. From the **Uplinks** section, click **Add Uplink**.
   The **Add Uplink** window is displayed.
4. Click **Add Network**.
   The **Define Network** window is displayed.
5. Enter **Name**, **Description**, **VLAN ID** and select the **Network Type**.

   For the network types, see the *Online Help*.

Editing uplink

To edit an existing uplink:

1. From the **Devices** drop-down, select **Fabric**.
   The **Fabric** page is displayed.
2. From the fabrics table, select the fabric and click **View Details**.
   The **Fabric Details** page is displayed.
3. From the **Uplinks** table, select the uplink and click **Edit**.
   The **Edit uplink** page is displayed.
4. Edit the **Name**, **Description**, and **Uplink Type** fields as necessary, and then click **Next**.
5. Select the necessary **Switch Ports** and select any **Tagged Networks** or **Untagged Networks**.

   To configure new network other than the existing ones, click **Add Network** and enter the network details. For more details see, Adding Network.

NOTE: You cannot edit the networks when uplinks are in FCoE, FC Gateway, or FC Direct Attach modes. Re-create the uplink to modify the networks.

Deleting uplinks

To delete an uplink:

1. From the **Devices** drop down, select **Fabric**.
   The **Fabric** page is displayed.
2. In the fabrics table, select any fabric and click **View Details**.
3. In the uplinks table, select the uplink to be deleted.
4. Click **Delete**. Click **Yes** to confirm the deletion.

Deleting fabric

To delete an existing fabric:

1. From the **Devices** drop-down, select **Fabric**.
   The **Fabric** page is displayed.
2. From the fabrics table, select the fabric that you want to delete.
3. Click **Delete**.
   A message is displayed prompting you to confirm the deletion.
4. Click **Yes** to proceed.

   After the fabric is deleted, the IOMs will reboot and start in Full Switch mode.

Viewing topology details

The fabric topology image displays only the operational status of the ports. If the operational status is "up", a check mark is displayed. To view the graphical representation of the validation errors in an MCM scenario, go to the **Group Topology** page on the OME–Modular web interface.

To view topology details:

- From the **Devices** drop-down, select **Fabric**.
- From the fabrics table, select the fabric and click **View Details**.
- From the **Fabric Details** page, click **Topology**.

The topology of the fabric is displayed.

Viewing Multicast VLANs

This page displays the list of configured VLANs on a Fabric and multicast versions of the IGMP and MLD protocols on the switch. You can also Define VLAN and add VLAN to L2 Multicast configuration.

To add VLANs to L2 Multicast:

- From the **Devices** drop-down, select **Fabric**.
- From the fabrics table, select the fabric and click **View Details**.
- From the **Fabric Details** page, click **Multicast VLANs** and then click **L2 Multicast**.
- From the **L2 Multicast** wizard, on the **IGMP** pane select available VLANs.
- Select Add Selected VLANs to MLD configuration if required. Click **Next**.
- From the **MLD** pane select available VLANs and click **Finish**.

The selected VLANs and its details are displayed.

VLANs for SmartFabric and FCoE

Create VLANs before creating the SmartFabric. The first VLAN that is created must be the default or native VLAN, typically VLAN 1. The default VLAN must be created for any untagged traffic to cross the fabric.

If you are implementing Fibre Channel configurations, you can also configure VLANs for FCoE. The storage arrays have two separate controllers that create two paths—SAN path A and SAN path B. These paths are connected to MX9116n FSE. For storage traffic to be redundant, two separate VLANs are created for that traffic.

The following table lists examples of VLAN attributes for FCoE traffic:

Table 22. VLAN attributes for FCoE

Name	Description	Network Type	VLAN ID	SAN
FC A1	FCOE A1	Storage - FCoE	30	A
FC A2	FCOE A2	Storage - FCoE	40	B

NOTE: For more information about SmartFabric and FibreChannel, see *Dell PowerEdge MX Networking Deployment Guide* available at https://infohub.delltechnologies.com/

Defining VLANs for FCoE

To define VLANs for FcoE, follow the steps below:

1. From the menu, click **Configuration** > **VLANs**.
2. In the **VLANs** pane, click **Define**.
   The **Define Network** window is displayed.
3. Enter a **Name** and **Description** for the VLAN.
   The description is optional.
4. Enter a **VLAN ID** and select the **Network Type**.
   For FCoE, the **Network Type** must be **Storage FCoE**.
5. Click **Finish**.

Editing VLANs

You can add or remove VLANs on the deployed servers in a SmartFabric.

To add or remove VLANs:

1. From the menu, click **Devices** > **Fabric**.
2. Select the fabric for which you want to add or remove the VLAN.
3. In the left pane, select **Servers** and select the required servers.
4. Click **Edit Networks**.
5. Select one of the following options:
   - **NIC teaming from LACP**
   - **No Teaming**
   - **Other**
6. Define the tagged and untagged VLANs to modify the VLAN selections as required.
7. Select VLANs on Tagged and Untagged Network for each Mezzanine card port.
8. Click **Save**.

VLAN scaling guidelines

The number of recommended VLANs differs between the modes as SmartFabric mode provides network automation capabilities that Full Switch mode does not.

The following table lists the maximum number of VLANs recommended per fabric, Uplink, and server port:

Table 23. Maximum number of VLANs recommended in SmartFabric mode

OS10 Version	Parameter	Value
10.5.4.1	Maximum VLANs per fabric	3000
	Maximum VLANs per uplink	3000
	Maximum VLANs per server port	1500
10.5.3.X	Maximum VLANs per fabric	3000
	Maximum VLANs per uplink	3000
	Maximum VLANs per server port	1024
10.5.2.4 and 10.5.2.6	Maximum VLANs per fabric	1536
	Maximum VLANs per uplink	1536
	Maximum VLANs per server port	512
10.5.1.6-10.5.1.7	Maximum VLANs per fabric	512
	Maximum VLANs per uplink	512
	Maximum VLANs per server port	256
10.5.0.1-10.5.0.7	Maximum VLANs per fabric	256
	Maximum VLANs per uplink	256
	Maximum VLANs per server port	64
10.4.0.R3S 10.4.0.R4S	Maximum VLANs per fabric	128
	Maximum VLANs per uplink	128
	Maximum VLANs per server port	32

NOTE: For instructions on enabling SmartFabric Services to support higher VLAN counts (more than 256 VLANs per fabric), see the *Dell PowerEdge MX Networking Deployment Guide* available at https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

Configuration guidelines for VLAN scale spanning tree

Table 24. Configuration guidelines for VLAN scale (STP flavor)

Scale	STP flavor
Number of VLANs configured in each IOM is less than 100	RPVST or RSTP can be configured.
Number of VLANs configured in each IOM is greater than 100	RSTP is the recommended configuration.

Table 25. Configuration guidelines for VLAN scale (VLAN configuration)

Scale	Scale-profile VLAN configuration
Number of port vlan (PV) combinations is less than 6144	Not required
Number of port vlan (PV) combinations is greater than 6144	Is mandatory

NOTE: For more information about scale-profile VLAN, see *Dell PowerEdge MX Networking Deployment Guide* available at https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

13

Managing networks

You can configure logical networks that represent your environment, for the tagged and untagged VLANs. These logical networks are used to provision the appropriate VLANs on the associated switch port for the physical server NIC port.

NOTE: VLANs are only assigned to servers connected to switches in SmartFabric mode. For servers connected to switches in Full Switch mode, the VLAN information is ignored.

In tagged networks, a port handles multiple VLANs. VLAN tagged networks help identify which packet belongs to the VLAN on the other side. A packet is tagged with a VLAN tag in the Ethernet frame. A VLAN ID is put in the header to identify the network to which it belongs.

In untagged networks, one port handles only one VLAN.

To view the list of networks, click **Configuration** > **VLANs**. The **VLANs** page with the list of networks is displayed. You can view the name, description, and VLAN ID of the networks.

A summary of the selected network is displayed on the right side.

You can perform the following tasks on the **Networks** page:

- Define networks
- Edit networks
- Delete networks
- Export networks

Topics:

SmartFabric VLAN management and automated QoS

Besides assigning VLANs to server profiles, SmartFabric Services automate QoS settings based on user input. When a VLAN is created and you select the related traffic type (such as iSCSI and vMotion), the SFS engine assigns the correct QoS setting to that VLAN. You can also select a “metal” such as gold and bronze to assign your own priority values to the traffic.

Table 26. Network traffic types - QoS settings

Network Traffic Type	Description	QoS Setting
General Purpose (Bronze)	Used for low-priority data traffic	2
General Purpose (Silver)	Used for standard/default priority data traffic	3
General Purpose (Gold)	Used for high–priority data traffic	4
General Purpose (Platinum)	Used for extremely high–priority data traffic	5
Cluster Interconnect	Used for cluster heartbeat VLANs	5
Hypervisor Management	Used for hypervisor management connections such as the ESXi management VLAN	5
Storage - iSCSI	Used for iSCSI VLANs	5

Table 26. Network traffic types - QoS settings (continued)

Network Traffic Type	Description	QoS Setting
Storage - FCoE	Used for FCoE VLANs	5
Storage - Data Replication	Used for VLANssupporting storage data replication such as for VMware VSAN	5
VM Migration	Used for VLANs supporting vMotion and similar technologies	5
VMWare FT Logging	Used for VLANs supporting VMware Fault Tolerance	5

Defining networks

To configure a logical network:

1. Click **Configuration** > **VLANs**.
   The **VLANs** page is displayed.
2. Click **Define**.
   The **Define Network** window is displayed.
3. Enter the name, description, VLAN ID.
   The format for a single VLAN ID is—123 while for an ID range, the format is—123-234.
4. Select the **Network Type**.
   For more details, see SmartFabric VLAN management and automated QoS. The available options are:
   - **General Purpose (Bronze)**
   - **General Purpose (Silver)**
   - **General Purpose (Gold)**
   - **General Purpose (Platinum)**
   - **Cluster Interconnect**
   - **Hypervisor Management**
   - **Storage - iSCSI**
   - **Storage - FCoE**
   - **Storage - Data Replication**
   - **Storage - NVMe/TCP**
   - **VM Migration**
   - **VMWare FT Logging**

   For more details, see SmartFabric VLAN management and automated QoS.

Editing VLANs

To edit a network:

1. On the **VLANs** page, select the network that you want to edit, and click **Edit**.
   The **Edit Network** window is displayed.
2. Make the required changes.
   While editing the network, ensure that only one VLAN is configured in both the ports.
   NOTE: In fabric mode, do not delete VLAN from OME–Modular, if the VLAN is associated with any uplink.

Exporting VLANs

To export the network configuration:

On the **VLANs** page, select the required network, click **Export**. Select **Export All as CSV** or **Export All as JSON**.

The network details are exported in a `.csv` or `.json` format as selected to a local drive on your system.

Importing VLANs

To import VLANs:

1. On the **VLANs** page, select the required network and click **Import**, and select **Import from File**.
   The **Import from File** window is displayed.
2. Click **Select a File** to browse and import the file from the destination. The supported file types are `.csv` and `.json`.
3. Click **Finish** to import the VLANs.

Deleting VLANs

To delete a VLAN:

On the **Networks** page, select the VLAN and click **Delete**.
If the network is associated with a fabric uplink, a warning message is displayed that deleting the network results in loss of connectivity.

14

Managing Fibre Channel IOMs

The MXG610s Fibre Channel (FC) switch is designed for mission critical applications accessing data on external storage. It is optimized for flash storage and virtualized server environments. The FC switch enables organizations to dynamically scale connectivity and bandwidth Ports-on-Demand (PoD). It enhances operations with consolidated management and simple server and storage connectivity.

OME–Modular makes the management of the MXG610s simple. The SSO feature in OME–Modular enhances security and convenience.

To view GUI of the MXG610s FC switch:

1. On the **Devices** > **I/O Modules** > page, click **IOM UI launch**.

   The MXG610s FC web tools interface is displayed.

15

Managing firmware

The firmware feature in OME–Modular helps you to update the firmware of all the components in the chassis. The components include compute sleds, ethernet IOMs, storage IOMs, and SAS IOMs. The firmware updates can be sources from the Dell website or a custom repository setup using Repository Manager.

You must have the chassis administrator role and the device update privilege for the chassis to update the firmware on the chassis. To update the firmware on the components, you must have the device-specific manager role and device update privilege to perform the updates.

The MX chassis bundle refers to the following update packages:

- Chassis manager DUP—This DUP contains the OME–Modular firmware.
- Storage sled DUP—This DUP contains updates for the Dell storage sleds in the chassis.
- Storage IOM DUP—This DUP contains updates for the chassis storage IOMs.

The DUPs for network IOMs and switches are licensed software and are available as individual DUPs. For external storage, the DUPs are bundled in the catalog. If the hard drives or storage enclosures are assigned to a compute sled, you can update them using iDRAC. However, you cannot update the assigned or unassigned hard drives through a chassis context. You can map the drives to a server to update them.

The compute sled bundle refers to the packages for the server components—BIOS, NIC, RAID, hard drives, and iDRAC.

The firmware update process involves specifying the catalog, retrieving the firmware inventory, checking compliance, and updating the firmware.

The available baselines are displayed on the **Configuration** > **Firmware Compliance** page. You can view a summary of the baseline compliance and a pie chart on the top of the page. You can also view the summary of the desired baseline on the right side of the **Firmware Compliance** page.

The baseline information that is displayed on the **Firmware Compliance** page is—compliance, name of the baseline, job status, catalog type, timestamp when the baseline was last used.

The compliance status of the baseline can be of the following types:

- Ok
- Critical
- Warning
- Downgrade
- Unknown

You can perform the following tasks on the **Firmware Compliance** page:

- Create baseline
- Edit baseline
- View report
- Delete baseline
- Manage catalogs
- Check compliance

Topics:

Managing catalogs

The catalog management feature in OME–Modular enables you to choose the list of DUPs to use with baselines to determine firmware compliance.

You can source catalogs from the following locations:

- Newest validated stacks of chassis firmware on Dell.com—Component and device firmware for the MX solution are rigorously tested together as an end-to-end validated solution stack or firmware baseline. The validated stack is the same as the latest solution baseline. For more information, see MX7000 solution baselines.

  NOTE: You must configure the HTTPS proxy as covered in Initial Configuration.
- Latest component firmware versions on Dell.com—The catalog is updated on the second and fourth Friday of each month with new firmware that may include versions of firmware for components that have been individually tested and released since the last validated solution stack of chassis firmware.
- Network path—The network share consists of NFS, CIFS, HTTP, or HTTPS.

  You can use the Repository Manager to create the customized catalog and store it on the network share. The directories multiple or previous catalogs can be kept available by using different Catalog file paths.

NOTE: When you create a catalog on a particular date and download it to the required location on your network or local drive, the download is successful. However, if you modify the catalog on the same day at different times and attempt downloading it, the modified catalog is not downloaded. If the repository type is NFS and the catalog file is not available on the specified NFS server, the system uses the catalog file that was last fetched.

To view the list of catalogs:

On the **Firmware Compliance** page, click **Catalog Management**.
The **Catalog Management** page is displayed.

Select a catalog to view the summary. The summary consists of the number of bundles in the catalog, date and time when the catalog was released, and name of the baselines associated with the catalog.

You can perform the following tasks on the **Catalog Management** page:

- Add catalogs
- Edit catalogs
- Check for catalog updates
- Delete catalogs

Viewing catalogs

You can view the following catalog information on the **Catalog Management** page.

- Catalog name
- Download status
- Repository type
- Repository location
- Catalog file
- Created date

1. On the menu bar, click **Configuration** > **Firmware** > **Catalog Management**.
   The **Catalog Management** page is displayed.
2. Select a catalog to view the summary on the right side.

   The summary comprises of the number of bundles in the catalog, release timestamp of the catalog, and the name of the associated bundles in the catalog.

Adding catalogs

To add catalogs:

1. On the **Catalog Management** page, click **Add**.
   The **Add Update Catalog** window is displayed.
2. Enter a name for the catalog and select the catalog source.

The available options are:

- **Validated firmware solution baseline on dell.com**—From the **Select version** dropdown, select the latest version or two other previous versions. You can create three validated stack catalogs. The versions of firmware in this catalog have been tested together as part of the latest OME - Modular firmware release.

  NOTE: When the **validated stacks** option is selected, the details will be available only after the data is persisted to the database.

  NOTE: If the proxy configuration is enabled, an error message appears and the list of validated stack options are not displayed. In this scenario, disable the proxy configuration and retry the update operation.
- **Latest component firmware versions on Dell.com**—This catalog is updated on the second and fourth Friday of every month with new firmware. It includes the versions of firmware for components that have been individually tested and released since the last validated solution stack of chassis firmware.
- **Network Path**—The folder where a catalog and optionally associated updates have been placed by unpacking the validated stack at **ftp.dell.com** or by using Dell Repository Manager.

3. Select the **Share Type** and enter the corresponding details for the share type.

   The available options are:
   - NFS
   - CIFS
   - HTTP
   - HTTPS

   NOTE: The **Share Type** option is available only if you select **Network Path**.

   NOTE: The HTTPS share feature with proxy does not work when authentication is enabled for both the proxy and HTTPS share.

4. Select the mode of updating the catalog.

   The available options are:
   - Manually
   - Automatically

   The default mode is manual.

5. Select the **Update Frequency**.
   - Daily
   - Weekly

   NOTE: The time can be in HH:MM format.

6. Select the **Backup Existing Catalog** checkbox to take back of the existing catalogs.

   NOTE: The **Backup Existing Catalog** is displayed only when you select the latest validated stack and select the mode of updating catalog as Automatic.

7. Click **Finish**.

Editing catalogs

You can only modify the catalog name, network share address, and catalog file path.

NOTE: This option is not available to validated stack catalogs created with older catalog versions.

To edit catalogs:

1. On the **Catalog Management** page, select the catalog that you want to edit and click **Edit**.
   The **Edit Firmware Catalog** window is displayed.
2. Make the required changes.

Checking for catalog updates

You can check for catalog updates on the **Catalog Management** page manually or automatically, and download them. If the check is scheduled on a weekly basis, and update is unavailable or the site is not reachable, OME-Modular cancels the scheduled check. Run the next check, manually. The manual check prevents unnecessary checks if the catalog is moved or deleted.

NOTE: This option is not available to validated stack catalogs created with older catalog versions.

To check for catalog updates:

1. On the **Firmware Compliance** page, click **Catalog Management**.
   The **Catalog Management** page, with the list of available catalogs, is displayed.
2. Select the catalog, which you want to check for updates and click **Check for update**.
   A message confirming the check is displayed.

Deleting catalogs

You can only delete catalogs that are not associated with a baseline. If you attempt deleting a catalog that is associated with a baseline, an error message is displayed.

To delete a catalog:

On the **Catalog Management** page, select the catalog that you want to delete and click **Delete**.

Creating baselines

To create a firmware baseline:

1. Click **Configuration** > **Firmware Compliance** > **Create Baseline** .
   The **Create Update Baseline** window is displayed.
2. Select the catalog type, enter a name and description for the baseline.
3. Click **Select only components with no reboot required** checkbox to select only components with no reboot required.
4. Click **Add**.
   The **Add Update Catalog** window is displayed.
5. Enter the required details and select the catalog source.
6. In the **Create Update Baseline** window, select the devices and groups for which you want to create the baseline.

   After the baseline is created, a message is displayed and a compliance check is performed on the baseline. The status of the job is displayed on the **Firmware** page.

   NOTE: If the baseline is created from the catalog, the information of the associated baseline is displayed.

Editing baselines

To edit a baseline:

1. On the **Firmware Compliance** page, select the baseline that you want to modify and click **Edit**.
   The **Edit Firmware Baseline** window is displayed.
2. Make the required changes.

Checking compliance

To check the compliance of a firmware baseline:

1. On the **Firmware Compliance** page, select the baseline and click **Check Compliance**.
   A summary of the compliance check is displayed on the right side of the **Firmware Compliance** page.
2. Click **View Report**.
   The **Compliance Report** page is displayed.

   You can see the details:

- Device Compliance
- Component Compliance
- Type
- Model
- Device Name Contains
- Component Contains
- Service Tag Contains
- Reboot Required
- Prerequisites
- Impact Assessment
- Current Version Contains
- Baseline Version Contains

NOTE: If the firmware DUP is not available in the catalog, an error message is displayed.

NOTE: Firmware downgrade for network IOMs is not supported from OME-M using DUP. For more information, see the *OpenManage Enterprise-Modular Edition for PowerEdge MX7000 Chassis User's Guide* or *OS10 Enterprise Edition User Guide*.

The compliance status can be of types:

- Unknown—The firmware version for the component or device is not available in the catalog.
- Critical—The firmware version on the device is older than the catalog firmware version and the status of the firmware update in the catalog is critical or urgent.
- Warning—The firmware version on the device is older than the catalog firmware version and the status of the firmware update in the catalog is critical.
- Downgrade—The firmware version on the device is later than the catalog firmware version.
- Ok—The firmware version on the device and the catalog firmware version are identical.

You can perform the following tasks on the **Compliance Report** page:

- **Make Compliant**— Updates the firmware for the selected device or component within a bundle.
- **Export** — Exports the compliance report in `.csv` format to the specified location.
- **Advanced Filters**—Sorts the device information.

When you update the firmware for SAS IOMs that are available as an individual component and a chassis component, using the compliance report method, the management module update fails. Select the SAS IOM from the chassis component or the SAS IOM listed individually in the compliance report.

3. Click **Prerequisites**to view the prerequisites and dependency requirements to perform firmware update
   - Prerequisites—displays the actions pending before performing the firmware update.
   - Dependency Requirements—displays the link to download the required DUP. Dependencies can be classified in to:
     - Intradependency—displays the sequential update order for the device or component according to the firmware update matrix.
     - Interdependency—displays a dependency between two distinct components or devices.

Updating firmware

Before updating the firmware on a chassis, compute, or storage sleds, ensure that all IOMs and network fabrics are healthy.

- Downgrading OME-M or MX7000 Network I/O components could result in loss of management configuration data and functionality.
- Selecting all components allows OME-Modular to properly sequence the component updates. When doing one or more individual components, see readme documents to ensure that all pre-requisites and sequencing requirements have been met to avoid failures.
- Selecting a component that is part of a high-availability group, updates all other components in the group even if they were not explicitly selected.
- When you select MX Network I/O module that is part of a fabric for ONIE update, all other nodes in the fabric are updated automatically.
- MX Storage I/O modules must be explicitly selected in order to be updated.
- When you select multiple network IOMs for firmware update, member IOMs are updated first and the main IOM is updated later.

- OS10 firmware cannot handle more than one update job at a time. When an update is in progress, any additional update requests are rejected and appropriate error messages are displayed.

NOTE: The **Update Firmware** button may be disabled temporarily during inventory refresh when a **Refresh Inventory** job or **Default Inventory** job is run.

NOTE: For downgrading iDRAC from version 5.10.xx.xx to versions earlier than 4.40.xx.xx, first downgrade to 4.40.xx and then to earlier versions. For example, if the current version of iDRAC firmware is 5.10.50.00 and you want to downgrade to 4.10.xx.xx, the downgrade must be in two phases. In the first phase, downgrade from 5.10.50.00 to 4.40.10.00. In the second phase, downgrade from 4.40.10.00 to 4.10.xx.xx or earlier.

To update firmware:

1. On the **Compliance Report** page, select the device or component for which you want to update the firmware. The **Update Firmware** window is displayed.
2. Select the **Update Now** option to update the firmware immediately or **Schedule Later** to update the firmware on the chosen date and time.

   NOTE: If the system displays the local clock on the **Time Configuration** page even after you configured the NTP servers, reconfigure the NTP servers.

   NOTE: During firmware update, when the active MM reboots and the standby MM is active, some messages on the **Execution Details** page for the firmware update are not displayed. The messages are not displayed owing to synchronization issues.

   NOTE: During the OME–Modular firmware update, multiple users can upload the OME–Modular DUP using any interface. However, a warning message may be displayed after the firmware update job is initiated.

   NOTE: For nondefault VLAN, the management IPv6 IP of MX9116n or MX5108n IOMs is unreachable, if the DHCP V6 configuration in ToR switch does not have the IPV6 default gateway.

   The number of IOMs that can be updated differs based on the IOM versions. The following table displays the number of IOMs that can be updated at a time.

Table 27. IOM Firmware update matrix

IOM Version	OME-M Version	No. of IOMs
10.5.0.5	1.10.20 or later	4
10.5.0.7	1.20.00 or later	6
10.5.1.6	1.20.10 or later	6
10.5.2.4	1.30.00 and later	No restrictions

You must group the IOMs for firmware update depending on the type of IOM. The following table displays an example of grouping 12 IOMs for firmware update.

Table 28. Grouping IOMs for firmware update

Example of 12 IOMs	Combination	Group 1	Group 2	Group 3
10.5.0.5	6 Fabrics	Fabric 1-2	Fabric 3-4	Fabric 5-6
	12 Full switch	IOM 1-4	IOM 5-8	IOM 9-12
	4 fabrics and 4 Full switch	Fabric 1-2	Fabric 3-4	4 Full switch IOM
10.5.0.7 or 10.5.1.6	6 Fabrics	Fabric 1-3	Fabric 4-6	Not Applicable
	12 Full switch	IOM 1-6	IOM 6-12	Not Applicable
	4 fabrics and 4 Full switch	Fabric 1-3	Fabric 4 and 4 full switch IOM	Not Applicable

Once all IOMs are updated to 10.5.2.4 stack, network IOMs display two software components for update. The available options are:

- Dell Networking SmartFabric OS10
- Dell Networking ONIE Firmware

Limitations for ONIE firmware update are:

- ONIE firmware update option is available only if the OS10 version is 10.5.2.4 or later.
- When you select the network IOM that is part of a fabric for ONIE update, other nodes in the fabric are updated automatically.
- If you insert an old version of IOM, the ONIE firmware cannot be updated before updating OS10 to 10.5.2.4 version.

NOTE: ONIE component firmware is not updated due to the issue of system not booting into ONIE, when GRUB menu is displayed with serial control character. This issue is addressed in 3.35.1.1-15 ONIE firmware version. If ONIE update fails or encounters ONIE booting issue, retry the ONIE component firmware update.

During firmware update in an MCM environment, the network might be disrupted for a few seconds as multiple chassis reboot. As a result, some jobs fail.

Update actions may fail when certain inventory actions are running on OME-Modular. Wait for a few minutes and retry the update to recover.

Rolling back firmware

If you are not convinced with the firmware update of a device or component, you can roll back the update to the version before the update. The rollback option is enabled only if OME–Modular can access the firmware package of the previous version. The following methods can be used to enable the access:

- A Device that has the rollback version (or N-1 version) that matches the previous version. Not all devices support a rollback or N-1 version. The rollback version is displayed as a rollback candidate even if it does not match the version before the update.
- An imported catalog that has a reference to the previous catalog version.
- You can browse for a firmware package that has the previous firmware version.

Rollback firmware update is not supported for network IOMs and chassis.

For downgrading iDRAC from version 5.10.xx.xx to versions earlier than 4.40.xx.xx, first downgrade to 4.40.xx and then to earlier versions. For example, if the current version of iDRAC firmware is 5.10.50.00 and you want to downgrade to 4.10.xx.xx, the downgrade must be in two phases. In the first phase, downgrade from 5.10.50.00 to 4.40.10.00. In the second phase, downgrade from 4.40.10.00 to 4.10.xx.xx or earlier.

To roll back a firmware update:

1. On the **Firmware** page, click **Rollback Firmware**.
   The **Rollback Firmware** window is displayed.
2. Select the component for which you want to roll back the firmware and click **Rollback**.

   NOTE: The device is always updated with individual DUP and is never updated or downgraded as part of catalog or baselines. But, when the device is associated with any baseline and an update is available as part of that catalog or baseline, the catalog option is given for the Rollback by default as it is a secure option.

Deleting firmware

You can delete firmware baselines, if you have the administrator privilege.

To delete a firmware baseline:

On the **Firmware** page, select the baseline that you want to delete, and click **Delete**.
A message is displayed prompting you to confirm the delete operation.

16

Monitoring alerts and logs

You can view and manage the alerts that are generated in the management system environment. You can filter alerts and perform the appropriate actions.

Every chassis in the MCM group receives Fabric alerts, irrespective of whether the MX5108N or MX9116N IOMs present in the chassis to accommodate new MX5108N or MX9116N IOMs in the chassis.

To view the alerts page, from the menu bar, click **Alerts**. The **Alerts** page with the following tabs is displayed:

- **Alert Log**
- **Alert Policies**
- **Alert Definition**

Topics:

Alert log

The **Alerts Log** page displays the list alert logs for events occurring in the chassis. On the menu bar, click **Alerts** > **Alert Log**. The **Alerts Log** page is displayed. You can view the alerts details—severity of the alert, timestamp, source, category, subcategory, message ID, and description of the alert.

The **Alerts Log** page displays 30,000 records. Select an alert to view the summary of the alert on the right side of the **Alerts Log** page. You can also perform the following tasks on the **Alerts Log** page:

- Acknowledge alerts
- Unacknowledge alerts
- Ignore alerts
- Export alerts
- Delete alerts

The latest unacknowledged alerts are displayed on the OME–Modular home page.

In MX9116N and MX5108N IOMs, when an uplink is removed and reinserted from the same port within 60 s, the latest alert message is not displayed on the **Alerts Log** page. This action is because the deduplication interval is set to 60 s to avoid recurrence of alerts.

Device name in alerts may take some time for update and hence, the device names set earlier are displayed.

If the network cable is disconnected and OME - Modular is not reachable, any alert that is generated during this time is dropped and does not reach the external alert destinations.

The alerts related to network IOM or Smart Fabric might get dropped during fabric manager onboarding task.

NOTE: If you use "&" in the Fabric and Device names, sending alerts to the email server is affected.

To ensure that events received from OME-Modular are resolved appropriately after OME-Modular firmware is updated to version 1.40.xx:

1. Download the latest SNMP v2 MIB file using OME-Modular Web interface or **https://www.dell.com/support.**
2. In the OpenManage Enterprise Web interface, go to **Monitor** > **MIBs** and upload the MIB file.

   Else, events from OME-Modular are categorized as "Miscellaneous" events in OpenManage Enterprise. For more details, see the Dell OpenManage Enterprise User's Guide.

Filtering alert logs

To filter alert logs:

1. On OME–Modular web interface, navigate to **Alerts** > **Alert Log**.
2. Click **Advanced Filters**.
3. Select or update the following based on your requirement:
   - **Severity**—To view all alerts with specific severity level.
   - **Acknowledge**—To view all alerts that were acknowledged.
   - **Start Date** and **End Date**—To view alerts from a specific period.
   - **Source Name**—To view the alerts from a specific system.
   - **Category** and **Subcategory**—To view alerts of specific category.
   - **Message**—To view alerts containing a specific word in the message column.

   Selections that are made in the filters are applied at real time.
4. To reset the filters, click **Clear All Filters**.

Acknowledging alert logs

You can acknowledge alert logs that are not already acknowledged. Acknowledging an alert prevents storing the same event in the system. For example, if a device is noisy and is generating the same event multiple times, you can ignore further recording of the alert by acknowledging the events that are received from the device. And, no events of the same type are recorded further.

To acknowledge alert logs:

On the **Alert Log** page, select the alert logs that you want to acknowledge and click **Acknowledge**.
A check mark is displayed in the **Acknowledge** column for the selected alert logs.

Unacknowledging alert logs

You can unacknowledge alert logs that are acknowledged. Unacknowledging an alert implies that all events from any device are recorded even when the same event recurs frequently. By default, all alerts are unacknowledged.

To unacknowledge alert logs:

On the **Alert Log** page, select the alert log that you want to unacknowledge and click **Unacknowledge**.
The check mark that is displayed in the **Acknowledge** column for the selected alert logs is cleared, indicating that the selected alert logs are unacknowledged.

Ignoring alert logs

You can ignore alert logs when you do not want to record an alert. No actions are initiated for any events occurring in the device with which the alert is associated. Alert policies for the selected device contain details of the events that must be ignored.

To ignore alert logs:

1. On the **Alert Log** page, select the alert logs that you want to ignore and click **Ignore** drop-down.
2. From the **Ignore** drop-down menu, select the required option. The possible options are:
   - Ignore on Selected Device(s) Only
   - Ignore All Alerts from Selected Device(s)
   - Ignore on All Devices

   A message is displayed indicating that an alert policy is created to ignore alert logs of the type you selected. The ignore policy is created from the device or multiple devices where the alert log is generated.

Exporting alert logs

You can export alert logs in `.csv` format to a network share or local drive on your system.

To export alert logs:

On the **Alert Log** page, select the alert logs that you want to export and click **Export** > **Export Selected**.

You can export all alert logs by clicking **Export** > **Export All**.

The alert logs are exported in `.csv` format.

Deleting alert logs

You can delete one or multiple alert logs.

To delete alert logs:

On the **Alert Log** page, select the alert logs that you want to delete and click **Delete**.
A message is displayed prompting to you confirm the action.

Alert policies

The alert policies feature enables you to view critical alerts and perform specific tasks. To view the list of alert policies, click **Alerts** > **Alert Policies**. The alert policy details include name and description of the alert policy, status of the alert policy, email ID of the administrator, and syslog.

NOTE: When there are multiple alert policies or destinations configured, there might be delay in receiving the alerts in SNMP destination.

You can perform the following tasks on the **Alert Policies** page:

- Create alert policies
- Edit alert policies
- Enable alert policies
- Disable alert policies
- Delete alert policies

OME–Modular also offers predefined alert policies for monitoring the systems, after the alert destinations are configured.

In MCM environment, if ignore alert policy is configured in the member chassis, the alerts in the member chassis are ignored and are not displayed in the member and lead chassis. However, the ignored alerts are forwarded to external destination owing to the alert forward policy in the lead chassis.

Creating alert policies

To receive Fabrics or Uplink related alerts from the source Fabric Manager, on the configured external destinations, select **Network IOM** or **All Devices** as **Groups** instead of **Devices** while configuring the alert policy.

NOTE: If you are configuring multiple alert policies, verify if the information like email address, destination address are correct. If there are any incorrect values, alerts for the policies may take longer time than expected to reach the external destination.

To create an alert policy:

1. From the menu bar, click **Alerts** > **Alert Policies** > **Create**.
   The **Create Alert Policy** wizard is displayed.
2. Enter the name and description for the alert policy.
3. Select **Enable Policy** to activate the alert policy and click **Next**.
   The **Category** tab is displayed.
4. Select all alert categories, or select the required option and click **Next**. The available categories are:
   - Application
   - Chassis
   - iDRAC
   - Network IOMs
   - Storage IOMs

   You can expand each category to view and select the subcategories.

   The **Message ID** tab is displayed.

5. Click **Select a file** to import a file with Message IDs or enter the message IDs separated by comma and click **Next**.

   NOTE: Selected message IDs can be ignored or forwarded to a destination. To ignore the message IDs, go to **Actions** and select **Ignore** checkbox.

   The **Devices** tab is displayed.
6. Select the required devices or groups and click **Next**.

   The available options are:
   - Select Devices
   - Select Groups
   - All Targets (Discovered and Undiscovered)

   The **Date and Time** tab is displayed.
7. Select the date, time, and days on which the alerts must be generated and click **Next**.
   The **Severity** tab is displayed.
8. Select the severity level and click **Next**.

   The available options are:
   - All
   - Unknown
   - Info
   - Normal
   - Warning
   - Critical

   The **Actions** tab is displayed.
9. Select the alert action and click **Next**. The available options are:
   - **Email (Enable)**—Click **Enable** to view the **Email Configuration** window where you can configure the email settings for the alert.
   - **SNMP Trap Forwarding (Enable)**—Click **Enable** to view the **SNMP Configuration** window where you can configure the SNMP settings for the alert.
   - **Syslog (Enable)**—Click **Enable** to view the **Syslog Configuration** window where you can configure the system log settings for the alert.
   - **Ignore**

   You can view the alert policy attributes in the **Summary** tab.

Enabling alert policies

You can enable alert policies that are disabled. You can enable more than one alert policy at a time.

To enable alert policies:

On the **Alert Policies** page, select the alerts that you want to enable and click **Enable**.
A confirmation message is displayed.

Editing alert policies

You can edit alert policies.

To edit alert policies:

On the **Alert Policies** page, select the alerts that you want to edit and click **Edit**.
A confirmation message is displayed.

Disabling alert policies

You can disable alert policies that are enabled. You can disable more than one alert policy at a time.

To disable alert policies:

On the **Alert Policies** page, select the alerts that you want to disable and click **Disable**.
A confirmation message is displayed.

Deleting alert policies

You can delete alert policies that are enabled. You can delete more than one alert policy at a time.

To delete alert policies:

1. On the **Alert Policies** page, select the alerts that you want to delete and click **Delete**.
   A message is displayed prompting you to confirm the action.
2. Click **Yes** to proceed.

Alert definitions

You can view description of the alert logs generated for events that associated with the chassis, and devices and components in the chassis, on the **Alerts Definition** page. The alert information that is displayed is as follows:

- Severity of the alert
- Message ID of the alert
- Alert message
- Category of the alert
- Subcategory of the alert

You can sort the list of alerts based on the **Advanced Filters**:

- **Message ID Contains**
- **Message Contains**
- **Category**
- **Subcategory**
- **Severity**

You can also select an alert to view the details on the right side of the **Alerts Definition** page. The details are—detailed description, recommended action, event source information, and criticality.

Filtering alert definitions

To filter alert definitions:

1. On OME–Modular web interface, navigate to **Alerts** > **Alert Definitions**.
2. Click **Advanced Filters**.
3. Select or update the following based on your requirement:
   - **Message Contains**—To view alerts containing a specific word in the message column.
   - **Message**—To view alerts containing a specific numeric or alphanumeric character.
   - **Category** and **Subcategory**—To view alerts of specific category.
   - **Severity**—To view all alerts with specific severity level.

   Selections that are made in the filters are applied at real time.
4. To reset the filters, click **Clear All Filters**.

17

Monitoring audit logs

The audit log feature in OME–Modular enables you to monitor log entries related to:

- Log in attempts
- Appliance setup
- Chassis configuration change using RESTful API
- Change in alert filter configuration

On the **Audit Log** page, you can perform the following tasks:

- Sort the audit logs using the Advanced Filter.
- Export all the audit logs in `.csv` format to a network share or local drive on your system.

NOTE: The audit logs for KVM and MM serial connection are not displayed after you log off from the session.

Quick Deploy audit logs are recorded as an overall operation, whenever they are created or updated. The quick deploy audit log details are similar to details of any other job that is created or updated in the system.

To view the **Audit Log** page:

From the menu bar, click **Monitor** > **Audit Logs**.
The **Audit Log** page is displayed.

Topics:

Filtering audit logs

To filter audit logs:

1. On the **Audit Logs** page, expand **Advanced Filters**.
2. Select or update the following based on your requirement:
   - **Severity**—To view audit logs of **Info**, **Warning**, **Critical**, or **All** severity levels.
   - **Start Time** and **End Time**—To view audit logs of a specific period.
   - **User**—To view audit logs from a specific user.
   - **Source Address**—To view audit logs from a specific system.
   - **Category**—To view audit logs of audit or configuration type.
   - **Description**—To view audit logs containing a specific word in the **Description** column.
   - **Message ID**—To view audit log containing a specific number or character

   Selections made in the filters are applied at real time. To reset the filers click **Clear All Filters**.

Exporting audit logs

You can export selected or all audit logs in a `.csv` format to a local drive on your system or a network share.

To export audit logs:

1. On the **Audit Logs** page, select the audit logs that you want to export.
2. Click **Export**, and select **Export Selected**.
   Else, you can click **Export** > **Export All**, to export all the audit logs.

Monitoring jobs

You can view the status of and details of jobs that are initiated in the chassis and its subcomponents, on the **Jobs** page. The jobs include firmware update and inventory refresh for devices.

To view the **Jobs** page, from the menu bar, click **Monitor** > **Jobs**.

You can perform the following tasks on the **Jobs** page:

- Filter jobs using **Advanced Filter**
- View a summary of the job
- Run jobs
- Stop jobs
- Enable jobs
- Disable jobs
- Delete jobs

The job status is "Completed with errors", when one or more sub-tasks fail the request and the status is set to "Warning". If all the sub tasks fail, status is "Failed". If all the tasks are completed successful, the status is displayed as "Completed".

A Quick Deployment job takes precedence over a slot-based profile deployment job. Conflicting settings, if any, revert to the Quick Deployment setting.

Sometimes, the offboarding task may not start until the refresh inventory job is completed.

NOTE: When the "Lockdown mode" is enabled on iDRAC, the **Blink LED** job status for iDRAC is displayed as "failed" on the OME–Modular **Jobs** page, even though the job is successful in iDRAC.

Filtering jobs

To filter jobs:

1. On the **Jobs** page, click **Advanced Filter**.
2. Select or update the following based on your requirement:
   - **Status**—To view jobs based on status. The available options are:
     - All
     - Scheduled
     - Queued
     - Starting
     - Running
     - Completed
     - Failed
     - New
     - Completed with errors
     - Aborted
     - Paused
     - Stopped
     - Canceled
     - Not Run
   - **State**—To view jobs based on state. The available options are:
     - All
     - Enabled
     - Disabled
   - **Job Type**—To view jobs based on the type. The available options are:
     - All
     - Appliance Backup
     - Appliance Restore
     - Chassis Profile
     - Backup
     - Backup Upload
     - Chassis Profile

- Data Synchronization
- Debug Logs
- Device Action
- Device Config
- Extract Logs
- Fabric Management
- Import VLAN Definitions
- Inventory
- MCM Assign Backup Lead
- MCM Group
- MCM OffBoarding
- MCM OnBoarding
- MCM Promote Backup Lead
- MCM Reassign Backup Lead
- MCM Retire Lead
- MCM Security Sync
- MCM Settings Propagation
- MCM Unassign Backup Lead
- OpenID Connect Provider
- Quick Deploy
- Restore
- Right Control Panel
- Settings Update
- Software Rollback
- Time Settings
- Update

NOTE: The option, Data Synchronization, is meant for troubleshooting and available only in the RESTful API interface. You can use this option with the help of technical support.

NOTE: When the inventory job starts, it tries to get the inventory details from the device. The maximum time configured for this job is two hours and the job fails if it exceeds the configured time. The inventory job fails before the maximum time only if there are other major issues like connectivity issue to device or oath failure.

- **Last Run Start Date** and **Last Run End Date**—To view jobs based on the last run period.
- **Source**—To view jobs based on the source. The available options are:
  - All
  - User generated
  - System generated

    NOTE: Refresh Inventory job is generated automatically on the lead chassis when you remove any device from the member chassis. In this scenario, the refresh inventory job fails in the lead chassis as the device is already removed and has no impact.

Selections that are made in the filters are applied at real time. To reset the filers click **Clear All Filters**.

MCM Security Settings Sync task is created only in the following scenarios:

- When a new member chassis is added to the lead chassis with OIDC provider. The OIDC settings are propagated from the lead chassis to the new member chassis.
- When the chassis is promoted as lead during the **Retire Chassis** or **Promote as Lead** workflow.

NOTE: MCM Security Settings Sync task is not created as part of OIDC provider setting propagation from Lead to member chassis.

Viewing job details

The Fabric Manager on-boarding is initiated when a Fabric Manager failover occurs in the IOM cluster. When a new Fabric Manager is discovered, OME-Modular initiates the on-boarding process to reestablish communication with the IOM cluster. In certain scenarios, multiple switchovers may occur within a short timespan resulting in failure of the tasks that are already in-progress. Only the last task is completed successfully. Following are the scenarios when multiple switchovers could occur:

- MM reset
- MM upgrade or switchover
- Inter-chassis link online insertion removal
- MM online insertion removal
- IOM main upgrade
- IOM main reset
- Fab-D congestions—Reasons for the congestion include downloading huge files that cause the FAB-D to drop other traffic

The details of the assigned MAC addresses for the respective NIC partitions are displayed on the **Jobs Details** page, that are based on the configuration results from iDRAC.

To view the details of a job:

1. On the **Jobs** page, select the job of which you want to view the details.
   A summary of the job is displayed on the right side of the **Jobs** page.
2. Click **View Details**.
   The **Job Details** page is displayed.

   The details including name, description, execution details, and the details of the system on which the job was run, are displayed.

   On **Job Details** page, you can perform the following tasks:

   - **Restart** the job
   - **Export** details of the job in a `.csv` format to a local drive on your system or a network share

   NOTE: The **Restart** option for the MCM onboarding task for adding a member chassis is disabled irrespective of the job status.

   Sometimes after a firmware update, `racreset` or management module failover, a message stating that the alerts could not be retrieved is displayed. The message that is displayed does not impact the functionality of OME–Modular.

Exporting job execution details

You can export the details of the job execution in a `.txt` format to a local drive on your system.

To export the job details:

On the **Job Details** page, click **Export** under the **Execution Details** tab.
The execution details are downloaded to a local drive on your system, in `.txt` format.

The job execution details are—start and end dates of the job, status, elapsed time, target system where the job is run, and message of the job.

NOTE: Always download the report in .txt format. The time format in the report displays GMT 24-hour format while the UI displays 12-hour format.

Running jobs

If a job is running from over 24 hours, stop the job after analyzing the job details. Rerun the job, if required.

You can use the **Jobs** page to run jobs immediately.

To run jobs:

On the **Jobs** page, select the jobs that you want to run and click **Run Now**.
A message is displayed to confirm that the task has restarted.

Stopping jobs

You can stop jobs that are in progress.

To stop jobs:

On the **Jobs** page, select the ongoing jobs that you want to stop and click **Stop**.
A message is displayed prompting you to confirm the operation.

Enabling jobs

You can enable jobs that are disabled.

To enable jobs:

On the **Jobs** page, select the disabled jobs that you want to enable and click **Enable**.
A confirmation message is displayed and the state of the selected jobs changes to "Enabled".

Disabling jobs

You can disable jobs that are enabled.

To disable jobs:

On the **Jobs** page, select the enabled jobs that you want to disable and click **Disable**.
A confirmation message is displayed and the state of the selected jobs changes to "Disabled".

Deleting jobs

To delete jobs:

On the **Jobs** page, select the jobs that you want to delete and click **Delete**.
A message is displayed prompting you to confirm the operation.

18

Use case scenarios

Use case scenarios for the backup lead chassis feature are described in this chapter.

Topics:

Assigning backup to the MCM Lead

The backup lead chassis feature facilitates management of systems in the chassis group when the existing lead chassis fails. Managing a chassis group consists of the following tasks:

- Assign—Allows assigning a member of the chassis group as a backup to the existing lead chassis.
- Unassign—Allows selection of another chassis in the group to replace the existing backup chassis.
- Promote—Allows the backup chassis to takeover as the lead chassis when the existing lead chassis fails.
- Retire—Allows the backup to takeover as the lead chassis when the existing lead chassis must be retired.

For more information, see Chassis groups.

Lifecycle of backup

The life cycle of the backup feature consists of the following stages:

1. Stage 1—Creating a chassis group with backup lead.
2. Stage 2—Monitoring the health of the lead and backup.
3. Stage 3—Replacing the primary lead chassis with backup lead or retiring the lead chassis.

Creating chassis group with backup lead

To create a chassis group and assign a backup to the lead chassis, perform the following steps:

1. Rack and stack the chassis.
2. Wire multiple chassis in the rack. For more information, see Wiring chassis and Pre-requisites for creating a distributed group.
3. Create a chassis group and add members to the group. For more information, see Chassis groups.

   Configuring a virtual IP is optional. The virtual IP enables a secondary IP on the lead that sticks with the lead. If the backup takes over as the new lead, then the secondary IP automatically moves to the new lead.
4. Configure the group from the lead chassis.

   If there are any settings and configurations on the member chassis that could conflict with lead, clear those configurations before the lead pushes its configuration across the group. Do the following, if required:
   a. Configure chassis settings.
   b. Update firmware.
   c. Configure firmware baselines.
   d. Configure alert policies.
   e. Configure templates and identity pools, and deploy to devices or slots.
   f. Configure other settings.
5. Assign one of the members of the chassis group as the backup lead.

   The initial configuration data synchronization from the lead chassis to backup chassis continues even after the assign job is completed. Both the lead and backup chassis report the health of the backup chassis.

Initially, the backup health status is displayed as "Critical" while the configuration data is being synchronized before changing to "OK". Wait for the backup health to transition to "OK" before proceeding. If the backup health continues to report "Critical" or "Warning" even after 30 minutes of the assign task, it is an indication that there are persistent communication issues. Unassign the backup and repeat the Step 5 to choose another member as the new backup. Also, Dell recommends that you create an alert policy on lead to take notification actions through email, SNMP trap, system log, for backup health alerts. Backup health alerts are part of the chassis configuration and system health category.

6. Configure the member chassis that is designated as the backup.

   It is mandatory for the backup chassis to have its own management network IP. The IP enables the backup to forward backup health alerts.

   Create an alert policy on the backup to take notification actions (email, SNMP trap, system log) for backup health alerts. Backup health alerts are part of Chassis (Configuration, System Health) category. The backup chassis raises warning or critical alerts when it detects that the backup synchronization status is bad because of communication or other irrecoverable errors.

Monitoring the MCM group

1. Complete all the configuration tasks before assigning the backup lead. However, if you have to modify the configuration after assigning the backup, the changes are automatically copied to the backup. The process of copying the changes to the backup may take up to 90 minutes, based on the configuration change.
2. The backup synchronization status of the lead and backup lead chassis is available at the following GUI locations:
   a. On the lead chassis:
      - **Home** page—**Backup Sync** status under the member (backup)
      - Lead **Overview** page—Redundancy and backup synchronization status under **Group Information**
   b. On the backup chassis:
      - **Home** > **Overview** page—**Backup Sync** status under the **Group Information**.
3. Interpreting the backup health:
   - If backup sync is healthy, the status is displayed as "Ok" and no further actions are needed.
   - If backup sync is not healthy, the status is displayed as "Warning" or "Critical". The "Warning" indicates a momentary synchronization problem that is resolved automatically. The "Critical" status indicates a permanent problem and requires user action.
   - When the backup sync status changes to "Warning" or "Critical", the associated alerts are generated under alert categories Chassis (Configuration, System Health). These alerts are logged to the **Home** > **Hardware Logs** and **Alerts** > **Alert Log**. The alerts are also shown as faults under the **Home** > **Chassis Subsystems** (top right-hand corner) under the MM subsystem. If an alert policy is configured, the actions are taken as configured in the policy.
4. Required user actions when Backup health is "Warning" or "Critical":
   - Warning—A momentary status and must transition to "Ok" or "Critical". But if the status continues to report "Warning" for more than 90 minutes, Dell recommends that you assign a new backup.
   - Critical—A permanent status indicative of issues with the backup or lead. Identify the underlying issues and take appropriate actions as described below:
     - Health is critical because of alert CDEV4006: The lead or member chassis has drifted its firmware version causing a lead/backup incompatibility. It is recommended that the firmware of the lead or member chassis is brought back to the same version (1.10.00 or later).
     - Health is critical because of alert CDEV4007: one of the several underlying issues contributes to this status, see the following flow chart to determine the cause and take the recommended action.

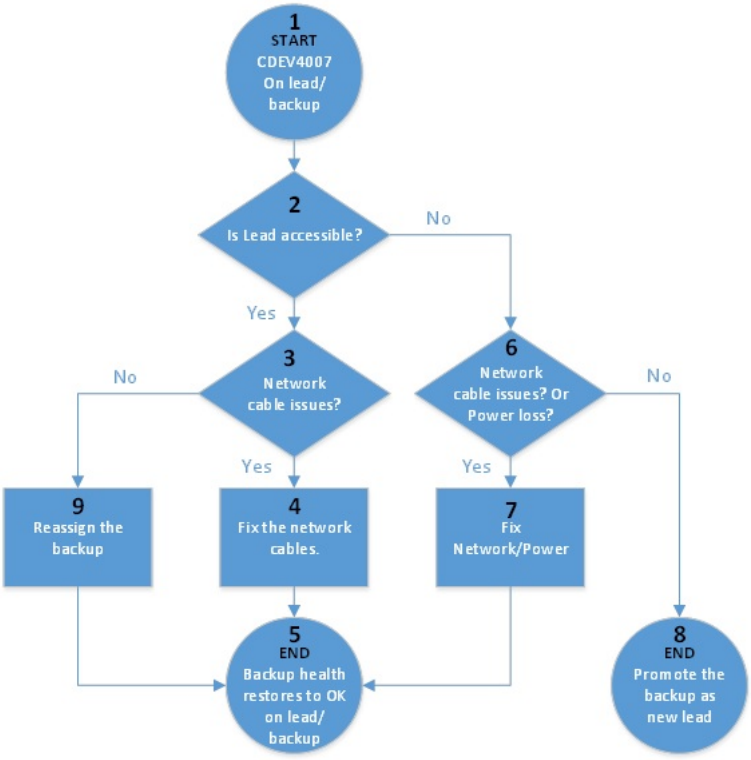


Figure 2. Network and power outage—flowchart

The alert, CDEV4007, is related to network or power issues that can be classified as:

- **Intermittent/recoverable issues—**Momentary power or network outages. The administrator can identify these types of failures and perform recovery actions locally or remotely. Do not promote the backup lead. Allow the lead chassis to recover connectivity automatically or the administrator fixes the power or network issues.
- **Partial failure—**Both management modules fail or malfunction. But the remaining chassis components are working. Promote the backup lead as the lead chassis to regain group management function through the new lead. For more information about promoting the backup and restoring the failed lead chassis to production state, see the section, Disaster recovery of lead chassis.
- **Complete failure—**Catastrophic failures. All the chassis components including the management modules are broken or nonresponsive. Promote the backup lead as the lead chassis to regain group management function through the new lead. For information about promoting the backup lead and clearing references to the failed lead chassis, see the section, Disaster recovery of lead chassis.

Scenarios when backup lead can take over as lead chassis

This section describes the situations in which a backup lead can take over as the lead chassis of the chassis group.

Disaster recovery of lead chassis

Catastrophic failures such as power loss, network loss, and failure of both MMs can result in the lead chassis being inaccessible or unavailable. In such cases, you can promote the backup to take over from the failed lead chassis for continued management of systems.

NOTE: Promoting the backup lead as the new lead restores the group management function for the member chassis that are not exposed to the failures. However, there are limitations on the extent of the functionality can be restored on the failed lead chassis. The restoration is based on the severity of the failures in the failed lead chassis.

Remember the following while recovering the lead chassis:

1. Before running the "promote" task on the backup lead chassis:
   a. The "promote" task is a disruptive operation and must be used only when there are no means to recover the inaccessible lead chassis. In partial failures of the lead chassis, for example; if only the management modules are nonresponsive, but the computes are working, running the promote task disrupts workloads that are still running on the lead chassis computes. For information about relocating working components that is, computes and network switches from the failed lead, see, the list item 3.c, "Steps that are required to restore the failed lead before putting it into production."
   b. After determining that the lead chassis has failed and is inaccessible, you must remotely shut down power to the lead chassis or physically remove the chassis from the stack before running the "promote" task on the backup. If lead chassis not turned off or removed from the stack before the promote task, the failed or partially failed lead chassis may revive after promoting the backup and cause situations of multiple leads. Multiple leads can create confusion and interference in managing the group.
2. Running the "promote" task on the backup lead chassis:
   a. If the lead chassis is up and running, the backup chassis web interface blocks the "promote" task. Ensure that the lead has failed and is inaccessible before initiating the promote task on backup. The backup may erroneously block the "promote" when the lead is accessible through the private network, but it may not be reachable on the public user management network. In such cases, OME-Modular RESTful API can be used to run the promote task forcefully. For more information, see the RESTful API guide.
   b. A job is created after the "promote" operation is started. The job may be completed in 10-45 minutes, depending on the number of chassis in the group and the size of configuration that are restored.
   c. If the lead chassis is configured to forward alerts to external destinations (email, trap, system log), any alerts that components in the group generate while the lead is down, are available only locally in their respective hardware or alert logs. During the lead outage, the leads cannot be forwarded to configured external destinations. The outage is the period between lead failure and successful promotion of backup.
3. Expected behavior after the "promote" task:
   a. The backup chassis becomes the lead and all the member chassis are accessible as they were on the earlier lead chassis. After the "promote" task, references to the old lead chassis exist as a member of the same group. The references are created to prevent any disruption to the working computes in the old lead in a lead chassis MM failure situation.

      The "promote" task rediscovers all the members in the group and if any member chassis is inaccessible then, the chassis is still listed in the lead home page with a broken connection and available repair options. You can use the repair option to add the member chassis again or remove the chassis from the group.

   b. All firmware baselines or catalogs, alert policies, templates or identity-pools, and fabrics settings are restored as they were on the failed lead chassis. However, following are some exceptions and limitations:
      i. Any recent configuration changes on the failed lead within the 90 minutes window that is needed for copying to the backup, those configurations may not be copied completely to the backup and are not restored completely after the "promote" task.
      ii. The in-progress and partially copied jobs that are associated with templates/identity-pools continue to run. You can perform one of the following tasks:
         i. Stop the running job.
         ii. Reclaim any identity-pool assignments.
         iii. Restart the job to redeploy the template.
      iii. Any template that is attached to an occupied slot through the lead before the backup takes over as the new lead, is not deployed on the existing sled when it is removed or reinserted. For the deployment to work, the administrator must detach the template from the slot, reattach the template to the slot, and remove or reinsert the existing sled. Or, insert a new sled.
      iv. Any firmware catalogs that are created with automatic update catalog on a schedule are restored as manual updates. Edit the catalog and provide automatic update method with update frequency.
      v. Alert Policies, with stale or no references to devices on the old lead, are not restored on the new lead.
   c. Steps that are required to restore the failed lead before putting it into production:
      i. On the new lead, turn off the chassis remotely before performing the "promote" task on the backup. If the chassis not turned off, the partially failed lead may come online and cause a situation of multiple leads. There is limited support in automatic detection and recovery of this situation. If the earlier lead comes online and automatic recovery is possible, the earlier lead is forced to join the group as a member.
      ii. On the new lead, remove the earlier lead chassis from the group to remove references to it.
      iii. On the old lead, gain physical access to the failed lead chassis as soon as possible and unstack it from the group. If there were any templates with identity-pool assignments that are deployed to any computes on the old lead, then reclaim the identity-pool assignments from the computes. Reclaiming the identity pool assignments is required to prevent any network identity collision when the old chassis is put back into production.
      iv. Do not delete fabrics from the old lead chassis as deleting the fabrics can lead to network loss once the old lead is added back to the network.
      v. On the old lead, run a force “reset configuration” using the following REST API payload:

URI: `/api/ApplicationService/Actions/ApplicationService.ResetApplication`

Method: `POST`

Payload: `{"ResetType": "RESET_ALL", "ForceReset": true}`

d. Relocate the working components of the old lead to other chassis in the group:
   i. Relocate network switches from the old lead to the new lead or member chassis in the group to restore the health of the fabrics.
   ii. Relocate computes from the old lead to the new lead or member chassis in the group. New templates or identities must be deployed on the computes before resuming workloads, which they were running on the old lead chassis.

Retiring lead chassis

The "retire" option enables a backup chassis to takeover as the lead of a chassis group when the lead chassis is running for a long time and must be removed from the production environment temporarily or permanently. The lead chassis can gracefully detach from the group. The "retire" option also facilitates the lead to retire from the lead role but remain a member of the group.

1. Run "retire" task from the lead chassis:
   a. A job is created when the "retire" task starts. The job may be completed in 10-45 minutes based on the number of chassis in the group and amount of configuration to restored.
   b. If the lead chassis is configured to forward alerts to external destinations (email, trap, system log), any alerts that the components in the group generate are only available locally in their respective hardware. Also, an alert is logged when the retire task and the backup chassis taking over the lead chassis is in progress. After the "retire" task is complete and before the backup is promoted, there is an outage in group management. The outage includes forwarding of alerts to configured external destinations.
2. Expected behavior of backup on completion of the "retire" task:
   a. The backup chassis becomes the new lead and all the member chassis are accessible as they were on the retired lead chassis. The new lead chassis rediscovers all the members in the group and if any member chassis is inaccessible then, the members are still listed on the **Home** page of the lead chassis with broken connection and available repair options. Use the repair option to re-add or remove the member chassis from the group.
   b. All firmware baselines or catalogs, alert policies, templates or identity-pools, and fabrics settings are restored, as they were on the retired lead chassis.
3. Expected behavior of old lead chassis on completion of the "retire" task:
   a. If the old lead is chosen to retire as a stand-alone chassis, it continues to carry the templates/identity-pools configuration. Perform the following steps to clear configuration to avoid conflicts with the new lead.
      i. Unstack the earlier lead from the group.
      ii. Reclaim any identity-pool IO identities that are deployed to computes on the old lead.
      iii. Do not delete fabrics from the old lead chassis as deleting the fabrics can lead to network loss once the old lead is added back to the network.
      iv. Run a force “reset configuration” using the following REST API payload:

      URI: `/api/ApplicationService/Actions/ApplicationService.ResetApplication`

      Method: `POST`

      Payload: `{"ResetType": "RESET_ALL", "ForceReset": true}`

   b. If the old lead is retired as a member of the current group, it no longer carries the identity-pools configuration. However, it contains the templates and profiles configuration. To avoid conflicts with the new lead, these configurations should not be modified or deleted until this chassis exits the MCM group.

19

Troubleshooting

This section describes the tasks for troubleshooting and resolving issues using the OME–Modular user interface.

- Firmware update is failing.
- Storage assignment is failing.
- Management role of IOMs is downgraded.
- IOM health is downgraded.
- Drives on compute sled are not visible.
- Storage sleds cannot be applied to IOMs.
- Drives in OpenManage are not visible.
- iDRAC drive information does not match OpenManage drive information.
- The assignment mode of storage sled is unknown.

NOTE: For more trouble shooting information, see *Dell PowerEdge MX Networking Deployment Guide* available at / infohub.delltechnologies.com

Topics:

Storage

This section describes the issues that are related to storage sleds and steps to resolve the issues.

Firmware update is failing

1. Firmware update may fail if one or more subcomponents fail to flash during the firmware update process.
2. If an IOM is downgraded owing to a chassis mismatch or faulty subcomponent, the firmware activation fails.

Storage assignment is failing

A storage assignment fails if:

1. The IOMs are currently downgraded.
2. There is only one IOM present.
3. Only one hot-swappable Expander is present on a storage sled.

SAS IOM status is downgraded

Both SAS IOMs are degraded if a:

1. Peer SAS IOM is detected but cannot be communicated with.
2. Firmware Mismatch is detected.
3. Chassis Mismatch is detected.

SAS IOM health is downgraded

The SAS IOM health is downgraded if:

1. One or more subcomponents are faulty.

2. A non-SAS IOM is detected.
3. An inconsistency is detected in the subcomponent firmware.

Drives on compute sled are not visible

1. If the compute sled is configured with a PERC controller and the drives have been reseated or moved, they are rediscovered as "Foreign".
2. If the drives are removed from the storage sled, they cannot be discovered.
3. If a storage sled is replaced, the storage configuration of the earlier sled cannot be applied to the replaced sled.

Storage configuration cannot be applied to SAS IOMs

1. If a storage sled is replaced, the storage configuration of the earlier sled cannot be applied to the replaced sled.
2. If a firmware mismatch is detected on the boot of the SAS IOM, the storage configuration is not applied.
3. If a chassis mismatch is detected on the boot of the SAS IOM, the storage configuration is not applied.
4. If the storage sled cannot be communicated with or has an Expander fault, the SAS IOM cannot apply the respective storage configuration.

Drives in OpenManage are not visible

1. The storage sled may have experienced an Expander failure which blocks the drives from being inventoried.
2. To view the drives, refresh the storage sled inventory.

iDRAC and OpenManage drive information do not match

The drive information of iDRAC and OpenManage may not match owing to the mechanisms that iDRAC and the SAS IOM used to fetch and detect the storage details for storage sleds.

The assignment mode of storage sled is unknown

1. If the IOM management role is currently downgraded, then the storage sled assignment mode may not be read.
2. You may have to refresh the **Storage** sled inventory page.
3. If the storage sled health is non-optimal the assignment mode may be downgraded.

Unable to access OME-Modular using Chassis Direct

On systems running Linux operating systems, you may be unable to access `ome-m.local` from your web browser using Chassis Direct. The inaccessibility could be due to missing IP address on the USB network link on the system. To fix this issue, perform one of the following steps while the USB cable is connected to the system and the chassis.

- On the system, go to the **Settings** > **Network** and enable **USB Ethernet**.
- On the top-right corner of the screen and click **Connect**.

Troubleshooting lead chassis failure

When a lead chassis is in phase of coming online after it has failed, the transition must be detected automatically. If you have promoted the backup lead chassis as the new lead chassis, ensure that the earlier lead chassis transitions properly before you put it back into the production environment.

Before putting the earlier lead chassis back into production, perform the following steps:

1. Disconnect the stacking cable.
2. Run the RESTful API to force reset to default.
   The lead chassis becomes a stand-alone chassis.

3. Connect the stacking cable and add the stand-alone member to the same or different chassis group.

A

Recommended slot configurations for IOMs

The table below contains the recommended IOM slot configurations.

Table 29. Recommended IOM slot matrix

Slot A1	Slot A2	Slot B1	Slot B2
MX9116n	MX9116n	Empty	Empty
MX5108n	MX5108n	Empty	Empty
MX7116n	MX7116n	Empty	Empty
25G PTM	25G PTM	Empty	Empty
10GBT PTM	10GBT PTM	Empty	Empty
MX9116n	MX9116n	MX9116n	MX9116n
MX5108n	MX5108n	MX5108n	MX5108n
MX7116n	MX7116n	MX7116n	MX7116n
MX9116n	MX7116n	Empty	Empty
MX7116n	MX9116n	Empty	Empty
MX9116n	MX7116n	MX9116n	MX7116n
MX7116n	MX9116n	MX7116n	MX9116n
25G PTM	25G PTM	25G PTM	25G PTM
10GBT PTM	10GBT PTM	10GBT PTM	10GBT PTM

Topics:

- Supported slot configurations for IOMs

Supported slot configurations for IOMs

The table below contains the supported IOM slot configurations.

Table 30. Supported IOM slot matrix

Slot A1	Slot A2	Slot B1	Slot B2
MX9116n	Empty	Empty	Empty
MX5108n	Empty	Empty	Empty
MX7116n	Empty	Empty	Empty
25G PTM	Empty	Empty	Empty
10GBT PTM	Empty	Empty	Empty
MX9116n	Empty	MX9116n	Empty
MX5108n	Empty	MX5108n	Empty
MX7116n	Empty	MX7116n	Empty
25G PTM	Empty	25G PTM	Empty

Table 30. Supported IOM slot matrix (continued)

Slot A1	Slot A2	Slot B1	Slot B2
10GBT PTM	Empty	10GBT PTM	Empty
MX9116n	MX9116n	MX9116n	Empty
MX5108n	MX5108n	MX5108n	Empty
MX7116n	MX7116n	MX7116n	Empty
25G PTM	25G PTM	25G PTM	Empty
10GBT PTM	10GBT PTM	10GBT PTM	Empty
MX9116n	MX9116n	MX5108n	MX5108n
MX9116n	MX9116n	25G PTM	25G PTM
MX9116n	MX9116n	10GBT PTM	10GBT PTM
MX9116n	MX7116n	MX5108n	MX5108n
MX7116n	MX9116n	MX5108n	MX5108n
MX9116n	MX7116n	25G PTM	25G PTM
MX7116n	MX9116n	25G PTM	25G PTM
MX9116n	MX7116n	10GBT PTM	10GBT PTM
MX7116n	MX9116n	10GBT PTM	10GBT PTM
MX7116n	MX7116n	MX5108n	MX5108n
MX7116n	MX7116n	25G PTM	25G PTM
MX7116n	MX7116n	10GBT PTM	10GBT PTM
MX5108n	MX5108n	MX9116n	MX9116n
MX5108n	MX5108n	MX7116n	MX7116n
MX5108n	MX5108n	MX9116n	MX7116n
MX5108n	MX5108n	MX7116n	MX9116n
MX5108n	MX5108n	25G PTM	25G PTM
MX5108n	MX5108n	10GBT PTM	10GBT PTM
25G PTM	25G PTM	MX9116n	MX9116n
25G PTM	25G PTM	MX7116n	MX7116n
25G PTM	25G PTM	MX9116n	MX7116n
25G PTM	25G PTM	MX7116n	MX9116n
25G PTM*	25G PTM*	10GBT PTM*	10GBT PTM*
10GBT PTM	10GBT PTM	MX9116n	MX9116n
10GBT PTM	10GBT PTM	MX7116n	MX7116n
10GBT PTM	10GBT PTM	MX9116n	MX7116n
10GBT PTM	10GBT PTM	MX7116n	MX9116n
10GBT PTM*	10GBT PTM*	25G PTM*	25G PTM*

LEGEND:

*—Combining two types of Pass-Through Modules (PTMs) is supported.

B

Updating components in phased update order through manual orchestration

NOTE: Phased update order is supported for OME-M 1.40.xx when updating to 2.00.00.

The phased update order helps you to manually orchestrate MX component updates with no workload disruption. Update the components in the following order:

1. OME-Modular
2. Network IOMs (Smart Fabrics and Full-Switches) and SAS IOMs
3. Server update—Phased update of servers (depending on clustering solution)

NOTE: It is recommended that you update the solution in two maintenance windows. During both the maintenance windows, there shall be no disruptions to the workloads running on the server.

Table 31. Nondisruptive update through manual orchestration

Maintenance window	Update order	Configuration changes allowed	Baseline version	OME-M	SAS IOMs	Network IOMs	Servers/ iDRAC components
Production		Yes	**1.40.xx**				
Day 1	OME-M	**No**	Combination of 1.40.XX and 2.00.00	**2.00.00**	1.40.xx	1.40.xx	1.40.xx
Day 1	SAS IOMs	**No**	Combination of 1.40.xx and 2.00.00	2.00.00	**2.00.00**	1.40.xx	1.40.xx
Day 1	Fabrics, switches, and PTMs	**No**	Combination of 1.40.xx and 2.00.00	2.00.00	2.00.00	**2.00.00**	1.40.xx
Break for 24 hours to 1 week		**No**	Combination of 1.40.xx and 2.00.00	2.00.00	2.00.00	2.00.00	1.40.xx
Day 2	Servers	**No**	Combination of 1.40.xx and 2.00.00	2.00.00	2.00.00	2.00.00	**2.00.00**
Production		Yes	**2.00.00**				

Scenario-based update process

Updating MX solution with smart fabrics and storage

1. Update OME-M on all chassis.
2. Update network IOM switches hosting the smart fabrics.
   - Fabric manager automatically orchestrates the switch update one at a time to ensure that there is no data path disruption.
3. Update SAS IOMs on all chassis
   - Active SAS IOM automatically orchestrates update of both active and passive SAS IOMs one at a time to ensure that there is no data path disruption.

4. Update Servers
   - Server update depends on the virtual solution and its capabilities that are used in hosting the server operating system. Typically, customer would have a clustering solution for high availability and scalability.
   - Follow the steps below to update one server at a time:
     - Put the server into the maintenance mode using the virtualized solution interfaces.

       NOTE: This action may force the workload on the server to be moved to another instance in the cluster.
     - Update all the server components using OME-M.
     - Put the server back into production mode using the virtualized solution interfaces.
     - Repeat this process for all servers in the solution.

Updating MX solution with full switch configuration and storage

1. Update OME-M on all chassis.
2. Update network IOM switches configured in full switch mode.

   NOTE: If the network IOM switches are in full switch mode, the nondisruptive update order of the individual switch is based on the VLT and other advanced configuration for multipathing.
3. Update SAS IOMs of all chassis
   - Active SAS IOM automatically orchestrates update of both active and passive SAS IOMs one at a time to ensure that there is no data path disruption.
4. Update Servers
   - Server update depends on the virtual solution and its capabilities that are used in hosting the server operating system. Typically, customer would have a clustering solution for high availability and scalability.
   - Follow the steps below to update one server at a time:
     - Put the server into the maintenance mode using the virtualized solution interfaces.

       NOTE: This action may force the workload on the server to be moved to another instance in the cluster.
     - Update all the server components using OME-M.
     - Put the server back into production mode using the virtualized solution interfaces.
     - Repeat this process for all servers in the solution.

C

Creating validated firmware solution baseline using Dell Repository Manager

Dell Repository Manager (DRM) allows you to create a repository and access catalogs from OME-M which can be later imported using CIFS, NFS, or HTTPS.

Adding repository for the baseline

After installing and launching the DRM, add a repository for the baseline that has to be standardized. You can select the previous version from the Index Catalog, and the list of solution baselines are available in the Validated MX Stack Catalog under catalog groups. The versions are numbered in the date year-month-number format. For more information about the catalog versions and the firmware versions, see MX7000 Solution Baselines. For more details on using Dell Repository Manager, see https://www.dell.com/support/kbdoc/000177083

To add repository:

1. On the DRM home page, click **Add Repository**.
2. Enter the **Repository Name** and **Description** of the repository.
3. Select the Base Catalog from the drop-down list. By default, the **Enterprise Sever Catalog** option is selected. The available options are:
   a. Enterprise Server Catalog
   b. Index Catalog
   c. Validated MX Stack Catalog

   The **Base Catalog** window is displayed when you select the **Index Catalog** for earlier versions of the Validated Stack Catalog.
4. On the **Base Catalog** window, select the required catalog from the **Catalogs** dropdown.
5. Click **Add**.

Downloading catalog and creating repository

After adding the repository, you must select a location to host the catalog and the Dell Update Packages (DUPs). The selected location must be a network share which is accessible to OpenManage - Modular on the chassis which uses the baseline. The downloads are done in the background through a job.

To download catalog:

1. On the DRM home page, select the catalog that you created, and click **Download**.

   The **Download Components** window is displayed.
2. Click **Browse**. The browse window is displayed.
3. Select a shared folder and click **Open** to download the baseline.

   NOTE: The shared folder must be accessible to OME-M through CIFS, NFS, or HTTPS from the chassis to use the baseline.

Accessing catalog from OME-Modular

To access catalog:

1. On the OME-M home page, click **Configuration** > **Firmware Compliance** > **Catalog Management**.
2. Click **Add**.
3. On the **Add Update Catalog** wizard, enter **Name**.

4. From the **Catalog Source** tab, select destination to update catalog. The possible options are:
   - Validated firmware solution baseline
   - Latest component versions on Dell.com
   - Network path
5. Enter corresponding network details, if you select the **Network Path** option.
6. Click **Test now** to verify the test connection.
7. Select the option to update catalog. The possible options are:
   - Manually
   - Automatically
8. Select the **Update Frequency**. The possible options are:
   - Daily
   - Weekly
9. Select the **Backup Existing Catalog** checkbox to take back of the existing catalogs.
10. Click **Finish**.

D

Upgrading networking switch using different OS10 DUP versions

The following sections provide you the information to upgrade OS10 using different DUP versions.

NOTE: When you upgrade VLT peers from 10.4.0E (R3S or R4S) to 10.5.0.1 or later during the maintenance window, it may impact traffic during the upgrade.

NOTE: The DUP update procedure is recommended to upgrade OS10 on the MX9116n and MX5108n.

Topics:

Upgrading networking switch to 10.5.0.7 or 10.5.0.9 using DUP

To upgrade network switch using DUP, follow these steps:

1. Download the latest DUP file for the switch from https://www.dell.com/support.
2. On the OME-Modular web interface, go to **Devices** > **I/O Modules**.
3. Select the IOM module on which you must carry out the OS10 upgrade.
4. Click **Update Firmware**.
5. Select the Individual package option, then click **Browse** and go to the location where the DUP was downloaded earlier. Wait for the compliance report, once done, the supported components are displayed.
6. Select the required components and click **Update**, to start the update.
7. Go to **Monitoring** > **Jobs** page, to view the job status.

Prerequisites for upgrading from versions earlier than 10.5.0.5

- When updating, ensure to update the IOMs in groups no larger than four per upgrade job.
- If there are two switches in a full-switch mode VLT, each switch must be part of different upgrade batch for redundancy.
- If there are two switches in a SmartFabric, select only one switch. The other switch is automatically updated and is counted as "2" in that upgrade group.
- Upgrade main or its peer fabric IOM in last group.

NOTE: Run the X.509v3 certificate upgrade script before upgrading any OS versions. For more details see, OS10 firmware update matrix.

To identify the main IOM:

1. Log in to any IOM switch
2. Go to linux prompt using the commands:
   a. `system bash`
   b. `sudo -i`

3. Go to the SmartFabric Services CLI prompt using the command:

```
python /opt/dell/os10/bin/rest-service/tool/dnv_cli.py
```

4. Get the main IOM service tag using below command:

```
show cluster
```

Prerequisites for upgrading from 10.5.0.5

- When updating, ensure to update the IOMs in groups no larger than four per upgrade job.
- If there are two switches in a full-switch mode VLT, each switch should be part of different upgrade batch for redundancy.
- If there are two switches in a SmartFabric, select only one switch. The other switch is automatically updated and is counted as "2" in that upgrade group.

NOTE: Run the X.509v3 certificate upgrade script before upgrading any OS versions. For more details see, OS10 firmware update matrix.

E

Upgrading networking switch using CLI

NOTE: Upgrade the MX9116n and MX5108n switches to 10.5.1.9 or 10.5.2.6 only if the switches are running 10.5.0.9 or certificate installed 10.5.0.7. For more information, see OS10 firmware update matrix.

NOTE: Upgrade the MX9116n and MX5108n switches to 10.5.1.X only if the switches are running 10.5.0.7 or later. While updating, ensure that the IOMs in the group are not more than six per upgrade job.

NOTE: To upgrade the networking switch from 10.4.0E (R3S or R4S), upgrade and reload both the VLT nodes simultaneously. Perform the update during the maintenance window as the data traffic may be affected during the upgrade.

Important notes to upgrade:

- Versions 10.5.0.1 and later—For a fabric or VLT, upgrade one IOM and then proceed with its peer after the completion of the first IOM.
- Versions 10.4.0E(R4S) and earlier to 10.5.0.7—Update both the IOMs of a fabric or VLT and reboot them simultaneously.
- Version 10.5.0.7/10.5.0.9—Upgrade up to maximum of six IOMs together.
- Versions earlier than 10.5.0.7—Upgrade up to maximum of four IOMs together.

1. Perform the following steps to upgrade the Networking I/O Module.
   a. **(Optional)** Back up the current running configuration to the startup configuration in EXEC mode.

Table 32. Command description

Command	Description
`OS10# copy running-configuration startup-configuration`	Back up the running configuration to startup configuration.

   b. Back up the startup configuration in EXEC mode.

Table 33. Command description

Command	Description
`OS10# copy config://startup.xml config://<backup file name>`	Back up the startup configuration in EXEC mode.

   c. Download the new software image from the Dell Support Site, extract the bin files from the tar file, and save the file in EXEC mode.

Table 34. Command description

Command	Description

`OS10# image download file-url`
Example:
`OS10# image download ftp://userid:passwd@hostip:/filepath`
	Download the new software image.

NOTE: Some Windows extract applications insert extra carriage returns (CR) or line feeds (LF) when they extract the contents of a .tar file, which may corrupt the downloaded OS10 binary image. Turn off this option, if you are using a Windows-based tool to extract an OS10 binary file.

   d. **(Optional)** View the current software download status in EXEC mode.

Table 35. Command description

Command	Description
`OS10# show image status`	View the current software download status.

e. Install the 10.5.0.5 software image in EXEC mode.

Table 36. Command description

Command	Description

`OS10# image install image-url`
Example:
`OS10# image install image://filename.bin`
	Install the software image.

f. **(Optional)** View the status of the current software install in EXEC mode.

Table 37. Command description

Command	Description
`OS10# show image status`	View the status of the current software install.

g. Change the next boot partition to the standby partition in EXEC mode. Use the active parameter to set the next boot partition from standby to active.

Table 38. Command description

Command	Description
`OS10# boot system standby`	Change the next boot partition to standby.

h. **(Optional)** Check whether the next boot partition has changed to standby in EXEC mode.

Table 39. Command description

Command	Description
`OS10# show boot detail`	Check whether the next boot partition has changed.

i. Reload the new software image in EXEC mode.

Table 40. Command description

Command	Description
`OS10# reload`	Reload the new software.

j. After the installation is complete, enter the show version command to check if the latest version of the software that you have installed is running in the system.

The example below shows that the 10.5.0.5 software is installed and running on the system.

```
OS10# show version
MX9116N-A2# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.5
Build Version: 10.5.0.5.661
Build Time: 2020-02-15T00:45:32+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 1 day 20:37:53
MX9116N-A2#
```

2. Run the command, `show smartfabric cluster member`, in the main networking switch. Confirm that the `STATUS` of the upgraded switch is `ONLINE` in the command output, after it has reloaded. The networking switches with version 10.5.01 and higher uses SFS CLI, whereas the lower versions like 10.4.0E(R3S) and 10.4.0E(R4S) use `python /opt/dell/os10/bin/rest-service/tool/dnv_cli.py` show cluster command. For steps to identify the main IOM, see upgrading from versions earlier than 10.5.0.5 section.

NOTE: During the image upgrade process in a VLT setup, if the VLT peers are running different software versions, do not change the configuration in any VLT peer. Ensure that both the nodes are upgraded to the same version before you change the configuration.

```
IOM# show smartfabric cluster member
Service-tag  IP Address  Status         Role        Type          Chassis-Service-Tag
 Chassis-Slot
MXWV122  xxxxxxxxxxx   ONLINE   MAIN     MX9116n  SKYMX02             A2
MXLE103    xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX10             B2
MXLE093   xxxxxxxxxxx   ONLINE    BACKUP     MX9116n  SKYMX09             B1
MXWV011  xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX01             A1
```

F

CLI commands not part of chassis backup

Chassis backup is not supported on some of the CLI configurations. The list of CLI configurations and respective commands are as in the table below.

Table 41. CLI commands

Module/Feature	Command	Description	Yang objects
AAA	aaa accounting <>	All aaa accounting command options	/dell-system: aaa
	aaa authentication <>	All aaa authentication commands	
	aaa re-authenticate [enable]		
Banner	banner login <>	All login banner command options	/dell-system:system
	banner motd <>	All login motd command options	
CLI	alias [alias-name [alias-value]]	Inclusive of all subcommands.	/dell-cli:cli-config
Clock	clock <>	All clock command options	/dell-system:system
Crypto	crypto [fips [enable]]		/dell-system:crypto
Eula consent	eula-consent support-assist [accept] | reject]		/dell-support-assist:sa-cfg
Exec timeout	exec-timeout [0-3600]		/dell-session:sessionconfig
FC	fc alias [fc-name]	Inclusive of all sub-commands.	/dell-fc-services:fc-cfg
	fc zone [zonename	Inclusive of all sub-commands.	
	fc zoneset [<string>]	Inclusive of all sub-commands.	
Hardware	hardware forwarding-table [mode [scaled-l2]]	scaled-l3-routes and scaled-l3-hosts options are not enabled because L3 aspects are not applicable in fabric mode	/dell-switch-resource:forwarding-table-config
Help	help		
Host description	host-description [<string>]		/dell-system:system
Hostname	hostname [<string>]		/dell-system:system
Hidden commands	allow unsupported-transceiver		/dell-equipment:media-optic-cfg
Line	line vty		/dell-policy:config/dell-policy:policy-vty-config
Logging	logging <>	All logging command options except for interface and VRF	/dell-policy:acl-logging /dell-logging:logging-trace
Login	login concurrent-session [limit []]		/dell-system:login /dell-system:login statistics
	login statistics [time-frame []] | enable]		

Table 41. CLI commands (continued)

Module/Feature	Command	Description	Yang objects
NTP	ntp <>	All ntp command options except for interface and VRF	/dell-ntp:ntp-config
Radius server	radius-server host	All radius-server host command options except interface and VRF	/dell-system:system
	radius-server retransmit [retries]		
	radius-server timeout [seconds]		
REST	rest api [intf_type]		/dell-rest:rest
	rest https cipher-suite [suite]		
	rest https server-certificate [name [<string>]]		
	rest https session [timeout []]		
SNMP server	snmp-server <>	All snmp-server command options except for VRF	/dell-snmp:snmp-server
SSH server	ip ssh server <>	All ip ssh server command options except for VRF	/dell-system:ssh-server-config
Support assist	support-assist	Inclusive of all sub commands except for interface specific	/dell-support-assist:sa-cfg
System	system identifier []		/dell-chmgr:system-identifier-cfg /dell-system:system /dell-cli:cli-config
	system-cli [disable]		
	system-user [linuxadmin [password [sys-passwd]] | disable]]		
Tacacs server	tacacs-server <>	All tacacs-server options except for interface and VRF	/dell-system:system
Telnet	ip telnet server <>	All ip telnet server command options except for VRF	/dell-system:system
STP	spanning-tree	All spanning-tree commands	/dell-xstp:config
Username	password-attributes <>	All password-attributes command options	/dell-system:system
	username <>	All username command options	
	userrole	All user role command options	
VFabric	vfabric []	Parent Command vfabric [vfabric-id]	/dell-fc-services:fc-cfg
	zoneset [activate [<string>]]	Sub-Command of "Vfabric"	

G

VMware ESXi/MX Baseline Validation Matrix

Table 42. VMware ESXi/MX Baseline Validation Matrix

		MX Baseline Version								
		OME-M 1.10.20	**OME-M 1.20.00**	**OME-M 1.20.10**	**OME-M 1.30.00**	**OME-M 1.30.10**	**OME-M 1.40.00**	**OME-M 1.40.10**	**OME-M 1.40.20**	**OME-M 2.00.00**
VMware ESXi Version	**ESXi 6.5**	No	No	No	No	No	No	No	No	No
	ESXi 6.5 U1	No	No	No	No	No	No	No	No	No
	ESXi 6.5 U2	No	No	No	No	No	No	No	No	No
	ESXi 6.5 U3	**Yes**	**Yes**	No	No	No	No	No	No	No
	ESXi 6.7	No	No	No	No	No	No	No	No	No
	ESXi 6.7 U1	No	No	No	No	No	No	No	No	No
	ESXi 6.7 U2	No	No	No	No	No	No	No	No	No
	ESXi 6.7 U3	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
	ESXi 7.0	No	**Yes**	**Yes**	No	No	No	No	No	No
	ESXi 7.0 U1	No	No	No	**Yes***	**Yes***	No	No	No	No
	ESXi 7.0 U2	No	No	No	**Yes****	**Yes****	No	No	No	No
	ESXi 7.0 U3c and later	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
	ESXi 8.0	No	No	No	No	No	No	No	No	**Yes*****

- *14th generation compute sleds only
- **15th generation compute sleds only
- ***16th generation compute sleds only

In an MX7000 chassis with MX9116n or MX7116n IOMs, port flapping is observed when Link Layer Discovery Protocol (LLDP) advertisement is active on the distributed virtual switch (vSwitch) settings with ESXi or other operating systems. Disable LLDP from the ESXi vSwitch or any other LLDP coming from the compute node operating system level.

H

MX7000 Solution Baselines for previous versions

Table 43. MX7000—OME-Modular 1.40.20 and previous solution baselines

Validated MX Stack Catalog Version	**NA**	**20.07.00**	**20.10.00**
Component	**v1.10.20**	**v1.20.00**	**v1.20.10**
iDRAC with Lifecycle Controller for PowerEdge MX740c and MX840c	4.11.11.11	4.20.20.20	4.22.00.00
iDRAC with Lifecycle Controller for PowerEdge MX750c	NA	NA	NA
Dell Server BIOS PowerEdge MX740c and 840c	2.5.4	2.8.2	2.9.4** 2.11.2**
Dell Server BIOS PowerEdge MX750c	NA	NA	NA
QLogic 26XX series Fibre Channel adapters	15.05.12	15.05.14	15.15.06
QLogic 27XX series Fibre Channel adapters	15.05.12	15.05.13	15.15.06
QLogic 41xxx series adapters	15.05.14	15.05.18	15.15.11
Broadcom 57504 Quad Port device adapters	NA	NA	21.65.33.33
Mellanox ConnectX-4 Lx Ethernet Adapter Firmware	14.25.80.00	14.26.60.00	14.27.61.22
Intel NIC Family Version Firmware for X710, XXV710, and XL710 adapters	19.5.12	19.5.12	19.5.12
Emulex Fibre Channel Adapter Firmware 32G	03.02.18	03.02.18	03.03.37
OpenManage Enterprise Modular	1.10.20	1.20.00	1.20.10
MX9116n Fabric Switching Engine OS10	10.5.0.5*	• 10.5.0.7*** • 10.5.0.9	• 10.5.1.6*** • 10.5.1.7*** • 10.5.1.9
MX5108n Ethernet Switch OS10	10.5.0.5*	• 10.5.0.7*** • 10.5.0.9	• 10.5.1.6*** • 10.5.1.7*** • 10.5.1.9
MX5016s Storage Sled	2.40	2.40	2.40
MX5000s SAS IOM	1.0.9.6	1.0.9.8	1.0.9.8
MXG610s	8.1.0_Inx3	• 8.1.0_Inx2 • 8.1.0_Inx3	• 8.1.0_Inx2 • 8.1.0_Inx3

Table 43. MX7000—OME-Modular 1.40.20 and previous solution baselines (continued)

Validated MX Stack Catalog Version	**NA**	**20.07.00**	**20.10.00**
Component	**v1.10.20**	**v1.20.00**	**v1.20.10**
Network IOM ONIE	NA	NA	NA
Delta AC PSU	68.5F	68.5F	68.5F
Artesyn AC PSU	36.6C	36.6C	36.6C

*Update to operating system 10.5.0.9 and then to 10.5.1.9 or 10.5.2.6. Run the X.509v3 certificate upgrade script before upgrading any operating system versions. For more details see, OS10 firmware update matrix.

**Update using individual DUP or obtain from the Latest component firmware versions on Dell.com catalog.

***Update restrictions apply. For more information, see OS10 firmware update matrix.

Upgrades from baselines before 1.20.00 might need a power cycle (cold boot) of the MX7000 chassis. Updating all applicable solution components after power cycle may be necessary as a last troubleshooting step. For details, see Controlling chassis power.

I

OME-Modular firmware update matrix for previous versions

Table 44. OME-Modular firmware update matrix for older versions

		To				
		OME-M 1.00.01	**OME-M 1.00.10**	**OME-M 1.10.00**	**OME-M 1.10.10**	**OME-M 1.10.20**
From	**OME-M 1.00.01**	Yes	Yes	—	—	—
	OME-M 1.00.10	—	Yes	Yes	Yes	—
	OME-M 1.10.00	—	—	Yes	Yes	Yes
	OME-M 1.10.10	—	—	—	Yes	Yes
	OME-M 1.10.20	—	—	—	—	Yes
	OME-M 1.20.00	—	—	—	—	—
	OME-M 1.20.10	—	—	—	—	—
	OME-M 1.30.00	—	—	—	—	—
	OME-M 1.30.10	—	—	—	—	—
	OME-M 1.40.00	—	—	—	—	—
	OME-M 1.40.10	—	—	—	—	—
	OME-M 1.40.20	—	—	—	—	—

NOTE: Installing an earlier version of OME-M resets the configuration to factory defaults. This option allows you to maintain a certain firmware level.