

Dell EMC OpenManage Enterprise-Modular Edition Version 1.10.20 for PowerEdge MX7000 Chassis

Release Notes

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2018 -2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

1 Release summary.....	5
2 Compatibility.....	6
Supported systems.....	6
Supported web browsers.....	6
3 New and enhanced features.....	7
4 Fixes.....	8
Fibre Channel Mezz card components not visible in exported profile while deploying virtual identities.....	8
MIB file formatted incorrectly.....	8
Management module reboots unexpectedly.....	8
Standby MM resets to unexpected defaults after failover.....	8
Quick deployment jobs from lead chassis to member chassis compute sled fail.....	8
Old password not retained after performing racresetcfg.....	8
Inventory calls for compute sled returns error response.....	9
5 Important Notes.....	10
Security.....	10
Support for untagged VLAN in FCoE.....	10
Networking switches updates.....	10
6 Known issues.....	11
Template deployment configuration job not created for sled.....	11
Service tag of IOM is reported incorrectly from OME-Modular after reset all.....	11
Multi-chassis firmware rollback fails with error.....	11
Deployment and Configuration Job created multiple times for some sleds during Quick Deploy and Attach operation for sleds.....	11
Error while assigning identities.....	12
Unable to log in to OME-Modular Web interface after performing factory reset.....	12
OME-Modular takes up to 30 minutes to fetch network IOM inventory.....	12
Member chassis storage sleds inventory for all drives displayed as encryption capable in lead chassis.....	12
HTTPS custom port in OME-Modular does not work after upgrading to 1.10.00 or later.....	13
Identity pool options missing in Edit Network view and during deployment.....	13
Member chassis displays error message on promoted lead chassis.....	13
7 Limitations.....	14
8 Installation.....	15
Downloading OME-Modular firmware.....	15
Updating firmware in OME-Modular.....	15
9 Resources and support.....	16

10 Contacting Dell EMC.....17

Release summary

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

Version

1.10.20

Release date

February 2020

Priority and recommendations

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

Compatibility

Supported 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

New and enhanced features

- Added an option to enter filename during chassis backup.
- Added an option to selectively force iDRAC reset from the OME-Modular web interface.
- Support for updating MX7000 components using the OME-Modular web interface.

Fixes

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.

Tracking Number

157922

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

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 reset of the module.

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 PowerEdge 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', <code>racadm racresetcfg</code> , 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: <ol style="list-style-type: none">1. Downgrading the MM firmware to 1.00.01 from 1.10.10 or 1.10.20.2. Performing any factory reset such as <code>racreset</code>, <code>racresetcfg</code>, <code>FIPS_ON</code>, or <code>FIPS_OFF</code>. 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, <code>racadm config -g cfglannetworking -o cfgDNSRegisterRac 0</code> , 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, <code>racresetcfg</code> 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 style="list-style-type: none"> • 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/angular.js/issues/12563 and 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 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.

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

Topics:

- [Downloading OME-Modular firmware](#)
- [Updating firmware in OME-Modular](#)

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.

Resources and support

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

Latest Release Notes

To access the latest Release Notes for this version:

1. Go to www.dell.com/openmanagemanuals.
2. Click **Dell OpenManage Enterprise**.
3. Click the link for this version of OME-Modular.
4. Click **DOCUMENTATION**.

Accessing documents using direct links


You can directly access the documents using the following links:

Table 1. Direct links for documents


URL	Product
www.dell.com/openmanagemanuals	OpenManage Enterprise Management
www.dell.com/idracmanuals	iDRAC and Lifecycle Controller
https://www.dell.com/serviceabilitytools	Serviceability Tools
www.dell.com/omconnectionsclient	Client System Management
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, and then click the desired version if applicable.
 **NOTE: For some products, you may need to go through the subcategories.**
5. Click **DOCUMENTATION**.

Contacting Dell EMC

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

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