**DELL**Technologies

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

## Revision history

**Current Release Version:** 2.00.00

| Date | Document revision | Description of changes |
|------|-------------------|------------------------|
| December 2022 | A01 | v2.00.00 - Updates resolved issues |
| August 2022 | A00 | v2.00.00 - Updates for new features and enhancements |
| March 2022 | A00 | v1.40.20 - Support for Apache log4j version 2.17.1 |
| December 2021 | A00 | v1.40.10 - Support for Apache log4j patch for CVE-2021-044228, CVE-2021-4104, CVE-2021-45046 |
| December 2021 | A00 | v1.40.00 - Updates for new features and enhancements |
| July 2021 | A01 | v1.30.10 - Updates for DC power supply |
| 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 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 |

## Introduction

The Dell OpenManage Enterprise - Modular is a system management hardware and software solution for managing the Dell PowerEdge MX7000 chassis.

This document contains the release notes for OME-Modular release versions.

For recommendation notes for a release upgrade, see the OME-Modular release version under the **Drivers & Downloads** tab under the platform model, on **dell.com/support**.

# Priority and recommendations

RECOMMENDATION: Dell Technologies recommends applying this update during your next scheduled update cycle. The update contains feature enhancements or changes that help keep your system software current and compatible with other system modules (firmware, BIOS, drivers, and software).

# Version matrix

The table below lists the OpenManage Enterprise Modular versions and release dates.

**Table 1. Version matrix**

| Release Version | Release Date | Release Notes |
|---|---|---|
| OpenManage Enterprise Modular version 2.00.00 | August 2022 | OpenManage Enterprise Modular 2.00.00 |
| OpenManage Enterprise Modular version 1.40.20 | March 2022 | OpenManage Enterprise Modular 1.40.20 |
| OpenManage Enterprise Modular version 1.40.10 | December 2021 | OpenManage Enterprise Modular 1.40.10 |
| OpenManage Enterprise Modular version 1.40.00 | December 2021 | OpenManage Enterprise Modular 1.40.00 |
| OpenManage Enterprise Modular version 1.30.10 | July 2021 | OpenManage Enterprise Modular 1.30.10 |
| OpenManage Enterprise Modular version 1.30.00 | May 2021 | OpenManage Enterprise Modular 1.30.00 |
| OpenManage Enterprise Modular version 1.20.10 | August 2020 | OpenManage Enterprise Modular 1.20.10 |
| OpenManage Enterprise Modular version 1.20.00 | June 2020 | OpenManage Enterprise Modular 1.20.00 |
| OpenManage Enterprise Modular version 1.10.20 | March 2020 | OpenManage Enterprise Modular 1.10.20 |
| OpenManage Enterprise Modular version 1.10.10 | November 2019 | OpenManage Enterprise Modular 1.10.10 |
| OpenManage Enterprise Modular version 1.10.00 | September 2019 | OpenManage Enterprise Modular 1.10.00 |
| OpenManage Enterprise Modular version 1.00.10 | February 2019 | OpenManage Enterprise Modular 1.00.10 |
| OpenManage Enterprise Modular version 1.00.01 | September 2018 | OpenManage Enterprise Modular 1.00.01 |

# OpenManage Enterprise Modular 2.00.00

## New and enhanced features

This release of OME-Modular supports:

- 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 swtich mode.

## 1.40.20

- 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 IOMs.
- Enhanced backup and restore for management configuration recovery.
  - System configurations
  - Catalog baselines
  - Alert policies
  - SmartFabric
- Enhanced validated stack 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

## 1.30.00

- Group configuration option on the **Home** page in multi chassis 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
  - 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 EMC PowerEdge MX7000 Enclosure Field Service Manual*.
- PowerEdge MX750c platform.

## 1.20.10

- Quad-Port Ethernet adapters in up to five MX7000 chassis in a scalable fabric.
- Up to 512 VLANs per fabric, 256 VLANs per server port, and up to 512 VLANs per uplink.
- The category, "Unknown" in compliance reports for components that are not supported in catalogs.
- Additional topologies for Fabric Expander Module connectivity.

## 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 Brocade 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.

## 1.10.10

- Technical preview of transparent Ethernet uplink configuration.

## 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

- Manages up to 20 chassis using a single interface—web or RESTful interface.

- Enables editing a VLAN after deployment, from the **Fabric Details** page.
- Certified for Federal Information Processing Standard (FIPS) 140-2 standards. For details, see certificate #2861 at csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2861.

## 1.00.01

- Provides a unified management interface for compute, storage, and networking components.
- Provides end-to-end life cycle management of all components.
- Manages up to 10 chassis using a single interface—web or RESTful interface.
- Manages fabric switch engines in SmartFabric Services mode across all chassis.

# Resolved issues

## Individual chassis MM failover behavior inconsistent among group members

Fixed an issue that was causing MM failover in the lead and member chassis to fail.

**Tracking number**

220552

## Upgrade and downgrade of all components in MCM displayed as completed

Fixed an issue that was causing the upgrade and downgrade of all components in MCM to display the status as "Completed" on the iDRAC interface. The "Completed" status was displayed even as the job was still running.

**Tracking number**

214058

# Known issues

## UI wizards display incorrect text in localized languages

| | |
|---|---|
| **Description** | During configuration template refresh task, the message, "Refresh Template feature is not supported for this template as its DeviceID association to the Reference Device is invalid." is not displayed correctly in localized languages. |
| **Workaround** | N/A |
| **Systems affected** | PowerEdge MX7000, PowerEdge MX740c, PowerEdge MX840c, PowerEdge MX750c |
| **Tracking number** | 230578 |

## USB keyboard controls On-Screen Display menu and sled items simultaneously through RCP

| | |
|---|---|
| **Description** | During KVM sled video session, users press HotKey (<PrtScr>+<PrtScr>) to view the On-Screen Display (OSD) menu. And, keyboard events are sent to OSD menu and the host operating system. |
| **Workaround** | <ul><li>Use mouse to navigate OSD page.</li><li>Use the iDRAC direct or vConsole to directly work on sled.</li></ul> |

| **Systems affected** | All systems supported in this release |
| --- | --- |
| **Tracking number** | 237121 |

## Unable to change the web server configuration HTTPS port from custom to default port

| **Description** | Changing HTTPS port from a custom port back to default port 443 may fail. |
| --- | --- |
| **Workaround** | Set SNMP inbound port configuration to default port 161 and then set HTTPS port configuration back to default port 443. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 237551 |

## OME-Modular with IPv4 IP network accessible from same subnet using different virtual machines

| **Description** | OME-Modular having Restricted or Allowed IP range with 32-bit CIDR configuration may allow more than one host to access OME-Modular. |
| --- | --- |
| **Workaround** | Perform a `racresetcfg` on the chassis to recover from this condition. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 237711 |

# Limitations

1. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
2. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
3. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
4. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
5. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.
6. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
7. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
8. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.

9. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
10. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
11. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
12. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
13. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
14. 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.
15. Odata filtering does not support special characters—**,\**, **_**, **%**, **#**, **'**, **)**, **+**, and **&** for usernames.
16. Remote racadm commands do not work when the TLS version is set to "TLSv1.3 only".

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch
- Generic IOM

## Supported web browsers

- Google Chrome version 102
- Google Chrome version 103
- Mozilla Firefox version 99
- Mozilla Firefox version 100
- Microsoft EDGE 94
- Microsoft EDGE 95
- Microsoft Internet Explorer 11
- Safari version 15

# Installation

See the *Dell OpenManage Enterprise - Modular Edition Version 2.00.00 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 2.00.00

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. The CVEs are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.
- CVE-2021-28041, CVE-2021-41617: The Qualys scan report displays these vulnerabilities when FIPS mode is enabled. These vulnerabilities are false positives.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that you use only **SNMP v3 Only** configuration. For more information, see the Dell OpenManage Enterprise Modular Edition for PowerEdge MX7000 Security Configuration Guide.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid nonself signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners relating to the default self-signed web server certificate, and default SNMP community name, produce.

(i) **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell OpenManage Enterprise - Modular Edition Version 2.00.00 for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

Firmware downgrade, synchronization, and part replacement actions with an older management module do not function when **TLS 1.3 Only** mode is configured. In such cases, change the **TLS Protocol** settings to default value, **TLS 1.2 and Higher**.

## Template deployment

- If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.40.20

## Resolved issues

N/A

## Known issues

For details, see the section, Known Issues under OpenManage Enterprise Modular 1.40.00.

## Limitations

1. OME–Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.
7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
14. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
15. 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.
16. Odata filtering does not support special characters— **,**,**\**, **_**, **%**, **#**, **'**, **)**, **+**, and **&** for usernames.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch
- Generic IOM

## Supported 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 14
- Safari version 15

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.40.20 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.40.20

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. These are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid nonself signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners, relating to the default self-signed web server certificate, and default SNMP community name, produce.

(i) **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

## Template deployment

- If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.40.10

## Resolved issues

For details, see the section, Fixes under OpenManage Enterprise Modular 1.40.00.

## Known issues

For details, see the section, Known Issues under OpenManage Enterprise Modular 1.40.00.

# Limitations

1. OME—Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
14. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
15. 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.
16. Odata filtering does not support special characters— **,,\**, **_**, **%**, **#**, **'**, **)**, **+**, and **&** for usernames.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

## Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

## I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch
- Generic IOM

## Supported 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 14
- Safari version 15

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.40.10 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.40.10

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition for PowerEdge MX7000 Chassis User's Guide* available at https://www.dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. These are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.

## Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid nonself signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners, relating to the default self-signed web server certificate, and default SNMP community name, produce.

ⓘ **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

## Template deployment

- If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.40.00

## Resolved issues

### iDRAC SSO in OME-Modular

Fixed an issue that was causing the iDRAC interface login page to not launch in a new tab from OME–Modular interface, when the custom port was configured to 8080.

**Tracking number**

188432

### Inconsistent behavior in lead and member chassis sleds

Fixed an issue that was causing inconsistent behavior in lead and member chassis sleds during profile deployment in slots.

**Tracking number**

189934

# Configured local time on lead and member chassis

Fixed an issue where the configured local time was not applied on the lead and member chassis after NTP was disabled.

**Tracking number**

192713

# MAC identities displayed in reserved state

Fixed an issue that was causing MAC identities to display RESERVED state for some partitions after Slot Deployment was performed using **Attach** and **Apply Immediately** operation.

**Tracking number**

194347

# Chassis alerts in Redfish event listener

Fixed an issue that was causing the Redfish event listener to not receive chassis alerts after management module failover.

**Tracking number**

195224

# Redeployment of MCM profiles for all member chassis sleds

Fixed an issue that was causing failure of server profile deployment with modified attributes for member chassis sleds when only VLAN configuration was modified.

**Tracking number**

195597

# All passive member chassis management system modules reboot

Fixed an issue that was causing all standby management system modules on the member chassis to reboot after `racadm racreset` task was performed on the lead chassis.

**Tracking number**

195686

# Power supply input voltage and input current display nil for PSUs

Fixed an issue that was causing the `PSUInputVoltage` and `PSUInputCurrent` to display "Nil" when a PSU was removed from the chassis and an SSE get call was run using a browser.

**Tracking number**

201641

# Windows keystroke ineffective on sleds

Fixed an issue that was causing the Windows key to be ineffective on sleds when the chassis was connected to KVM.

**Tracking number**

202510

# Empty PSU slot in DC chassis displays AC

Fixed an issue that was causing empty PSU slot in DC chassis to display AC in two SNMP and RESTful API interfaces.

**Tracking number**

202369

# Known issues

## Upgrade and downgrade of all components in MCM is marked completed when the job is running

| | |
|---|---|
| **Description** | In MCM environment, upgrade and downgrade of all components is displayed as "Completed" on the iDRAC user interface even as the job is in progress. |
| **Workaround** | None |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 214058 |

## MXG610s uplinked to Nexus9000 C93180YC-FX does not come online

| | |
|---|---|
| **Description** | MXG610s, in AG mode, when uplinked to Nexus9000 C93180YC-FX does not come online with speed set to **AutoNegotiate**. |
| **Workaround** | Hard-set the speed to 32G on both sides of the link to come up. During testing, it was observed that setting 32G fixed speed on both ends of link always brings up the ports. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 214065 |

## Template deployment for all sleds in MCM fails

| | |
|---|---|
| **Description** | In MCM, template deployment for all sleds fails when the original template extracted from iDRAC 4.40.10.00 is deployed in iDRAC 5.10.00.00 firmware. |
| **Workaround** | <ul><li>Always capture and deploy templates to and from identical hardware and firmware configurations.</li><li>Before applying a server profile, ensure the number of ports on a profile matches that of the target server.</li><li>Ensure all the server ports are properly connected to I/O modules.</li></ul> |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 211447 |

## Some sled alerts display source as "Member chassis" instead of "Member sled"

| | |
|---|---|
| **Description** | In a multichassis environment, when sleds are removed and reinserted from the lead and member chassis, some sled alerts display the source as "Member chassis" instead of "Member sled". |
| **Workaround** | When post inventory of sled is completed in Lead chassis, the expected sled source name is displayed in alerts. |
| **Systems affected** | All systems supported in this release |

**Tracking number**     204373

## Advanced Filter option not working in Audit Logs

**Description**          On the **Audit Logs** page, the **Advanced Filter** does not work when you enter search text containing special characters such as accented vowel.

**Workaround**          Use filter search on other parts of the text which do not use UTF-8 characters.

**Systems affected**    All systems supported in this release

**Tracking number**     154213

## Maximum template deployment from OpenManage Enterprise causes inaccessibility of management module chassis

**Description**          When maximum template (160 sleds) deployment is triggered from OpenManage Enterprise, OME-Modular becomes unresponsive.

**Workaround**          Deploy templates in smaller groups or wait for OpenManage Enterprise to complete the job and the system recovers.

**Systems affected**    All systems supported in this release

**Tracking number**     198313

# Limitations

1. OME—Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.

10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
14. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
15. 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.
16. Odata filtering does not support special characters— **,,\\**, **_**, **%**, **#**, **'**, **)**, **+**, and **&** for usernames.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch
- Generic IOM

## Supported 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 14
- Safari version 15

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.40.00 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.40.00

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition for PowerEdge MX7000 Chassis User's Guide* available at https://www.dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. These are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners, relating to the default self-signed web server certificate, and default SNMP community name, produce.

(i) **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

## Template deployment

- If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.30.10

## Resolved issues

### Incorrect dependency component download link

Fixed an issue where the dependency information link was incorrect when baseline is accessed using **Device** > **Update** > **Baseline** > **Prerequisite**.

**Tracking number**

194579

### Video refreshes slowly on screen refresh

Fixed an issue with KVM performance while using the DisplayPort on the front of the chassis.

**Tracking number**

203780

## Known issues

### Advanced Filter option not working in Audit Logs

| | |
|---|---|
| **Description** | On the **Audit Logs** page, the **Advanced Filter** does not work when you enter search text containing special characters such as accented vowel. |
| **Workaround** | Use filter search on other parts of the text which do not use UTF-8 characters. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 154213 |

### iDRAC SSO does not work in OME-Modular

| | |
|---|---|
| **Description** | For iDRAC SSO login, click **Compute Overview** > **Launch iDRAC** or **Compute Overview** > **Virtual Console**. The iDRAC user interface login page is not launched in a new tab from the OME-Modular interface when the custom port is configured to 8080. |
| **Workaround** | Use a port other than 8080 or the default port, 443. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 188432 |

### Inconsistent behavior in lead and member chassis sleds during slot deployment

| | |
|---|---|
| **Description** | In MCM environment, when you attach a profile to a member chassis slot from the lead chassis and insert a compute and perform an erase operation on the compute, the profile is not deployed after the compute comes up. But in stand-alone and lead chassis, where the sled is physically present on the chassis, the profile is deployed after the erase operation. |
| **Workaround** | Unassign profiles that are deployed on an erased compute. |

**Systems affected**   All systems supported in this release

**Tracking number**   189934

# Configured local time not applied on lead chassis and member chassis after disabling NTP

**Description**   When you clear the external NTP and change the local time, internal NTP is slow in identifying the correct time source. As a result, the time is reverted.

**Workaround**   Set the required time on the **Application Settings** > **Network** > **Time Configuration** page.

**Systems affected**   All systems supported in this release

**Tracking number**   192713

# MAC identities displayed in RESERVED state

**Description**   MAC identities displayed in RESERVED state for some of the partitions after Slot Deployment is performed using Attach and Apply Immediately operation.

**Workaround**   Redeploy OME-Modular.

**Systems affected**   All systems supported in this release

**Tracking number**   194347

# Chassis alerts not received in Redfish event listener after management module failover task

**Description**   After the first management module (MM) failover:
- POST subscribers do not receive alerts and telemetry events.
- Telemetry customizations are not effective but are not lost.

**Workaround**   Perform a second MM failover task.

**Systems affected**   All systems supported in this release

**Tracking number**   195224

# Redeployment of MCM profiles for all member chassis sleds fails when VLAN is modified in device-based deployment

**Description**   Server Profile deployment with modified attributes is failing for member sleds when only VLAN configuration is modified.

**Workaround**   While modifying the VLAN configuration from the **Edit Network** page, select the **Propagate VLAN** checkbox. Perform full redeployment of the profile.

**Systems affected**   All systems supported in this release

**Tracking number**   195597

# All member chassis passive module is getting rebooted when performing "racadm racreset" in lead chassis

| | |
|---|---|
| **Description** | Standby management system modules on the Member chassis are rebooted after "racadm racreset" operation is performed on Lead chassis. |
| **Workaround** | • If the system is already in failed state, a user can change the timezone to something other than GMT from Lead MSM GUI/Standalone which propagates the new timezone to all the Members in the group. Else, irrespective of MCM or Standalone setup, before performing "racadm racresetcfg", set the time zone to GMT.<br>• If the setup is already in MCM group, remove the member chassis from the group and change the timezone as stated above before performing the "racadm racresetcfg". |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 195686 |

# Maximum template deployment from OpenManage Enterprise on management module sleds causes management module chassis to be inaccessible

| | |
|---|---|
| **Description** | When maximum template (160 sleds) deployment is triggered from OpenManage Enterprise, OME-Modular becomes unresponsive. |
| **Workaround** | Deploy templates in smaller groups or wait for OpenManage Enterprise to complete the job and the system recovers. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 198313 |

# Power supply input voltage and input current display nil for PSUs that are removed

| | |
|---|---|
| **Description** | When a Power Supply Unit (PSU) is removed from the chassis and an SSE get call is run using a browser, the `PSUInputVoltage` and `PSUInputCurrent` display "Nil" for the PSU. |
| **Workaround** | Remove the external power supply to prevent the issue. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 201641 |

# Windows keystroke does not work on sled when chassis is connected to KVM

| | |
|---|---|
| **Description** | The Windows key is not effective when you press it from the KVM session. |
| **Workaround** | All keystrokes work correctly with Virtual Network Computing (VNC) and vConsole. You can switch to vConsole or VNC. |
| **Systems affected** | All systems supported in this release. |
| **Tracking number** | 202510 |

# PSU type displays AC for removed PSU or empty PSU slot in DC chassis in SNMP and RESTful API interfaces

**Description**        Empty PSU slot in DC chassis displays AC in two SNMP and RESTful API interfaces.

**Workaround**        None

**Systems affected**   All systems supported in this release

**Tracking number**   202369

# Limitations

1. OME−Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.
7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
14. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
15. 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.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch

## Supported web browsers

- Google Chrome version 90
- Google Chrome version 91
- Mozilla Firefox version 88
- Mozilla Firefox version 89
- Microsoft EDGE 90
- Microsoft EDGE 91
- Microsoft Internet Explorer 11
- Safari version 13
- Safari version 14

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.30.10 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.30.10

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.30.00 for PowerEdge MX7000 Chassis User's Guide* available at https://www.dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. These are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners, relating to the default self-signed web server certificate, and default SNMP community name, produce.

(i) **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.30.00 for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

## Template deployment

- If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.30.00

## Resolved issues

For the list of issues fixed, see the *OpenManage Enterprise-Modular Edition for PowerEdge MX7000 Chassis Release Notes* for 1.30.10, available on **dell.com/manuals**.

## Deployment and configuration job for sleds

Fixed an issue that was creating multiple deployment and configuration jobs for some sleds during **Quick Deploy** and **Attach** tasks.

**Tracking number**

141623

## Assigning identities

Fixed an issue that was causing errors while assigning identities on the **Template Deployment** > **Reserve Identities Error** page.

**Tracking number**

142004

## Disabled NIC partitions

Fixed an issue that was enabling NIC partitions that were disabled, and displaying in iDRAC and operating system after template deployment.

**Tracking number**

166566

## Jobs for all device actions

Fixed an issue that was creating jobs for all device actions instead of the selected or filtered device actions.

**Tracking number**

174924

## Storage devices on member chassis

Fixed an issue that was causing storage devices on member chassis to be reported as unknown, though storage firmware was present in the catalog.

**Tracking number**

174410

## Validated stack catalog download

Fixed an issue that was causing an error while downloading validated stack catalog using the option, **Newest validated stacks of chassis firmware on Dell.com**.

**Tracking number**

192282

# Known issues

## Advanced Filter option not working in Audit Logs

| | |
|---|---|
| **Description** | On the **Audit Logs** page, the **Advanced Filter** does not work when you enter search text containing special characters such as accented vowel. |
| **Workaround** | Use filter search on other parts of the text which do not use UTF-8 characters. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 154213 |

# iDRAC SSO does not work in OME-Modular

| | |
|---|---|
| **Description** | For iDRAC SSO login, click **Compute Overview** > **Launch iDRAC** or **Compute Overview** > **Virtual Console**. The iDRAC user interface login page is not launched in a new tab from the OME-Modular interface when the custom port is configured to 8080. |
| **Workaround** | Use a port other than 8080 or the default port, 443. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 188432 |

# Inconsistent behavior in lead and member chassis sleds during slot deployment

| | |
|---|---|
| **Description** | In MCM environment, when you attach a profile to a member chassis slot from the lead chassis and insert a compute and perform an erase operation on the compute, the profile is not deployed after the compute comes up. But in stand-alone and lead chassis, where the sled is physically present on the chassis, the profile is deployed after the erase operation. |
| **Workaround** | Unassign profiles that are deployed on an erased compute. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 189934 |

# Configured local time not applied on lead chassis and member chassis after disabling NTP

| | |
|---|---|
| **Description** | When you clear the external NTP and change the local time, internal NTP is slow in identifying the correct time source. As a result, the time is reverted. |
| **Workaround** | Set the required time on the **Application Settings** > **Network** > **Time Configuration** page. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 192713 |

# MAC identities displayed in RESERVED state

| | |
|---|---|
| **Description** | MAC identities displayed in RESERVED state for some of the partitions after Slot Deployment is performed using Attach and Apply Immediately operation. |
| **Workaround** | Redeploy OME-Modular. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 194347 |

# Chassis alerts not received in Redfish event listener after management module failover task

| | |
|---|---|
| **Description** | After the first management module (MM) failover:<br>• POST subscribers do not receive alerts and telemetry events.<br>• Telemetry customizations are not effective but are not lost. |
| **Workaround** | Perform a second MM failover task. |

**Systems affected**    All systems supported in this release

**Tracking number**    195224

# Redeployment of MCM profiles for all member chassis sleds fails when VLAN is modified in device-based deployment

**Description**    Server Profile deployment with modified attributes is failing for member sleds when only VLAN configuration is modified.

**Workaround**    While modifying the VLAN configuration from the **Edit Network** page, select the **Propagate VLAN** checkbox. Perform full redeployment of the profile.

**Systems affected**    All systems supported in this release

**Tracking number**    195597

# All member chassis passive module is getting rebooted when performing "racadm racreset" in lead chassis

**Description**    Standby management system modules on the Member chassis are rebooted after "racadm racreset" operation is performed on Lead chassis.

**Workaround**

- If the system is already in failed state, a user can change the timezone to something other than GMT from Lead MSM GUI/Standalone which propagates the new timezone to all the Members in the group. Else, irrespective of MCM or Standalone setup, before performing "racadm racresetcfg", set the time zone to GMT.
- If the setup is already in MCM group, remove the member chassis from the group and change the timezone as stated above before performing the "racadm racresetcfg".

**Systems affected**    All systems supported in this release

**Tracking number**    195686

# Limitations

1. OME−Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. A blinking cursor is not displayed in the text fields when going to the console for the first time owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.
14. For slot-based template deployment, the previous and current virtual identity MAC address values that are displayed on the **Results for Deploy and Configuration Check** page are the same.
15. 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.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX750c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I/O Modules

- PowerEdge MX 25Gb Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch

## Supported web browsers

- Google Chrome version 90
- Google Chrome version 91
- Mozilla Firefox version 88

- Mozilla Firefox version 89
- Microsoft EDGE 90
- Microsoft EDGE 91
- Microsoft Internet Explorer 11

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.30.00 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.30.00

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.30.10 for PowerEdge MX7000 Chassis User's Guide* available at https://www.dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- CVE-2017-15906, CVE-2018-15919, CVE-2018-15473: Security scan may report these CVEs on OME-Modular. These are false positives as, OME–Modular disables the Secure Copy Protocol (SCP) by default. The SFTP and lockout policies are in place to avoid brute force attack.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell Technologies recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell Technologies recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that the vulnerability scanners, relating to the default self-signed web server certificate, and default SNMP community name, produce.

(i) **NOTE:** Dell Technologies recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.30.10 for PowerEdge MX Chassis User's Guide*.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

## Template deployment

● If you deploy a template on servers with PERC controllers in HBA mode, then the profile deployment may fail. Check the iDRAC Lifecycle Controller logs for the error details.

# OpenManage Enterprise Modular 1.20.10

## Resolved issues

### Reclaim identities task

Fixed an issue that was causing the reclaim identities or detach profile task to fail, when the associated identity pool did not have enough identities to reserve.

**Tracking number**

168225

### Duplicate or missing devices

Fixed an issue that was causing duplicate or missing devices in the list of devices that was fetched using the API, `/api/DeviceService/Devices`.

**Tracking number**

169223

## Known issues

### Deployment and Configuration Job created multiple times for some sleds during Quick Deploy and Attach operation for sleds

| | |
|---|---|
| **Description** | In MCM Setup, the "Deployment and Configuration" job is created multiple times for some sleds during **Quick Deploy** and **Attach** operation. Jobs fail due to the duplicate deployment. |
| **Workaround** | Ignore the failed deployment jobs. The duplicate jobs do not result in any issue. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 141623 |

### Error while assigning identities

| | |
|---|---|
| **Description** | While assigning identities on the **Template Deployment** > **Reserve Identities Error** page, you may get the errors, "Error assigning Identities" and "An application request timed out. Please contact your support representative if the issue persists." The errors are displayed when many devices are selected or the system is busy to process all selected devices before the OME-Modular Web interface timeout occurs. |
| | The number of devices which can be processed varies based on several factors including the contents of the server configuration templates, configured pools, number of identities, and types of identities. |
| **Workaround** | Select fewer devices for deployment or try again later when the system is not busy. |
| **Systems affected** | The OME-Modular console during server file deployment. |

**Tracking number**     142004

## Advanced Filter option not working in Audit Logs

**Description**          On the **Audit Logs** page, the **Advanced Filter** does not work when you enter search text containing special characters such as accented vowel.

**Workaround**        Use filter search on other parts of the text which do not use UTF-8 characters.

**Systems affected**    All systems supported in this release

**Tracking number**     154213

## Disabled NPAR NIC partitions enabled and listed in iDRAC and operating system after template deployment

**Description**          A reference template, containing configuration changes for BIOS, NIC, and iDRAC was deployed on compute sleds in the chassis. The NIC configuration is N-PAR enabled. The first NIC partition is enabled, the second partition is enabled with FCoE, while the third and fourth partitions are disabled for A and B Fabric. After the template is deployed, the third and fourth NIC partitions must be disabled. But, all partitions are NIC enabled.

**Workaround**       
- Redeploy the template that has virtualization mode and NIC partition changes.
- Create two jobs—one for changing the virtualization mode and the other for changing NIC partitions. After the virtualization mode is complete, initiate a job for NIC partition changes.

**Systems affected**    All systems supported in this release

**Tracking number**     166566

## Job created for all targets instead of filtered or selected targets

**Description**          Performing a device action on specific devices across multiple pages while filtering devices on a chassis, ignores the chassis filter. Instead, the device action targets all devices across all the pages.

**Workaround**        Alternate filters can be used when performing a device action. Chassis filters can be used, but only for devices on that page, not across all pages.

**Systems affected**    All systems supported in this release

**Tracking number**     174294

## Storage devices reported as unknown even though catalog contains storage firmware

**Description**          For storage devices on member chassis, the device compliance status is reported as "Unknown".

**Workaround**        Trigger the inventory of the storage sled manually and rerun the compliance task.

**Systems affected**    All systems supported in this release

**Tracking number**     174410

# Limitations

1. OME—Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.

2. A blinking cursor is not displayed in the text fields when going to the console for the first time. This is owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.

3. The 'up' and 'down' buttons in a numeric input field, when using Firefox on Windows Server 2012, are not displayed correctly. The issue exists from Firefox version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.

5. If the text has no spaces or punctuation, the HTML titles containing long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge. This is the default behavior of IE and Microsoft Edge.

6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.

8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.

9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.

10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace the hardware. Physically reseat the Chassis Direct USB connection.

11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.

12. Alert policy configurations are deleted after downgrading OME-Modular firmware. Configure the alert policies after OME-Modular firmware downgrade is completed.

13. The **HTTPS Test connection** feature does not work. Ignore the test connection error message, and download the Catalog using valid credentials.

14. CIFS path names beginning with back slash (\), are not supported despite the OME-Modular share validation being successful.

# Environment and system requirements

## Supported systems

### Chassis

● Dell PowerEdge MX7000

### Sleds

● Dell PowerEdge MX740c
● Dell PowerEdge MX840c
● Dell PowerEdge MX5016s

### I/O Modules

● PowerEdge MX 25Gb Ethernet Pass-Through Module

- PowerEdge MX 10GBASE-T Ethernet Pass-Through Module
- PowerEdge MX5000s SAS Switch
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX7116n Fabric Expander Module
- Dell EMC MX5108n Ethernet Switch
- Dell EMC MXG610s Fibre Channel Switch

## Supported web browsers

- Google Chrome version 83
- Google Chrome version 84
- Mozilla Firefox version 77
- Mozilla Firefox version 78
- Microsoft EDGE 83
- Microsoft EDGE 84
- Microsoft Internet Explorer 11
- Safari version 12
- Safari version 13

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.20.10 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.20.10

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.20.10 for PowerEdge MX7000 Chassis User's Guide* available at dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME−Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME−Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

ⓘ **NOTE:** Dell EMC recommends changing the default password for OME–Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.20.10 for PowerEdge MX Chassis User's Guide*.

ⓘ **NOTE:** You can update up to six IOMs simultaneously. However, the OME-Modular web interface displays a recommendation message to update only four IOMs simultaneously to ensure network stability.

## Upgrading or downgrading OME-Modular

Clear the browser cache before or after upgrading or downgrading OME-Modular.

# OpenManage Enterprise Modular 1.20.00

## Resolved issues

### Firmware rollback for compute device components on member chassis

Fixed an issue that was causing failure of firmware rollback for member chassis compute device components, when the rollback source was the MCM group lead.

**Tracking number**

136224

### Blank service tags for IOMs

Fixed an issue that was causing OME-Modular to display blank service tags for IOMs after a `'reset all', racadm racresetcfg` operation.

**Tracking number**

142890

### Logging in to OME-Modular web interface after factory reset

Fixed an issue that was not allowing users to log in to OME-Modular web interface after the following tasks were performed on a Management Module (MM):

1. Downgrading the MM firmware to 1.00.01 from 1.10.10 or 1.10.20.
2. Performing any factory reset such as `racreset, racresetcfg, FIPS_ON`, or `FIPS_OFF`.

**Tracking number**

143891

### Template deployment configuration job for sled

Fixed an issue that was the template deployment configuration job for sleds that are removed and reinserted after promotion of a backup lead.

**Tracking number**

145969

# HTTPS custom port in OME-Modular

Fixed an issue that was causing the automatic redirection to HTTPS custom port to fail after updating the OME-Modular firmware.

**Tracking number**

146489

# Network IOM inventory

Fixed an issue that was causing OME-Modular to take about 30 minutes to fetch inventory data when a new network IOM was inserted into a chassis and the inventory was not refreshed.

**Tracking number**

146808

# Member chassis storage sled inventory for all drives

Fixed an issue that was causing the member chassis storage sled inventory for all drives to be displayed as **Encryption Capable** in the lead chassis, though the drives did not support encryption.

**Tracking number**

147384

# Identity pool options in Edit Network view and during deployment

Fixed an issue that was causing identity pool options to not display when the name of a template or NIC teaming was changed after restoring the configuration to a new lead. The identity pool options were not displayed in the **Edit Network** view and during deployment.

**Tracking number**

147605

# Sub system health and inventory calls for compute sleds

Fixed an issue that was causing the calls for sub system health and inventory for compute sleds on the member chassis, to fail from promoted lead.

**Tracking number**

154251

# Known issues

## Deployment and Configuration Job created multiple times for some sleds during Quick Deploy and Attach operation for sleds

| Description | In MCM Setup, the "Deployment and Configuration" job is created multiple times for some sleds during **Quick Deploy** and **Attach** operation. Jobs fail due to the duplicate deployment. |
|---|---|
| Workaround | Ignore the failed deployment jobs. The duplicate jobs do not result in any issue. |

| **Systems affected** | All systems supported in this release |
|---|---|
| **Tracking number** | 141623 |

# Error while assigning identities

| **Description** | While assigning identities on the **Template Deployment** > **Reserve Identities Error** page, you may get the errors, "Error assigning Identities" and "An application request timed out. Please contact your support representative if the issue persists." The errors are displayed when many devices are selected or the system is busy to process all selected devices before the OME-Modular Web interface timeout occurs. |
|---|---|
| | The number of devices which can be processed varies based on several factors including the contents of the server configuration templates, configured pools, number of identities, and types of identities. |
| **Workaround** | Select fewer devices for deployment or try again later when the system is not busy. |
| **Systems affected** | The OME-Modular console during server file deployment. |
| **Tracking number** | 142004 |

# Advanced Filter option not working in Audit Logs

| **Description** | On the **Audit Logs** page, the **Advanced Filter** does not work when you enter search text containing special characters such as accented vowel. |
|---|---|
| **Workaround** | Use filter search on other parts of the text which do not use UTF-8 characters. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 154213 |

# Disabled NPAR NIC partitions enabled and listed in iDRAC and operating system after template deployment

| **Description** | A reference template, containing configuration changes for BIOS, NIC, and iDRAC was deployed on compute sleds in the chassis. The NIC configuration is N-PAR enabled. The first NIC partition is enabled, the second partition is enabled with FCoE, while the third and fourth partitions are disabled for A and B Fabric. After the template is deployed, the third and fourth NIC partitions must be disabled. But, all partitions are NIC enabled. |
|---|---|
| **Workaround** | ● Redeploy the template that has virtualization mode and NIC partition changes. |
| | ● Create two jobs—one for changing the virtualization mode and the other for changing NIC partitions. After the virtualization mode is complete, initiate a job for NIC partition changes. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 166566 |

# Reclaim identities task fails

| **Description** | If the associated identity pool does not have enough identities to reserve, the **Reclaim Identities** or **Detach Profile** task fails. |
|---|---|
| **Workaround** | Generate template, which can be referred to during the reclaim identities task as part of the deployment. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 168225 |

# Devices duplicated or missing in list fetched using /api/DeviceService/Devices

| | |
|---|---|
| **Description** | Some devices are duplicated while some others are missing in the list of devices that is fetched by using the API, `/api/DeviceService/Devices`. The devices are picked from the database, randomly. |
| **Workaround** | Use the "Order By" filter to sort the list that is based on service tag or identifier of the device. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 169223 |

# Error encountered in member chassis after downgrading to OME-Modular version 1.10.20

| | |
|---|---|
| **Description** | An error is encountered in the member chassis when the OME-Modular version in the member chassis is downgraded to 1.10.20 from 1.20.00 |
| **Workaround** | Clear the browser cache before and after upgrading or downgrading firmware. |
| **Systems affected** | All systems supported in this release. |
| **Tracking number** | 168228 |

# Operating system display menu and iDRAC screen cropped when chassis is connected to 17 or 19-inch monitors

| | |
|---|---|
| **Description** | When the system is set to legacy BIOS mode, the initial BIOS boot screen that is rendered with resolution 720x400@70Hz is distorted. The distortion is due to a mismatch in aspect ratio in lower-end monitors of 17 or 19 inches. |
| **Workaround** | Set the system to UEFI mode for the BIOS screens to display correctly. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 169777 |

# Limitations

1. OME–Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When going to the console for the first time, a blinking cursor is not displayed in the text fields. This is owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. The issue exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace he hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware to 1.00.01 from 1.10.00. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. The **HTTPS Test connection** feature does not work. Ignore the test connection error message, and download the Catalog using valid credentials.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I-O Modules

- PowerEdge MX 25Gb — Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
- PowerEdge MX5000s — SAS Switch
- Dell EMC MX9116n — Fabric Switching Engine
- Dell EMC MX7116n — Fabric Expander Module
- Dell EMC MX5108n — Ethernet Switch
- Dell EMC MXG610s — Fibre Channel Switch

## Supported web browsers

- Google Chrome version 82
- Google Chrome version 83
- Mozilla Firefox version 75
- Mozilla Firefox version 76
- Microsoft EDGE 43
- Microsoft EDGE 44
- Microsoft Internet Explorer 11
- Safari version 12
- Safari version 13

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.20.00 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.20.00

## Downloading OME-Modular firmware

To download the latest OME−Modular firmware:

1. Go to dell.com/support.
2. Click **Browse all products**.
   The **All products** window is displayed.
3. Click **Servers**.
   The **All products / Servers** window is displayed.
4. Click **PowerEdge**.
   The **All products / Servers / PowerEdge** window is displayed.
5. Click **Modular Infrastructure**.
   The **All products / Servers / PowerEdge / Modular Infrastructure** window is displayed.
6. Click **PowerEdge MX7000**.
   The **PowerEdge MX7000** page is displayed.
7. Click **DRIVERS & DOWNLOADS** to download the required component.

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.20 for PowerEdge MX7000 Chassis User's Guide* available at dell.com/openmanagemanuals.

# Important Notes

## Keywords

From OME-Modular version 1.30, references to the following keywords shall be deprecated:

- MSM, LEX, Lexington, EC, Enclosure Controller, Poleg, CMC, Pathfinder, Sojourner, Senna, Insight, Galileo
- Weaver, Spinner, HE Switch, LE Switch, WeaverSwitch, HE, LE, DNV
- HEIOM, HE-IOM, HE_IOM, HE IOM, LEIOM, LE-IOM, LE_IOM, LE IOM
- FCIOM, FC-IOM, FC_IOM, FC IOM, Starlynx, Skylynx

## Security

OpenVAS vulnerability scanner may report the following issues:

- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME−Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME−Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

## Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

ⓘ **NOTE:** Dell EMC recommends changing the default password for OME—Modular.

## Ethernet Switch firmware update

For instructions about updating network IOMs, see the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.20.00 for PowerEdge MX Chassis User's Guide*.

A firmware update for passthrough and MX7116n modules is staged for deployment on the next power cycle or virtual reseat of the module.

# OpenManage Enterprise Modular 1.10.20

## Resolved issues

### Fibre Channel Mezz card components not visible in exported profile while deploying virtual identities

Fixed an issue that prevented users from viewing Fibre Channel Mezz card components in the exported profile while deploying virtual identities.

**Tracking Number**

145643

### MIB file formatted incorrectly

Fixed an issue that was causing incorrect formatting of MIB files.

**Tracking Number**

155088

### Management module reboots unexpectedly

Fixed memory leak and stability issues that were causing unexpected management module (MM) reboots.

**Tracking numbers**

157921 , 151134, 157943, 158722

### Standby MM resets to unexpected defaults after failover

Fixed an issue that was causing the standby management module to reset to default after a failover.

## Quick deployment jobs from lead chassis to member chassis compute sled fail

Fixed an issue that was causing failure of quick deploy jobs from lead chassis to member chassis compute sleds.

**Tracking Number**

157926

## Old password not retained after performing racresetcfg

Fixed an issue that was causing the nonretention of old password after performing racresetcfg.

## Inventory calls for compute sled returns error response

Fixed an issue that was causing inventory calls for compute sled to return error response 500.

**Tracking Number**

157259

# Known issues

## Template deployment configuration job not created for sled

| | |
|---|---|
| **Description** | Template deployment configuration job is not created for a sled that is removed and reinserted after the backup lead is promoted. The job is not created because profiles are attached to the occupied slots from the original lead. |
| **Workaround** | Detach and reattach the required profiles for the occupied slots after backup lead is promoted and before removing or reinserting the sleds. |
| **Systems affected** | iDRAC, PowerEdge MX740c, and PowerEge MX840c |
| **Tracking number** | 145969 |

## Service tag of IOM is reported incorrectly from OME-Modular after reset all

| | |
|---|---|
| **Description** | OME-Modular reports a blank service tag for the IOMs after a 'reset all', `racadm racresetcfg`, operation. |
| **Workaround** | Perform management module reset or failover. |
| **Systems affected** | All systems supported in this release. |
| **Tracking number** | 142890 |

# Multi-chassis firmware rollback fails with error

| | |
|---|---|
| **Description** | When you try firmware rollback for compute device components on the member chassis, with components rollback source as "Device", from the MCM group lead, a job is created on the member chassis and the job fails. |
| **Workaround** | You can roll back firmware with the source as "Device" directly on the respective member chassis. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 136224 |

# Deployment and Configuration Job created multiple times for some sleds during Quick Deploy and Attach operation for sleds

| | |
|---|---|
| **Description** | In MCM Setup, the "Deployment and Configuration" job is created multiple times for some sleds during **Quick Deploy** and **Attach** operation. Jobs fail due to the duplicate deployment. |
| **Workaround** | Ignore the failed deployment jobs. The duplicate jobs do not result in any issue. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 141623 |

# Error while assigning identities

| | |
|---|---|
| **Description** | While assigning identities on the **Template Deployment** > **Reserve Identities Error** page, you may get the errors, "Error assigning Identities" and "An application request timed out. Please contact your support representative if the issue persists." The errors are displayed when many devices are selected or the system is busy to process all selected devices before the OME-Modular Web interface timeout occurs.<br><br>The number of devices which can be processed varies based on several factors including the contents of the server configuration templates, configured pools, number of identities, and types of identities. |
| **Workaround** | Select fewer devices for deployment or try again later when the system is not busy. |
| **Systems affected** | The OME-Modular console during server file deployment. |
| **Tracking number** | 142004 |

# Unable to log in to OME-Modular Web interface after performing factory reset

| | |
|---|---|
| **Description** | Users may be unable to log in to OME-Modular Web interface after performing the following operations on a 240 GB MM:<br>1. Downgrading the MM firmware to 1.00.01 from 1.10.10 or 1.10.20.<br>2. Performing any factory reset such as `racreset`, `racresetcfg`, `FIPS_ON`, or `FIPS_OFF`.<br>The chassis is in bad state despite the reset operation being successful. You may be unable to access the MM Web interface. The MM IP takes over an hour to come up in such cases. You can run the command, `racadm config -g cfglannetworking -o cfgDNSRegisterRac 0`, through serial to get the IP. |
| **Workaround** | Downgrading the OME-Modular firmware to 1.00.01 is not recommended. For systems that are in bad state, remove the MM from the chassis. Reinsert the management modules one after the other and run the command, `racresetcfg` in each module. |
| **Systems affected** | All systems supported in this release, with 240 GB MM when downgraded to 1.00.10. |
| **Tracking number** | 143891 |

# OME-Modular takes up to 30 minutes to fetch network IOM inventory

**Description**       When you insert a new network IOM into a chassis and do not refresh inventory, OME-Modular may take up to 30 minutes to fetch inventory data.

**Workaround**       Refresh inventory on the new IOM manually or wait until the next default inventory task is complete.

**Systems affected**   All systems supported in this release

**Tracking number**   146808

# Member chassis storage sleds inventory for all drives displayed as encryption capable in lead chassis

**Description**       Member chassis storage sled inventory for all drives is displayed as **Encryption Capable** in the lead chassis though the drives do not support encryption.

**Workaround**       In the MCM environment, you can get the correct **Encryption Capable** information directly from the member chassis.

**Systems affected**   No physical systems affected. Information may be displayed incorrectly for storage sleds installed on member chassis, from the lead chassis web interface.

**Tracking number**   147384

# HTTPS custom port in OME-Modular does not work after upgrading to 1.10.00 or later

**Description**       Automatic redirection to HTTPS custom port does not work after updating to the OME-Modular firmware.

**Workaround**       Enter the hostname and custom port, for example, 10.10.10.10:1234, manually in the address bar of the browser to access OME-Modular. Reconfiguring the custom port after the firmware update helps resolve the issue.

**Systems affected**   OME-Modular with customized HTTPS port that is updated to the OME-Modular 1.10.00 or later.

**Tracking number**   146489

# Identity pool options missing in Edit Network view and during deployment

**Description**       The identity pool options are not displayed when the name of a template or NIC teaming is changed after restoring configuration to a new lead after retiring the existing lead. The identity pool options are not displayed during deployment and in the **Edit Network** view. However, this does not affect deployed identities that are displayed on the **Identity Pools** page.

**Workaround**
- Clone the template and use the clone for all new device deployments.
- Delete the old template, if it is not deployed.
- If the old template is deployed, it works for the existing devices and can be retained.

**Systems affected**   All systems supported in this release.

**Tracking number**   147605

# Member chassis displays error message on promoted lead chassis

| | |
|---|---|
| **Description** | Sub system health and inventory calls for compute sled on the member chassis are failing from the promoted lead. |
| **Workaround** | Identify the member chassis where the compute sled is located and offboard the chassis. Then, perform the onboard task for the same chassis. |
| **Systems affected** | MX740c, MX840c |
| **Tracking number** | 154251 |

# Limitations

1. OME–Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When going to the console for the first time, a blinking cursor is not displayed in the text fields. This is owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. The issue exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.
7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace he hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs is displayed as 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware to 1.00.01 from 1.10.00. Configure the alert policies after OME-Modular firmware downgrade is completed.
13. The **HTTPS Test connection** feature does not work. Ignore the test connection error message, and download the Catalog using valid credentials.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I-O Modules

- PowerEdge MX 25Gb — Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
- PowerEdge MX5000s — SAS Switch
- Dell EMC MX9116n — Fabric Switching Engine
- Dell EMC MX7116n — Fabric Expander Module
- Dell EMC MX5108n — Ethernet Switch
- Dell EMC MXG610s — Fibre Channel Switch

## Supported web browsers

- Google Chrome version 75
- Google Chrome version 76
- Mozilla Firefox version 57
- Mozilla Firefox version 58
- Mozilla Firefox version 67
- Mozilla Firefox version 68
- Microsoft EDGE 43
- Microsoft EDGE 44
- Microsoft Internet Explorer 11
- Safari version 11
- Safari version 12

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.10.20 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration
- Updating MX7000 components using OME-Modular 1.10.20

## Downloading OME-Modular firmware

To download the latest OME–Modular firmware:

1. Go to dell.com/support.
2. Click **Browse all products**.
   The **All products** window is displayed.
3. Click **Servers**.
   The **All products / Servers** window is displayed.
4. Click **PowerEdge**.
   The **All products / Servers / PowerEdge** window is displayed.
5. Click **Modular Infrastructure**.
   The **All products / Servers / PowerEdge / Modular Infrastructure** window is displayed.
6. Click **PowerEdge MX7000**.
   The **PowerEdge MX7000** page is displayed.
7. Click **DRIVERS & DOWNLOADS** to download the required component.

## Updating firmware in OME-Modular

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.20 for PowerEdge MX7000 Chassis User's Guide* available at dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME−Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME−Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

> ⓘ **NOTE:** Dell EMC recommends changing the default password for OME - Modular.

## Support for untagged VLAN in FCoE

In SmartFabric mode, OS10 enables you to use any untagged VLAN for FCoE Ethernet uplinks and Ethernet server ports, which are part of the FCoE VLAN. The FCoE uplink identifies FIP Snooping bridge (FSB) mode at the switch. Configure the same untagged VLAN on the FCoE uplinks and server ports for the FCoE sessions to come up. In SmartFabric mode, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN. The FCoE VLAN can have one or many FC Gateway uplinks. The FC Gateway uplink identifies N-Port Proxy Gateway (NPG) mode at the switch. Also, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN, which has one or many FC Direct attach uplinks. The FC Direct attach uplink identifies F-Port mode at the switch.

## Restrictions

- SmartFabric mode does not support multiple FCoE uplinks from the same IOM.
- In FCoE mode, the untagged VLAN on the server port and the FCoE uplink must be the same. This condition ensures that the untagged FIP VLAN discovery packets in the L2 frame, switch to the untagged VLAN.
- You cannot configure multiple FCoE uplinks corresponding to different untagged VLANs.

## Networking switches updates

After upgrading all management modules to 1.10.10, upgrade the networking switches to OS10.5.0.1. You can find the switches at support.dell.com.

A firmware update for passthrough and MX7116n modules is staged for deployment on the next power cycle or virtual reseat of the module.

# OpenManage Enterprise Modular 1.10.10

## Resolved issues

### Network configuration attributes

Fixed an issue that caused failure in restoration of the network configuration attributes—**Network Auto Negotiation**, **Network Speed**, and **Duplex Mode** during the restore operation.

**Tracking number**

107884

### Check Compliance operation

Fixed an issue that was causing the **Check Compliance** operation to fail, for non-administrator users, and not display an error message.

**Tracking number**

108258

### Display of HWC2131 in Chassis Fault List

Fixed an issue that was causing the alert, `HWC2131`, to not display in the **Chassis Fault List** on the dashboard.

**Tracking number**

108458

### Chassis KVM output in compute sleds

Fixed an issue that was causing loss of chassis KVM output when the AC power was restored after an outage in compute sleds.

**Tracking number**

108499

# Display of ISL cabling diagram in Internet Explorer and Microsoft Edge

Fixed an issue that was causing improper display of the ISL cabling diagram , during fabric creation, in Internet Explorer and Microsoft Edge.

**Tracking number**

107300

# iDRAC on sled may lose communication with the management module and display HWC1228 after updating OME-Modular to 1.10.00

Fixed an issue that was causing iDRAC versions earlier than 3.36.36.36, to stop communicating with the management module and display the error, HWC1228—"iDRAC on the sled is not communicating with the management module", while updating OME-Modular to 1.10.00.

**Tracking number**

141576

# Firmware catalog

Fixed an issue that was causing automatic deletion of firmware catalog, if incorrect information was entered while creating the catalog.

**Tracking number**

106989

# iDRAC restore from lead chassis

Fixed an issue that was causing failure of the iDRAC restore operation from the lead chassis.

**Tracking number**

108114

# Chassis profile export

Fixed an issue that was causing the chassis profile export task, using the hostname or FQDN, to fail.

**Tracking number**

108459

# Request to join group using Microsoft Edge or Internet Explorer

Fixed an issue that was causing failure of requests to join group using Microsoft Edge or Internet Explorer.

**Tracking number**

107147

# Device display in member chassis

Fixed an issue that was causing devices to not display when they are moved from the lead chassis to member chassis in MCM environment.

**Tracking number**

108286

# Set proxy operation using hostname ending with numeric character

Fixed an issue that was causing failure of set proxy operation if the hostname ended with a numeric character.

**Tracking number**

109454

# iDRAC password with special characters

Fixed an issue that was causing the iDRAC password setting task, with special characters, to fail.

**Tracking number**

110940

# Descriptive error for compute sleds

Fixed an issue that was causing descriptive errors to not display when compute sleds are in lockdown mode and VLAN settings are changed.

**Tracking number**

112537

# Last run date for jobs

Fixed an issue that caused incorrect display of the last run date for some jobs after firmware update.

**Tracking number**

115338

# IOM or storage device updates

Fixed an issue that was causing updates of IOM or storage devices to not start, when IOM or storage devices are selected as chassis components while updating firmware baselines.

**Tracking number**

115635

# IOM firmware update

Fixed an issue that was causing failure of IOM firmware update when IOMs or storage devices are selected as part of the chassis component using the Compliance Report method.

**Tracking number**

115639

# Multiple firmware update jobs

Fixed an issue that caused multiple firmware update jobs to start when IOMs or storage devices are selected while updating the firmware from baselines.

**Tracking number**

115640

# OME-Modular web interface slows down while deploying compute sleds

Fixed an issue that caused the OME-Modular web interface to slow down when more than 150 compute sleds were deployed in a 20-chassis setup.

**Tracking number**

118264

# PowerEdge MX 10GbT Passthrough Module

Fixed an issue that caused the graphical representation of the PowerEdge MX 10GbT Passthrough Module to not display on the **Group Topology** page owing to errors in identifying the correct IOM image.

**Tracking number**

118761

# MCM lead chassis does not display alerts

Fixed an issue that caused the MCM lead chassis to not display alerts from chassis components.

**Tracking number**

117677

# Bandwidth settings on IOMs in fabric mode

Fixed an issue that caused failure of bandwidth settings deployment on IOMs in fabric mode when an imported template is used.

**Tracking number**

117251

# OME-M MCM Group Lead does not display network IOMs of member chassis

Fixed an issue that caused the MCM group lead in OME-Modular to not display the network IOMs of the member chassis.

**Tracking number**

151831

# Technical preview of Transparent Ethernet uplink using OME-Modular and SmartFabric operating system 10.5.0.3

Fixed an issue that was causing the configuration of Technical Preview of transparent Ethernet uplinks, using OME-Modular to fail.

**Tracking number**

150737

# Storage sled drive inventory details in lead chassis

Fixed an issue that was causing improper display of inventory details of storage sled drives in the lead chassis when:

- The storage sleds are present in the same slot on both the lead and member chassis.

- The storage sleds are moved from one slot to another slot in member chassis.

**Tracking number**

151625, 153362, 153485

# Retire lead operation

Fixed an issue that was causing the "Retire Lead operation" to fail owing to permission issues caused by Operating System internal services.

**Tracking Number**

150964

# OME-Modular inaccessible after updating to 1.10.00 on 172.17.0.1/16 subnet

Fixed an issue that was causing OME-Modular to be inaccessible after updating to 1.10.00 on 172.17.0.1/16 subnet.

**Tracking Number**

PSE-9062

# Limitations

1. OME–Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When going to the console for the first time, a blinking cursor is not displayed in the text fields. This is owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. The issue exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.

7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace he hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs refer to 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.

**12.** Alert policy configurations are deleted after downgrading OME-Modular firmware to 1.00.01 from 1.10.00. Configure the alert policies after OME-Modular firmware downgrade is completed.

# Environment and system requirements

## Supported systems

### Chassis

● Dell PowerEdge MX7000

### Sleds

● Dell PowerEdge MX740c
● Dell PowerEdge MX840c
● Dell PowerEdge MX5016s

### I-O Modules

● PowerEdge MX 25Gb — Ethernet Pass-Through Module
● PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
● PowerEdge MX5000s — SAS Switch
● Dell EMC MX9116n — Fabric Switching Engine
● Dell EMC MX7116n — Fabric Expander Module
● Dell EMC MX5108n — Ethernet Switch
● Dell EMC MXG610s — Fibre Channel Switch

## Supported web browsers

● Google Chrome version 75
● Google Chrome version 76
● Mozilla Firefox version 57
● Mozilla Firefox version 58
● Mozilla Firefox version 67
● Mozilla Firefox version 68
● Microsoft EDGE 43
● Microsoft EDGE 44
● Microsoft Internet Explorer 11
● Safari version 11
● Safari version 12

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.10.00 for PowerEdge MX Chassis User's Guide* for the following information:

● Prerequisites
● Hardware and software requirements
● Installation and configuration

# Downloading OME-Modular firmware

To download the latest OME–Modular firmware:
1. Go to dell.com/support.
2. Click **Browse all products**.
   The **All products** window is displayed.
3. Click **Servers**.
   The **All products / Servers** window is displayed.
4. Click **PowerEdge**.
   The **All products / Servers / PowerEdge** window is displayed.
5. Click **Modular Infrastructure**.
   The **All products / Servers / PowerEdge / Modular Infrastructure** window is displayed.
6. Click **PowerEdge MX7000**.
   The **PowerEdge MX7000** page is displayed.
7. Click **DRIVERS & DOWNLOADS** to download the required component.

# Updating firmware in OME-Modular

The update order for this release is as follows:
1. iDRAC 3.36.36.36 or the server bundle of all components on the compute sled
2. OME-Modular 1.10.00
3. Network IOMs to OS10.5.01

Dell recommends Catalog-based updates over Individual package method. The OME-Modular Web interface displays "Catalog" as the default option. You can update the firmware in OME–Modular using the following methods:
1. Individual package method—Through OME–Modular web interface or CLI (REST)
2. Catalog-based compliance method

   If you are using a catalog, you can select both iDRAC and OME-Modular as OME-Modular sequences the update.

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.00 for PowerEdge MX7000 Chassis User's Guide* available at dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:
- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME–Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME–Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

> (i) **NOTE:** Dell EMC recommends changing the default password for OME - Modular.

## Support for untagged VLAN in FCoE

In SmartFabric mode, OS10 enables you to use any untagged VLAN for FCoE Ethernet uplinks and Ethernet server ports, which are part of the FCoE VLAN. The FCoE uplink identifies FIP Snooping bridge (FSB) mode at the switch. Configure the same untagged VLAN on the FCoE uplinks and server ports for the FCoE sessions to come up. In SmartFabric mode, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN. The FCoE VLAN can have one or many FC Gateway uplinks. The FC Gateway uplink identifies N-Port Proxy Gateway (NPG) mode at the switch. Also, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN, which has one or many FC Direct attach uplinks. The FC Direct attach uplink identifies F-Port mode at the switch.

### Restrictions

- SmartFabric mode does not support multiple FCoE uplinks from the same IOM.
- In FCoE mode, the untagged VLAN on the server port and the FCoE uplink must be the same. This condition ensures that the untagged FIP VLAN discovery packets in the L2 frame, switch to the untagged VLAN.
- You cannot configure multiple FCoE uplinks corresponding to different untagged VLANs.

## Networking switches updates

After upgrading all management modules to 1.10.10, upgrade the networking switches to OS10.5.0.1. You can find the switches at support.dell.com.

A firmware update for passthrough and MX7116n modules is staged for deployment on the next power cycle or virtual reseat of the module.

# OpenManage Enterprise Modular 1.10.00

## Resolved issues

### Network configuration attributes

Fixed an issue that caused failure in restoration of the network configuration attributes—**Network Auto Negotiation**, **Network Speed**, and **Duplex Mode** during the restore operation.

**Tracking number**

107884

### Check Compliance operation

Fixed an issue that was causing the **Check Compliance** operation to fail, for non-administrator users, and not display an error message.

**Tracking number**

108258

### Display of HWC2131 in Chassis Fault List

Fixed an issue that was causing the alert, `HWC2131`, to not display in the **Chassis Fault List** on the dashboard.

**Tracking number**

108458

## Chassis KVM output in compute sleds

Fixed an issue that as causing loss of chassis KVM output when the AC power was restored after an outage in compute sleds.

**Tracking number**

108499

## Display of ISL cabling diagram in Internet Explorer and Microsoft Edge

Fixed an issue that was causing improper display of the ISL cabling diagram , during fabric creation, in Internet Explorer and Microsoft Edge.

**Tracking number**

107300

## iDRAC on sled may lose communication with the management module and display HWC1228 after updating OME-Modular to 1.10.00

Fixed an issue that was causing iDRAC versions earlier than 3.36.36.36, to stop communicating with the management module and display the error, HWC1228—"iDRAC on the sled is not communicating with the management module", while updating OME-Modular to 1.10.00.

**Tracking number**

141576

## Firmware catalog

Fixed an issue that was causing automatic deletion of firmware catalog, if incorrect information was entered while creating the catalog.

**Tracking number**

106989

## iDRAC restore from lead chassis

Fixed an issue that was causing failure of the iDRAC restore operation from the lead chassis.

**Tracking number**

108114

## Chassis profile export

Fixed an issue that was causing the chassis profile export task, using the hostname or FQDN, to fail.

**Tracking number**

108459

## Request to join group using Microsoft Edge or Internet Explorer

Fixed an issue that was causing failure of requests to join group using Microsoft Edge or Internet Explorer.

**Tracking number**

107147

# Device display in member chassis

Fixed an issue that was causing devices to not display when they are moved from the lead chassis to member chassis in MCM environment.

**Tracking number**

108286

# Set proxy operation using hostname ending with numeric character

Fixed an issue that was causing failure of set proxy operation if the hostname ended with a numeric character.

**Tracking number**

109454

# iDRAC password with special characters

Fixed an issue that was causing the iDRAC password setting task, with special characters, to fail.

**Tracking number**

110940

# Descriptive error for compute sleds

Fixed an issue that was causing descriptive errors to not display when compute sleds are in lockdown mode and VLAN settings are changed.

**Tracking number**

112537

# Last run date for jobs

Fixed an issue that caused incorrect display of the last run date for some jobs after firmware update.

**Tracking number**

115338

# IOM or storage device updates

Fixed an issue that was causing updates of IOM or storage devices to not start, when IOM or storage devices are selected as chassis components while updating firmware baselines.

**Tracking number**

115635

# IOM firmware update

Fixed an issue that was causing failure of IOM firmware update when IOMs or storage devices are selected as part of the chassis component using the Compliance Report method.

**Tracking number**

115639

# Multiple firmware update jobs

Fixed an issue that caused multiple firmware update jobs to start when IOMs or storage devices are selected while updating the firmware from baselines.

**Tracking number**

115640

# OME-Modular web interface slows down while deploying compute sleds

Fixed an issue that caused the OME-Modular web interface to slow down when more than 150 compute sleds were deployed in a 20-chassis setup.

**Tracking number**

118264

# PowerEdge MX 10GbT Passthrough Module

Fixed an issue that caused the graphical representation of the PowerEdge MX 10GbT Passthrough Module to not display on the **Group Topology** page owing to errors in identifying the correct IOM image.

**Tracking number**

118761

# MCM lead chassis does not display alerts

Fixed an issue that caused the MCM lead chassis to not display alerts from chassis components.>

**Tracking number**

117677

# Bandwidth settings on IOMs in fabric mode

Fixed an issue that cause failure of bandwidth settings deployment on IOMs in fabric mode when an imported template is used.

**Tracking number**

117251

# Known issues

## Template deployment configuration job not created for sled

| Description | Template deployment configuration job is not created for a sled that is removed and reinserted after the backup lead is promoted. The job is not created because profiles are attached to the occupied slots from the original lead. |
| --- | --- |
| Workaround | Detach and reattach the required profiles for the occupied slots after backup lead is promoted and before removing or reinserting the sleds. |
| Systems affected | iDRAC, PowerEdge MX740c, and PowerEge MX840c |
| Tracking number | 145969 |

# Service tag of IOM is reported incorrectly from OME-Modular after reset all

| | |
|---|---|
| **Description** | OME-Modular reports a blank service tag for the IOMs after a 'reset all', `racadm racresetcfg`, operation. |
| **Workaround** | Perform management module reset or failover. |
| **Systems affected** | All systems supported in this release. |
| **Tracking number** | 142890 |

# Multi-chassis firmware rollback fails with error

| | |
|---|---|
| **Description** | When you try firmware rollback for compute device components on the member chassis, with components rollback source as "Device", from the MCM group lead, a job is created on the member chassis and the job fails. |
| **Workaround** | You can roll back firmware with the source as "Device" directly on the respective member chassis. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 136224 |

# Deployment and Configuration Job created multiple times for some sleds during Quick Deploy and Attach operation for sleds

| | |
|---|---|
| **Description** | In MCM Setup, the "Deployment and Configuration" job is created multiple times for some sleds during **Quick Deploy** and **Attach** operation. Jobs fail due to the duplicate deployment. |
| **Workaround** | Ignore the failed deployment jobs. The duplicate jobs do not result in any issue. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 141623 |

# Error while assigning identities

| | |
|---|---|
| **Description** | While assigning identities on the **Template Deployment** > **Reserve Identities Error** page, you may get the errors, "Error assigning Identities" and "An application request timed out. Please contact your support representative if the issue persists." The errors are displayed when many devices are selected or the system is busy to process all selected devices before the OME-Modular Web interface timeout occurs. |
| | The number of devices which can be processed varies based on several factors including the contents of the server configuration templates, configured pools, number of identities, and types of identities. |
| **Workaround** | Select fewer devices for deployment or try again later when the system is not busy. |
| **Systems affected** | The OME-Modular console during server file deployment. |
| **Tracking number** | 142004 |

# Unable to log in to OME-Modular Web interface after performing factory reset

| | |
|---|---|
| **Description** | Users may be unable to log in to OME-Modular Web interface after performing the following operations on a 240 GB MM:<br>1. Downgrading the MM firmware to 1.00.01 from 1.10.10 or 1.10.20. |

**2.** Performing any factory reset such as `racreset`, `racresetcfg`, `FIPS_ON`, or `FIPS_OFF`.

The chassis is in bad state despite the reset operation being successful. You may be unable to access the MM Web interface. The MM IP takes over an hour to come up in such cases. You can run the command, `racadm config -g cfglannetworking -o cfgDNSRegisterRac 0`, through serial to get the IP.

| | |
|---|---|
| **Workaround** | Downgrading the OME-Modular firmware to 1.00.01 is not recommended. For systems that are in bad state, remove the MM from the chassis. Reinsert the management modules one after the other and run the command, `racresetcfg` in each module. |
| **Systems affected** | All systems supported in this release, with 240 GB MM when downgraded to 1.00.10. |
| **Tracking number** | 143891 |

## OME-Modular takes up to 30 minutes to fetch network IOM inventory

| | |
|---|---|
| **Description** | When you insert a new network IOM into a chassis and do not refresh inventory, OME-Modular may take up to 30 minutes to fetch inventory data. |
| **Workaround** | Refresh inventory on the new IOM manually or wait until the next default inventory task is complete. |
| **Systems affected** | All systems supported in this release |
| **Tracking number** | 146808 |

## Member chassis storage sleds inventory for all drives displayed as encryption capable in lead chassis

| | |
|---|---|
| **Description** | Member chassis storage sled inventory for all drives is displayed as **Encryption Capable** in the lead chassis though the drives do not support encryption. |
| **Workaround** | In the MCM environment, you can get the correct **Encryption Capable** information directly from the member chassis. |
| **Systems affected** | No physical systems affected. Information may be displayed incorrectly for storage sleds installed on member chassis, from the lead chassis web interface. |
| **Tracking number** | 147384 |

## HTTPS custom port in OME-Modular does not work after upgrading to 1.10.00 or later

| | |
|---|---|
| **Description** | Automatic redirection to HTTPS custom port does not work after updating to the OME-Modular firmware. |
| **Workaround** | Enter the hostname and custom port, for example, 10.10.10.10:1234, manually in the address bar of the browser to access OME-Modular. Reconfiguring the custom port after the firmware update helps resolve the issue. |
| **Systems affected** | OME-Modular with customized HTTPS port that is updated to the OME-Modular 1.10.00 or later. |
| **Tracking number** | 146489 |

## Identity pool options missing in Edit Network view and during deployment

| | |
|---|---|
| **Description** | The identity pool options are not displayed when the name of a template or NIC teaming is changed after restoring configuration to a new lead after retiring the existing lead. The identity pool options are |

not displayed during deployment and in the **Edit Network** view. However, this does not affect deployed identities that are displayed on the **Identity Pools** page.

| | |
|---|---|
| **Workaround** | <ul><li>Clone the template and use the clone for all new device deployments.</li><li>Delete the old template, if it is not deployed.</li><li>If the old template is deployed, it works for the existing devices and can be retained.</li></ul> |
| **Systems affected** | All systems supported in this release. |
| **Tracking number** | 147605 |

# Limitations

1. OME–Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When going to the console for the first time, a blinking cursor is not displayed in the text fields. This is owing to an issue in Chrome. For details and status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. The issue exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component that is used for certain selection inputs may not respond to arrow key presses. The issue is limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues that are related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not developing IE. For alternatives, see the list of approved and supported browser versions.
7. While uploading a DUP using Microsoft Edge, the upload progress bar always shows 0%.
8. The array, `ComponentComplianceReports`, is expanded by default. The navigation link is no longer in the payload.
9. Some OME-Modular web interface sessions are not terminated even after the web interface inactivity timeout value expires. The session works if the browser is in the foreground or if you close the browser and enables the session to expire. Browsers such as Chrome contain a flag that facilitates disabling the throttle. This enables the automatic logout to work irrespective of browser being in the background or foreground.
10. The Chassis Direct sessions through MacBook may result in display of the alerts. In such cases, do not replace he hardware. Physically reseat the Chassis Direct USB connection.
11. On the **Jobs** page, the last run date for some jobs refer to 1970. In such cases, do not replace hardware. OME-Modular reverts to the correct date and timestamp once the management module syncs with its time source.
12. Alert policy configurations are deleted after downgrading OME-Modular firmware to 1.00.01 from 1.10.00. Configure the alert policies after OME-Modular firmware downgrade is completed.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

## Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

## I-O Modules

- PowerEdge MX 25Gb — Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
- PowerEdge MX5000s — SAS Switch
- Dell EMC MX9116n — Fabric Switching Engine
- Dell EMC MX7116n — Fabric Expander Module
- Dell EMC MX5108n — Ethernet Switch
- Dell EMC MXG610s — Fibre Channel Switch

# Supported web browsers

- Google Chrome version 75
- Google Chrome version 76
- Mozilla Firefox version 57
- Mozilla Firefox version 58
- Mozilla Firefox version 67
- Mozilla Firefox version 68
- Microsoft EDGE 43
- Microsoft EDGE 44
- Microsoft Internet Explorer 11
- Safari version 11
- Safari version 12

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.10.00 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration

# Downloading OME-Modular firmware

To download the latest OME−Modular firmware:

1. Go to dell.com/support.
2. Click **Browse all products**.
   The **All products** window is displayed.
3. Click **Servers**.
   The **All products / Servers** window is displayed.
4. Click **PowerEdge**.
   The **All products / Servers / PowerEdge** window is displayed.
5. Click **Modular Infrastructure**.
   The **All products / Servers / PowerEdge / Modular Infrastructure** window is displayed.
6. Click **PowerEdge MX7000**.
   The **PowerEdge MX7000** page is displayed.
7. Click **DRIVERS & DOWNLOADS** to download the required component.

# Updating firmware in OME-Modular

The update order for this release is as follows:

1. iDRAC 3.36.36.36 or the server bundle of all components on the compute sled
2. OME-Modular 1.10.00
3. Network IOMs to OS10.5.01

Dell recommends Catalog-based updates over Individual package method. The OME-Modular Web interface displays "Catalog" as the default option. You can update the firmware in OME–Modular using the following methods:

1. Individual package method—Through OME–Modular web interface or CLI (REST)
2. Catalog-based compliance method

    If you are using a catalog, you can select both iDRAC and OME-Modular as OME-Modular sequences the update.

For steps to update firmware using the individual package or catalog, see the *Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.00 for PowerEdge MX7000 Chassis User's Guide* available at dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME–Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME–Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME-Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

> (i) **NOTE:** Dell EMC recommends changing the default password for OME - Modular.

## Support for untagged VLAN in FCoE

In SmartFabric mode, OS10 enables you to use any untagged VLAN for FCoE Ethernet uplinks and Ethernet server ports, which are part of the FCoE VLAN. The FCoE uplink identifies FIP Snooping bridge (FSB) mode at the switch. Configure the same untagged VLAN on the FCoE uplinks and server ports for the FCoE sessions to come up. In SmartFabric mode, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN. The FCoE VLAN can have one or many FC Gateway uplinks. The FC Gateway uplink identifies N-Port Proxy Gateway (NPG) mode at the switch. Also, you can assign any untagged VLAN to Ethernet server ports that belong to a FCoE VLAN, which has one or many FC Direct attach uplinks. The FC Direct attach uplink identifies F-Port mode at the switch.

### Restrictions

- SmartFabric mode does not support multiple FCoE uplinks from the same IOM.
- In FCoE mode, the untagged VLAN on the server port and the FCoE uplink must be the same. This condition ensures that the untagged FIP VLAN discovery packets in the L2 frame, switch to the untagged VLAN.

- You cannot configure multiple FCoE uplinks corresponding to different untagged VLANs.

## Networking switches updates

After upgrading all management modules to 1.10.00, upgrade the networking switches to OS10.5.0.1. You can find the switches at support.dell.com.

A firmware update for passthrough and MX7116n modules is staged for deployment on the next power cycle or virtual reseat of the module.

# OpenManage Enterprise Modular 1.00.10

## Resolved issues

### Bandwidth and port details

Corrected the bandwidth and port details for MX5108n and MX9116n IOMs displayed in the OME-Modular Help for **Fabrics Topology**.

**Tracking number**

102685

### Single Sign-On with CSR

Fixed an issue to facilitate working of OME-Modular to iDRAC Single Sign-On (SSO) with CSR-generated certificates.

**Tracking number**

106477

### Storage sled and storage IOM updates

Fixed an issue to enable update of storage sleds when scheduled with storage IOMs (PowerEdge MX5000s, Dell EMC MXG610s) as a single job during a compliance report-based update.

**Tracking number**

107979

### Root password application

Fixed an issue to apply the root password to compute sleds in slots when the deploy and configuration job is run.

**Tracking number**

108964

### FCoE virtual MAC addresses

Fixed an issue that was causing FCoE virtual MAC addresses to display improperly under certain conditions.

**Tracking number**

108238

# OME-Modular unresponsive

Fixed an issue that was causing OME-Modular to become unresponsive and display an error message.

**Tracking number**

107168

# HTTPS firmware catalog share

Fixed an issue that was displaying an error message while creating an HTTPS firmware catalog share.

**Tracking number**

103960

# Compute sled firmware updates in member chassis

Fixed an issue that was causing failure of firmware updates for compute sleds in a member chassis using the Dell Online Repository method.

**Tracking number**

108884

# Compute sled updates

Fixed an issue that was causing failure of updates to compute sleds in member chassis, using Validated Stack Repository method.

**Tracking number**

108947

# Failure of compute sled updates in MCM

Fixed an issue that was causing failure of updates of some compute sleds in MCM.

**Tracking number**

107401

# Firmware update job status

Fixed an issue that was causing the status of OME-Modular firmware update job to be displayed as "Completed" even when it failed.

**Tracking number**

110520

# Single management module connectivity

Fixed an issue that was causing single management module to lose connectivity when the external port link changed.

**Tracking number**

110421

# Known issues

## Unable to restore network configuration attributes

| | |
|---|---|
| **Description** | The restore operation does not restore the network configuration attributes—**Network Auto Negotiation**, **Network Speed**, and **Duplex Mode**. |
| **Workaround** | Log in to OME—Modular, go to **Chassis Settings** > **Network** and configure the network settings—**Network Auto Negotiation**, **Network Speed**, and **Duplex Mode**. |
| **Systems affected** | All system supported by this release. |
| **Tracking number** | 107884 |

## Fault list does not contain HWC2131

| | |
|---|---|
| **Description** | The hardware log contains the entry `HWC2131 "The Management Module cannot communicate with the right control panel because of internal issues"`. However, this error message is not displayed on the **Chassis Fault List** on the dashboard. This issue can occur during the management module firmware update. |
| **Workaround** | If the hardware log message HWC2131 was generated during a management module firmware update, ignore the message. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 108458 |

## Chassis KVM output may be lost after AC power outage in chassis

| | |
|---|---|
| **Description** | If the compute sleds have NVDIMMs and if AC power is lost while the NVDIMM is in read or write mode, the KVM output may not be restored when the AC power is restored. |
| **Workaround** | Reset the management module twice or perform failover on the management module twice using OME—Modular web interface or RACADM. To perform a reset using the OME—Modular web interface, go to **Home** > **Troubleshoot** > **Reset Management Module**. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 108499 |

## ISL Cabling Diagram not shown correctly in Microsoft Edge and Internet Explorer

| | |
|---|---|
| **Description** | During fabric creation, a diagram of the selected Fabric Design is displayed. The diagram indicates the type of IOMs used and ISL cabling between them. Internet Explorer and Edge do not display these diagrams correctly and may display black shapes instead of the correct ISL cabling. |
| **Workaround** | Use Chrome or Firefox. If you cannot use either of these browsers, the fabric creation workflow provides a printable summary of the defined fabric that you can use to view the image correctly. |
| **Systems affected** | MX9116n, MX7116n |
| **Tracking number** | 107300 |

# Unable to view details of template created from a reference device

**Description**    If you create a template using a reference device and that device is then removed from the chassis, you cannot view all the attributes captured in that template through the OME–Modular web interface. The template can still be deployed or used normally.

**Workaround**    To view the template attributes on the web interface, wait for the chassis inventory to be refreshed. The inventory is refreshed automatically every 30 minutes. You can also manually refresh the inventory using the OME–Modular web interface.

**Systems affected**    PowerEdge MX7000, PowerEdge MX740c, PowerEdge MX840c

**Tracking number**    107891

# Firmware catalog may be deleted automatically after editing

**Description**    If you enter incorrect information while editing a firmware catalog, the catalog may be deleted from OME–Modular.

**Workaround**    If you want to modify the catalog source or repository location, it is recommended that you create a catalog instead of editing the existing catalog. Editing the existing catalog is prone to errors.

**Systems affected**    PowerEdge MX7000

**Tracking number**    106989

# Error displayed when creating a local user account under certain conditions

**Description**    You may encounter the error, `Error - User could not be saved` when performing the following tasks:
1. Create a new local user account in OME–Modular.
2. Update the new user account name without changing the password.
3. Delete the user account.
4. Create a new local user account using the original account name.

**Workaround**    
1. Always update the user account password when modifying the user account name.
2. Run the `racadm racresetcfg` command to restore OME–Modular to factory defaults.
3. You can use the same username with different cases as user account names are case insensitive. For example: "test01" and "Test01"

**Systems affected**    PowerEdge MX7000

**Tracking number**    105270

# Cannot perform a graceful shut down of all compute sleds

**Description**    When using the option to select **Across all pages** on the **Compute Devices** grid, the **Power Off (Graceful)** option is not displayed.

**Workaround**    
- Select compute sleds individually and perform a graceful power off operation.
- Filter the **All Devices** page to view only compute sleds and then perform a power off operation.

**Systems affected**    PowerEdge MX740c, PowerEdge MX840c

**Tracking number**    108133

# Check Compliance operation fails to run and no error message is displayed

| | |
|---|---|
| **Description** | Even if a compliance report contains devices that you do not have permission to manage, the **Check Compliance** button is still enabled. When you click **Check Compliance**, no error message is displayed but the compliance report is not updated. |
| **Workaround** | Ensure that you have the permission to manage all devices contained within a compliance report before running a compliance check. |
| **Systems affected** | All systems supported by this release. |
| **Tracking number** | 108258 |

# Unable to deploy chassis profile after removing syslog or SNMP destinations

| | |
|---|---|
| **Description** | If you have administrator privileges and export a chassis profile and attempt to deploy the profile after removing the syslog or SNMP destination, the deployment fails. |
| **Workaround** | Do not delete any syslog or SNMP destinations manually from an exported chassis profile. Instead, let the destination entry be blank. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 104215 |

# Unable to edit firmware catalog in specific scenarios

| | |
|---|---|
| **Description** | When an existing firmware catalog is updated using **Configuration** > **Firmware** > **Catalog Management** > **Edit** to point to a catalog with incorrect repository credentials, OME–Modular does not refresh the catalog information. |
| **Workaround** | Remove the catalog and add a new one with the desired repository details. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 106990 |

# Unable to restore iDRAC from the lead chassis

| | |
|---|---|
| **Description** | The iDRAC restore operation performed from the lead chassis fails. |
| **Workaround** | Retry the restore operation to successfully restore the configuration and firmware. |
| **Systems affected** | All system supported by this release. |
| **Tracking number** | 108114 |

# Unable to export chassis profile using hostname or FQDN

| | |
|---|---|
| **Description** | When you export a profile using hostname or FQDN of the network share address, the export profile task fails with the message `Kindly provide valid input values. Check help for details..` |
| **Workaround** | Use the IP address of the share server instead of hostname or FQDN . |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 108459 |

# Request to join a group fails when using Microsoft Edge or Internet Explorer

| | |
|---|---|
| **Description** | If you use Microsoft Edge or Internet Explorer to initiate an action to join a multi-chassis group, the action may fail. OME−Modular loads portions of the application as they are needed. Environmental factors such as network disruption, web browser choice, and version, may disrupt that process. |
| **Workaround** | If the OME−Modular web interface is behaving unexpectedly, these troubleshooting steps address most issues:<br>● Refresh the web browser to reload the application.<br>● Verify network connection stability.<br>● Use Chrome or Firefox. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 107147 |

# Devices may not appear after being moved from the lead chassis to a member chassis

| | |
|---|---|
| **Description** | In a multi-chassis management (MCM), if you move a device from the lead chassis to one of the member chassis, the change may not be displayed immediately in the lead chassis inventory. This issue does not occur when moving a device between member chassis, or from a member chassis to the lead chassis. |
| **Workaround** | Wait for the scheduled automatic inventory refresh to complete. This refresh happens every 30 minutes. |
| **Systems affected** | All systems supported by this release. |
| **Tracking number** | 108286 |

# Set Proxy operation fails when using a hostname ending with a numeric character

| | |
|---|---|
| **Description** | While setting the proxy server, if the hostname ends with a numeric character, the proxy settings cannot be saved. For example, setting the proxy server to *hostname123* fails. |
| **Workaround** | Use either FQDN or IP address for the proxy server address. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 109454 |

# Using special characters while setting iDRAC password causes error

| | |
|---|---|
| **Description** | Using the special character, ^, while setting an iDRAC password from **Devices** > **Compute** > **View Details** > **Settings** > **Management** page, causes an error. |
| **Workaround** | Log in to the iDRAC console to set the iDRAC password. |
| **Systems affected** | PowerEdge MX740c, PowerEdge MX840c |
| **Tracking number** | 110940 |

# Descriptive error not displayed when compute sled is in lockdown mode and VLAN settings are changed

| | |
|---|---|
| **Description** | An error message is displayed when you try to change the VLAN setting on the **Chassis** > **Overview** > **Hardware** > **Chassis Slots** page when iDRAC is in lockdown mode. But, the error message does not describe the cause of the failure of the task. |
| **Workaround** | No action is required. A descriptive error message will be provided in a future update of OME - Modular. |
| **Systems affected** | PowerEdge MX840c, PowerEdge MX740c |
| **Tracking number** | 112537 |

# Last run date for some jobs may be displayed incorrectly after firmware update

| | |
|---|---|
| **Description** | After firmware update, some jobs may display the last run date as "1970". The issue is only seen when NTP servers are configured as the time source. After a firmware update, the public network takes some time to get established, which delays synchronizing the system time with the NTP server. Any jobs run before the system time synchronizes to the NTP server, display the year as 1970. |
| **Workaround** | The date and time are fixed automatically when the next job is run. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 115338 |

# Unable to start MM Update when IOMs or storage components are selected as chassis components while updating firmware from baselines

| | |
|---|---|
| **Description** | IOMs or storage device update does not start when IOMs/Storage devices are selected as chassis components while performing a Firmware Update from a baseline. |
| **Workaround** | Select the IOMs/Storage components as individual devices and retry the firmware update. |
| **Systems affected** | All Systems supported by this release. |
| **Tracking number** | 115635 |

# IOM firmware updates fail intermittently when IOMs are selected as part of chassis component while updating firmware from baselines

| | |
|---|---|
| **Description** | IOM updates can fail when IOMs or storage devices are selected as part of the chassis component using the Compliance Report Update method. |
| **Workaround** | Selecting the IOMs as individual devices and retry the firmware update. |
| **Systems affected** | All Systems supported by this release. |
| **Tracking number** | 115639 |

# Multiple Firmware Update jobs start for IOMs or storage devices when IOMs or storage devices are selected while updating firmware from baselines

| | |
|---|---|
| **Description** | Multiple firmware update jobs are started when IOMs or storage devices are selected while updating firmware from a baseline. |
| **Workaround** | When the firmware update fails, select the IOMs or storage device as individual devices and retry the firmware update. |
| **Systems affected** | All Systems supported by this release. |
| **Tracking number** | 115640 |

# OME - Modular slows down while deploying many compute sleds in 20 chassis setup

| | |
|---|---|
| **Description** | The OME - Modular web interface becomes slow while deploying more than 150 compute sleds in 20 chassis MCM setup. The sluggishness is due to high CPU consumption from data synchronization when an alert storm or multiple inventory refresh jobs occur. |
| **Workaround** | Once the synchronization ends, the system recovers automatically. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 118264 |

# PowerEdge MX 10GbT PTM is not displayed on chassis Group Topology page

| | |
|---|---|
| **Description** | On the Multi-chassis **Group Topology** page, the graphical representation of the PowerEdge MX 10GbT Passthrough Module is not displayed owing to errors in identifying the correct IOM image. |
| **Workaround** | There is no workaround for this issue. However, the MCM Topology is not impacted. |
| **Systems affected** | PowerEdge MX 10GbT Passthrough Module |
| **Tracking number** | 118761 |

# MCM Lead chassis does not display alerts from chassis components

| | |
|---|---|
| **Description** | If many actions or criteria are used in an alert policy, alerts may not be seen on the lead chassis. |
| **Workaround** | Refine the alert policy criteria and reduce the number of actions that are triggered on the lead chassis. |
| **Systems affected** | All systems supported by this release. |
| **Tracking number** | 117677 |

# Bandwidth settings are not deployed on IOMs in fabric mode when an imported template is used

| | |
|---|---|
| **Description** | When a template is exported from a chassis, it does not include the attributes which are needed for a switch to set bandwidth settings. Hence, when a template is imported into chassis B from chassis A, the switch bandwidth settings from chassis A are not replicated in chassis B. |
| **Workaround** | Reconfigure the network switch settings manually instead of using an imported template. |

**Systems affected**   All systems affected by this release

**Tracking number**   117251

# Alerts are not received through SYSLOG, SNMP, or EMAIL after downgrading OME-Modular firmware

**Description**      Alerts policy configurations are deleted after downgrading the OME-Modular firmware to 1.00.01 from 1.00.10.

**Workaround**      Configure the alert policies after the firmware downgrade is completed.

**Systems affected**   All PowerEdge MX7000 systems, with user-configured alerts policies, where OME-Modular firmware is downgraded to 1.00.01 from 1.00.10.

**Tracking number**   121423

# Limitations

1. OME−Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When navigating to the console for the first time, a blinking cursor does not appear in the text fields. This is owing to a bug in Chrome. For details and current status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. This bug exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.

4. An open-source component used for certain selection inputs may not respond to arrow key presses. This issue is currently limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not actively developing IE. For alternatives, refer to the list of approved and supported browser versions.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c

- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

## I-O Modules

- PowerEdge MX 25Gb — Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
- PowerEdge MX5000s — SAS Switch
- Dell EMC MX9116n — Fabric Switching Engine
- Dell EMC MX7116n — Fabric Expander Module
- Dell EMC MX5108n — Ethernet Switch
- Dell EMC MXG610s — Fibre Channel Switch

## Supported web browsers

- Google Chrome version 63
- Google Chrome version 64
- Mozilla Firefox version 57
- Mozilla Firefox version 58
- Microsoft EDGE
- Microsoft Internet Explorer 11
- Safari version 11

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.00.10 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration

# Downloading OME-Modular firmware

To download the latest OME−Modular firmware:
1. Go to dell.com/openmanagemanuals.
   The **Enterprise Systems Management** page is displayed.
2. Click **Dell OpenManage Enterprise**.
   The **Dell OpenManage Enterprise** page is displayed.
3. Click **Dell OpenManage Enterprise Modular Version 1.00.10 for Dell PowerEdge MX7000**.
   The **Support for Dell OpenManage Enterprise-Modular Version 1.00.10 for Dell PowerEdge MX7000** page is displayed.
4. On the left panel, click **Drivers & downloads**.

# Updating firmware in OME-Modular

You can update the firmware in OME−Modular using the following methods:

1. Individual package method—Through OME−Modular web interface or CLI (REST)
2. Catalog-based compliance method

For steps to update firmware using the individual package or catalog, see the *Dell OpenManage Enterprise-Modular for PowerEdge MX7000 Chassis User's Guide* available at https://www.dell.com/openmanagemanuals.

# Important Notes

## Security

OpenVAS vulnerability scanner may report the following issues:

- NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (OID: 1.3.6.1.4.1.25623.1.0.812051). This is a false positive based on the OpenSSH version that OME–Modular carries. No SFTP is exposed or supported.
- NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611). OME–Modular supports secure algorithms and upgrades SSH clients to the appropriate option. Configure your SSH client to autonegotiate the crypto algorithms used.

### Security best practices

- SNMP
  - Security scanners may identify SNMP. If you do not use SNMP in your deployment, you can disable SNMP.
  - If SNMP is required, Dell EMC recommends that the default community name is changed from `public`.
- By default, a self-signed certificate is generated to enable HTTPS communication. Dell EMC recommends generating a CSR and installing a valid non-self signed certificate.

Besides improving the security of OME - Modular, these actions eliminate warnings that are produced by vulnerability scanners relating to the default self-signed web server certificate and default SNMP community name.

> (i) **NOTE:** Dell EMC recommends changing the default password for OME - Modular.

### VLAN

When you configure non-default untagged or native VLAN for FCoE enabled interfaces, the configuration is accepted, but not applied to the hardware.

# OpenManage Enterprise Modular 1.00.01

## Resolved issues

Not applicable.

## Known issues

### Incorrect information for IOMs displayed in the Help for Fabrics Topology

| | |
|---|---|
| **Description** | The port details for MX5108n and MX9116n IOMs, and the bandwidth mentioned in the OME–Modular Help for **Fabric Topology** are incorrect. |
| **Workaround** | N/A |
| **Systems affected** | All systems supported by this release |
| **Tracking number** | 102685 |

# Unable to restore network configuration attributes

| | |
|---|---|
| **Description** | The restore operation does not restore the network configuration attributes—**Network Auto Negotiation**, **Network Speed**, and **Duplex Mode**. |
| **Workaround** | Log in to OME–Modular, go to **Chassis Settings** > **Network** and configure the network settings— **Network Auto Negotiation**, **Network Speed**, and **Duplex Mode**. |
| **Systems affected** | All system supported by this release. |
| **Tracking number** | 107884 |

# OME-Modular to iDRAC Single Sign-On may not work with CSR generated certificates

| | |
|---|---|
| **Description** | The iDRAC has a limit of 2810 bytes for SSO server certificates. If the CSR-based server certificate exceeds 2810 bytes, OME–Modular cannot configure iDRACs in the chassis for Single Sign-On (SSO). |
| **Workaround** | If CSR generated certificates exceeding 2810 bytes are required then, use non-SSO based mode to log in to iDRAC. |
| **Systems affected** | PowerEdge MX740c, PowerEdge MX840c |
| **Tracking number** | 106477 |

# Fault list does not contain HWC2131

| | |
|---|---|
| **Description** | The hardware log contains the entry `HWC2131 "The Management Module cannot communicate with the right control panel because of internal issues"`. However, this error message is not displayed on the **Chassis Fault List** on the dashboard. This issue can occur during the management module firmware update. |
| **Workaround** | If the hardware log message HWC2131 was generated during a management module firmware update, ignore the message. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 108458 |

# Unable to perform simultaneous firmware update of storage sleds and storage IOMs

| | |
|---|---|
| **Description** | Sometimes, during a compliance report based update, if the firmware update of storage sleds is scheduled with storage IOMs (PowerEdge MX5000s, MXG610s), the update fail. |
| **Workaround** | Schedule separate jobs for storage sleds and SAS IOMs. |
| **Systems affected** | PowerEdge MX5016s, PowerEdge MX5000s, MXG610s |
| **Tracking number** | 107979 |

# Chassis KVM output may be lost after AC power outage in chassis

| | |
|---|---|
| **Description** | If the compute sleds have NVDIMMs and if AC power is lost while the NVDIMM is in read or write mode, the KVM output may not be restored when the AC power is restored. |
| **Workaround** | Reset the management module twice or perform failover on the management module twice using OME– Modular web interface or RACADM. To perform a reset using the OME–Modular web interface, go to **Home** > **Troubleshoot** > **Reset Management Module**. |

| Systems affected | MX7000 |
|---|---|
| Tracking number | 108499 |

# Deployment and Configuration jobs fail with a root password update error

| Description | If a slot is configured with both Quick Deploy and a profile, and you insert a computer sled, the root password may not be applied. In such cases, the jobs fail with the following error: `Update root password failed to execute.` |
|---|---|
| Workaround | Reset the iDRAC root password manually from the OME–Modular **Quick Deploy** page or from the **Settings** page of the affected compute sled. |
| Systems affected | PowerEdge MX740c, PowerEdge MX840c |
| Tracking number | 108964 |

# ISL Cabling Diagram not shown correctly in Microsoft Edge and Internet Explorer

| Description | During fabric creation, a diagram of the selected Fabric Design is displayed. The diagram indicates the type of IOMs used and ISL cabling between them. Internet Explorer and Edge do not display these diagrams correctly and may display black shapes instead of the correct ISL cabling. |
|---|---|
| Workaround | Use Chrome or Firefox. If you cannot use either of these browsers, the fabric creation workflow provides a printable summary of the defined fabric that you can use to view the image correctly. |
| Systems affected | MX9116n, MX7116n |
| Tracking number | 107300 |

# Unable to view details of template created from a reference device

| Description | If you create a template using a reference device and that device is then removed from the chassis, you cannot view all the attributes captured in that template through the OME–Modular web interface. The template can still be deployed or used normally. |
|---|---|
| Workaround | To view the template attributes on the web interface, wait for the chassis inventory to be refreshed. The inventory is refreshed automatically every 30 minutes. You can also manually refresh the inventory using the OME–Modular web interface. |
| Systems affected | PowerEdge MX7000, PowerEdge MX740c, PowerEdge MX840c |
| Tracking number | 107891 |

# Incorrect FCoE virtual MAC address displayed

| Description | In certain scenarios, the FCoE virtual MAC address details may not be displayed correctly. |
|---|---|
| Workaround | When using the Identity Pools feature, follow these guidelines to prevent duplicate addresses from being deployed. When using template deployment to assign virtual identities to a system, ensure the following:<br>● If deploying a template to a sled, use the OME–Modular web interface to reassign the template to the slot before removing the sled from the chassis. On the details page of the sled, the option **Associate Profile to Slot** makes the necessary change.<br>● If the template is not reassigned to the sled, the virtual identities associated with the sled are made available for reuse immediately after the sled is removed.<br>● The chances of duplicate identities being assigned decreases as the size of the virtual address pool grows. A larger pool of identities reduces the chance of redeployment. |

**Systems affected**    PowerEdge MX7000

**Tracking number**    108238

# OME−Modular can become unresponsive and display an error message

**Description**    If the page is partially loaded and is stuck for 10 minutes or more, the message, `An application request timed out. Please contact your support representative if the issue persists.`, is displayed on the bottom right side of the page.

**Workaround**    Log out, and log in again.

**Systems affected**    PowerEdge MX7000

**Tracking number**    107168

# Firmware catalog may be deleted automatically after editing

**Description**    If you enter incorrect information while editing a firmware catalog, the catalog may be deleted from OME−Modular.

**Workaround**    If you want to modify the catalog source or repository location, it is recommended that you create a catalog instead of editing the existing catalog. Editing the existing catalog is prone to errors.

**Systems affected**    PowerEdge MX7000

**Tracking number**    106989

# Error displayed when creating a local user account under certain conditions

**Description**    You may encounter the error, `Error - User could not be saved` when performing the following tasks:
1. Create a new local user account in OME−Modular.
2. Update the new user account name without changing the password.
3. Delete the user account.
4. Create a new local user account using the original account name.

**Workaround**   
1. Always update the user account password when modifying the user account name.
2. Run the `racadm racresetcfg` command to restore OME−Modular to factory defaults.
3. You can use the same username with different cases as user account names are case insensitive. For example: "test01" and "Test01"

**Systems affected**    PowerEdge MX7000

**Tracking number**    105270

# Error may be displayed while creating an HTTPS firmware catalog share

**Description**    If you use an FQDN for the share address and select the**Certificate Check** option while creating an HTTPS firmware catalog, the error message, `Error occurred while retrieving certificate information`, is displayed.

**Workaround**    Use an IP Address instead of an FQDN. The **Certificate Check** passes, and the expected FQDN listed is displayed during the certificate check.

**Systems affected**    PowerEdge MX7000

**Tracking number**    103960

## Cannot perform a graceful shut down of all compute sleds

**Description**    When using the option to select **Across all pages** on the **Compute Devices** grid, the **Power Off (Graceful)** option is not displayed.

**Workaround**
- Select compute sleds individually and perform a graceful power off operation.
- Filter the **All Devices** page to view only compute sleds and then perform a power off operation.

**Systems affected**    PowerEdge MX740c, PowerEdge MX840c

**Tracking number**    108133

## Check Compliance operation fails to run and no error message is displayed

**Description**    Even if a compliance report contains devices that you do not have permission to manage, the **Check Compliance** button is still enabled. When you click **Check Compliance**, no error message is displayed but the compliance report is not updated.

**Workaround**    Ensure that you have the permission to manage all devices contained within a compliance report before running a compliance check.

**Systems affected**    All systems supported by this release.

**Tracking number**    108258

## Unable to deploy chassis profile after removing syslog or SNMP destinations

**Description**    If you have administrator privileges and export a chassis profile and attempt to deploy the profile after removing the syslog or SNMP destination, the deployment fails.

**Workaround**    Do not delete any syslog or SNMP destinations manually from an exported chassis profile. Instead, let the destination entry be blank.

**Systems affected**    PowerEdge MX7000

**Tracking number**    104215

## Unable to edit firmware catalog in specific scenarios

**Description**    When an existing firmware catalog is updated using **Configuration** > **Firmware** > **Catalog Management** > **Edit** to point to a catalog with incorrect repository credentials, OME−Modular does not refresh the catalog information.

**Workaround**    Remove the catalog and add a new one with the desired repository details.

**Systems affected**    PowerEdge MX7000

**Tracking number**    106990

## Unable to restore iDRAC from the lead chassis

**Description**    The iDRAC restore operation performed from the lead chassis fails.

**Workaround**    Retry the restore operation to successfully restore the configuration and firmware.

**Systems affected**    All system supported by this release.

**Tracking number**    108114

## Unable to export chassis profile using hostname or FQDN

**Description**    When you export a profile using hostname or FQDN of the network share address, the export profile task fails with the message `Kindly provide valid input values. Check help for details..`

**Workaround**    Use the IP address of the share server instead of hostname or FQDN .

**Systems affected**    MX7000

**Tracking number**    108459

## Request to join a group fails when using Microsoft Edge or Internet Explorer

**Description**    If you use Microsoft Edge or Internet Explorer to initiate an action to join a multi-chassis group, the action may fail. OME−Modular loads portions of the application as they are needed. Environmental factors such as network disruption, web browser choice, and version, may disrupt that process.

**Workaround**    If the OME−Modular web interface is behaving unexpectedly, these troubleshooting steps address most issues:
- Refresh the web browser to reload the application.
- Verify network connection stability.
- Use Chrome or Firefox.

**Systems affected**    PowerEdge MX7000

**Tracking number**    107147

## Firmware update for compute sleds in a member chassis fails when using the Dell online repository

**Description**    In a multi-chassis environment, if you use the Dell online repository, firmware update of compute sleds in member chassis fails.

**Workaround**    Use a single DUP update method from the lead chassis or perform the updates from the member chassis using a PDK catalog.

**Systems affected**    All systems supported by this release.

**Tracking number**    108884

## Firmware update for compute sleds in member chassis fails when using validated stack repository method

**Description**    In a multi-chassis environment, if you use a validated stack repository from the lead chassis, firmware update of compute sleds in member chassis failed.

**Workaround**    Use a single DUP update method from the lead chassis or perform the updates from the member chassis using a PDK catalog.

**Systems affected**    All systems supported by this release.

**Tracking number**    108947

# Devices may not appear after being moved from the lead chassis to a member chassis

**Description**  In a multi-chassis management (MCM), if you move a device from the lead chassis to one of the member chassis, the change may not be displayed immediately in the lead chassis inventory. This issue does not occur when moving a device between member chassis, or from a member chassis to the lead chassis.

**Workaround**  Wait for the scheduled automatic inventory refresh to complete. This refresh happens every 30 minutes.

**Systems affected**  All systems supported by this release.

**Tracking number**  108286

# Firmware update of compute sleds fails

**Description**  If you schedule a firmware update job for the compute sleds and the management module together, the firmware update for compute sleds may fail. In a multi-chassis scenario, the management module and sled firmware update actions run in parallel. The management module firmware update causes the management module to reboot, which causes the the sled firmware update to fail.

**Workaround**  Perform firmware update for management module and the compute sleds separately.

**Systems affected**  All systems supported by this release.

**Tracking number**  108123

# Set Proxy operation fails when using a hostname ending with a numeric character

**Description**  While setting the proxy server, if the hostname ends with a numeric character, the proxy settings cannot be saved. For example, setting the proxy server to *hostname123* fails.

**Workaround**  Use either FQDN or IP address for the proxy server address.

**Systems affected**  PowerEdge MX7000

**Tracking number**  109454

# Emails not sent as part of alert policy on FIPS enabled systems

**Description**  If SMTP settings are configured with SSL enabled on a FIPS-enabled system, mails are not sent as part of an alert policy.

**Workaround**  To receive emails, disable SSL for SMTP when FIPS mode is enabled.

**Systems affected**  PowerEdge MX7000

**Tracking number**  109796

# Deployment and configuration jobs not triggered for newly inserted servers

**Description**  When Quick Deploy is configured for all chassis slots, the Deployment and Configuration jobs are not triggered for newly-inserted servers.

**Workaround**  After inserting servers, manually refresh the inventory through the OME−Modular web interface (**Devices** > **Chassis** > **blue refresh icon**).

| | |
|---|---|
| **Systems affected** | PowerEdge MX7000, PowerEdge MX740c, PowerEdge MX840c |
| **Tracking number** | 109724 |

# Unable to migrate profile after detaching profile

| | |
|---|---|
| **Description** | After detaching a profile from a slot and attempting to migrate the profile to a different server, the following error message is displayed: `Unable to migrate profile because deployment in progress.` |
| **Workaround** | Select the **Edit Profile** option on the server where the profile is detached and save the profile settings. This detaches the profile from the server and makes it available for migration. |
| **Systems affected** | PowerEdge MX740c, PowerEdge MX840c |
| **Tracking number** | 109879 |

# Unable to log in to the chassis if the password contains certain special characters

| | |
|---|---|
| **Description** | When the user account password contains special characters such as "+?>-}|,[;]/=<:{I^~", you may be unable to log in using SSH, Serial, or KVM. You can log in using the web interface and remote RACADM. |
| **Workaround** | Do not use special characters in account passwords. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 110160 |

# Lead chassis displays incorrect OME–Modular version for member chassis in domain-related APIs

| | |
|---|---|
| **Description** | The lead chassis shows incorrect OME–Modular version for member chassis after upgrading the member chassis to the latest OME–Modular firmware using the following APIs:<br>● `/api/ManagementDomainService/Domains`<br>● `/api/ManagementDomainService/PendingDomains`<br>● `/api/ManagementDomainService/DiscoveredDomains` |
| **Workaround** | ● Remove and add member to the group again.<br>● Use the web interface to see the OME–Modular version on the member chassis. |
| **Systems affected** | PowerEdge MX7000 |
| **Tracking number** | 109587 |

# Firmware updates for compute sleds fail in multi-chassis environment

| | |
|---|---|
| **Description** | While updating compute sleds in MCM, the update sometimes fails for one of the compute sleds with the following message: `Internal Error Occurred.` |
| **Workaround** | Retry the updates on the failed compute sled. |
| **Systems affected** | All systems supported by this release. |
| **Tracking number** | 107401 |

# Firmware update job status displayed incorrectly

| | |
|---|---|
| **Description** | OME−Modular firmware update job status may be displayed as **Completed** though it failed. This issue affects only OME−Modular update. |
| **Workaround** | Retry the update. |
| **Systems affected** | All systems supported by this release |
| **Tracking number** | 110520 |

# Using special characters while setting iDRAC password causes error

| | |
|---|---|
| **Description** | Using the special character, ^, while setting an iDRAC password from **Devices** > **Compute** > **View Details** > **Settings** > **Management** page, causes an error. |
| **Workaround** | Log in to the iDRAC console to set the iDRAC password. |
| **Systems affected** | PowerEdge MX740c, PowerEdge MX840c |
| **Tracking number** | 110940 |

# Single MM chassis loses connectivity after external port link change

| | |
|---|---|
| **Description** | Single MM chassis that is connected to a switch, which does not emit LLDP, loses connectivity if the link state changes. |
| **Workaround** | 1. Enable LLDP on connected switch.<br>2. Install a second MM.<br>3. Reset through chassis KVM, serial port RACADM, or physically reseat the MM. |
| **Systems affected** | All systems supported by this release. |
| **Tracking number** | 110421 |

# Limitations

1. OME−Modular is supported only on TLS 1.2 and later. Versions earlier than 1.2 may or may not work. Also, support for earlier versions of TLS is not provided.
2. When navigating to the console for the first time, a blinking cursor does not appear in the text fields. This is owing to a bug in Chrome. For details and current status, see bugs.chromium.org/p/chromium/issues/detail?id=740652.
3. When using Firefox on Windows Server 2012, the 'up' and 'down' buttons in a numeric input field are not displayed correctly. This bug exists in Firefox since version 37. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=1158435.

   This issue also affects other versions of Firefox depending on the positioning of the numeric input. The numeric up and down buttons are not sized correctly when used in a data grid in MCSI. However, the manual input of values is not impacted. For details, see bugzilla.mozilla.org/show_bug.cgi?id=947365.
4. An open-source component used for certain selection inputs may not respond to arrow key presses. This issue is currently limited to the AD/LDAP import wizard. For details, see github.com/select2/select2/issues/3472.
5. The HTML titles that consist of long strings of text are truncated in Internet Explorer (IE) and Microsoft Edge, if the text has no spaces or punctuation. This is the default behavior of IE and Microsoft Edge.
6. Internet Explorer has performance issues related to DOM rendering and manipulation, both of which are widely used in a single-page application. For details, see developer.microsoft.com/en-us/microsoft-edge/platform/issues/7636678/.

   These issues result in poor performance in AngularJS and many other open-source UI components. For details, see github.com/angular-ui/ui-grid/issues/5855.

   Version upgrades or design changes may be explored in future releases, which may help reduce these performance issues in IE. However, the possibilities for improvement may be limited as Microsoft is not actively developing IE. For alternatives, refer to the list of approved and supported browser versions.

# Environment and system requirements

## Supported systems

### Chassis

- Dell PowerEdge MX7000

### Sleds

- Dell PowerEdge MX740c
- Dell PowerEdge MX840c
- Dell PowerEdge MX5016s

### I-O Modules

- PowerEdge MX 25Gb — Ethernet Pass-Through Module
- PowerEdge MX 10GBASE-T — Ethernet Pass-Through Module
- PowerEdge MX5000s — SAS Switch
- Dell EMC MX9116n — Fabric Switching Engine
- Dell EMC MX7116n — Fabric Expander Module
- Dell EMC MX5108n — Ethernet Switch
- Dell EMC MXG610s — Fibre Channel Switch

## Supported web browsers

- Google Chrome version 63
- Google Chrome version 64
- Mozilla Firefox version 57
- Mozilla Firefox version 58
- Microsoft EDGE
- Microsoft Internet Explorer 11
- Safari version 11

# Installation

See the *Dell EMC OpenManage Enterprise - Modular Edition Version 1.00.01 for PowerEdge MX Chassis User's Guide* for the following information:

- Prerequisites
- Hardware and software requirements
- Installation and configuration

# Downloading OME-Modular firmware

To download the latest OME−Modular firmware:
1. Go to dell.com/openmanagemanuals.
   The **Enterprise Systems Management** page is displayed.
2. Click **Dell OpenManage Enterprise**.
   The **Dell OpenManage Enterprise** page is displayed.
3. Click **Dell OpenManage Enterprise Modular Version 1.00.01 for Dell PowerEdge MX7000**.

The **Support for Dell OpenManage Enterprise-Modular Version 1.00.01 for Dell PowerEdge MX7000** page is displayed.

4. On the left panel, click **Drivers & downloads**.

# Updating firmware in OME-Modular

You can update the firmware in OME–ModularOME Modular using the following methods:

1. Individual package method—Through OME–Modular web interface or CLI (REST)
2. Catalog-based compliance method

To update the firmware using the Individual package method:

1. Download the DUP from the dell.com/support/drivers.
2. On the OME–Modular web interface, navigate **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 navigate 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. Select the required components, for example: OME Modular, and click **Update** to start the firmware update.
7. Navigate to the **Monitor** > **Jobs** page to view the job status.

   (i) **NOTE:** The console is inaccessible during and after the OME–Modular update process.

# Catalog-based compliance method

To update the firmware using the catalog-based method:

1. Download the DUP from the dell.com/support/drivers.
2. Use the Dell Repository Manager (Repository Manager) to create the `catalog.xml` file.
3. Place the `catalog.xml` that you created using Repository Manager, in a shared location.
4. Navigate to the **Configuration Firmware** page to create the catalog and baseline.
5. On the OME–Modular web interface, navigate to the **Devices** > **Chassis** page.
6. Click the **Update Firmware**.
   The **Select Firmware Source** window is displayed.
7. Select the **Baseline** option and select the required baseline from the drop-down.
8. Select the OME–Modular component from the comparison report.
   The supported components are displayed.
9. Select the required components, for example: OME–Modular, and click **Update** to start the firmware update.
10. Navigate to the **Monitor** > **Jobs** page to view the job status.

    (i) **NOTE:** Click **Configuration** > **Firmware** > **Catalog Management** > **Add** to download the catalog from the dell.com/support.

    For more information, see the Dell EMC OpenManage Enterprise-Modular Edition Version 1.00.01 for PowerEdge MX Chassis User's Guide, available at dell.com/openmanagemanuals.

# Resources and support

For more information about the features of this release, see the documentation for OpenManage Enterprise Modular (OME-Modular) available at https://www.dell.com/openmanagemanuals.

# Latest Release Notes

To access the latest Release Notes for this version:

1. Go to https://www.dell.com/openmanagemanuals.
2. Click **Dell OpenManage Enterprise**.
3. Click **Dell OpenManage Enterprise-Modular**.
4. Click **Documentation** and scroll down to the **Manuals and Documents** section to view the Release Notes.

# Accessing documents using direct links

You can directly access the documents using the following links:

**Table 2. Direct links for documents**

| URL | Product |
|---|---|
| https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/ | PowerEdge MX Networking Whitepapers and videos |
| https://www.dell.com/openmanagemanuals | OpenManage Enterprise Management |
| https://www.dell.com/idracmanuals | iDRAC and Lifecycle Controller |
| https://www.dell.com/serviceabilitytools | Serviceability Tools |
| https://www.dell.com/omconnectionsclient | Client System Management |
| https://www.dell.com/esmmanuals | OpenManage Connections Enterprise Systems Management |

# Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to **https://www.dell.com/support**.
2. Click **Browse all products**.
3. Click the desired product category, such as Servers, Software, Storage, and so on.
4. Click the desired product.
   > (i) **NOTE:** For some products, you may have to go through the subcategories.
5. Click **Documentation** and scroll down to the **Manuals and Documents** section.

# Contacting Dell

> (i) **NOTE:** If you do not have an active Internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country or region and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues, see https://www.dell.com/contactdell.

## 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.**