Dell EMC OpenManage Enterprise Version 3.2.1

Release Notes

Dell EMC OpenManage Enterprise Version 3.2.1 Release Notes

This document describes the new features, enhancements, and known issues in Dell EMC OpenManage Enterprise version 3.2.1

Release type and definition

Dell EMC OpenManage Enterprise

OpenManage Enterprise is a systems management and monitoring application that provides a comprehensive view of the Dell EMC servers, chassis, storage, and network switches on the enterprise network. With OpenManage Enterprise, a web-based and one-to-many systems management application, you can:

- Discover and manage devices in a data center environment.
- Create and manage OpenManage Enterprise users.
- Group and manage devices.
- Monitor the health of your devices.
- Manage device firmware versions, and perform system updates and remote tasks.
- Create and deploy device configuration templates.
- Create and assign identity pools, and perform stateless deployment on target devices.
- Create configuration compliance baselines and remediate devices.
- View and manage system alerts and alert policies.
- View hardware inventory and compliance reports.
- Monitor and report about warranty and licenses.

Version

3.2.1

Release date

August 2019

Previous version

3.2

Importance

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

For the latest updates to the release notes, see Delltechcenter.com/OMEnt.

Platforms affected

For a complete list of affected Dell EMC systems and supported operating systems, see the *Dell EMC OpenManage Enterprise Version 3.2 Support Matrix* at Delltechcenter.com/OMEnt or Dell.com/OpenManageManuals.

What is supported

For a complete list of supported devices, operating systems, and web browsers, see the *Dell EMC OpenManage Enterprise Version 3.2 Support Matrix* at Delltechcenter.com/OMEnt or Dell.com/OpenManageManuals.

New in this release

- Support for additional extensions (plug-ins) such as the Power Manager extension to enhance the functionality of the appliance.
- Discovery and monitoring of PowerVault MD3, PowerVault ME4 devices
- In-band discovery of Windows servers and hypervisors using the OpenSSH protocol
- Support for the latest versions of KVM, ESXi, and Hyper-V
- Support for deployment of IOA template

- Programmatic appliance deployment for VMware ESXi (OVF form factor only) version 6.5 or later
- Faster login with AD accounts
- Support for Autodeployment: Ability to designate an existing template to configure servers and chassis that are yet to be discovered
- Onboarding servers and MX7000 chassis enables both alert reception and sets the community string
- Support for multiple device management URLs (if available)
- Option to support firmware catalog updates automatically or manually
- Availability of the Test Connection option in firmware catalog wizards where external share details are required
- Ability to configure the appliance's session inactivity logout
- Option to hide the previously acknowledged alerts in the console using the alert display settings
- Enhancements:
    - Reduced upgrade process time as the user can login without waiting for the completion of the background refresh discover task.
    - Improved error messages for all features and functions, to help troubleshoot failure and error conditions
    - Improved filter functionality for better sorting of records on various grids
    - Select-all works across pages for grids with the Across all pages checkbox
    - Ability to edit chassis templates
    - Ability to track users who acknowledge alerts
    - Custom report builder enhanced to better handle field selections, reordering, and display
    - Enhanced remote script execution to run up to 100 individual RACADM/IPMI, or SSH commands in a batch
    - Improvements to Warranty - settings are uniformly reflected in home widget, warranty report, and scoreboard
    - Ability to schedule automatic updating of the firmware catalogs
    - Firmware compliance report shows only components that have updates in critical or warning status
    - Improved robustness and scaling for firmware updates
    - Firmware update improvements to included mitigation options
    - Descriptive error messages on SMB versions misalignment
    - The appliance tracks user-acknowledged alerts enabling a better filtering of the alert log

Limitations

- You can select a maximum of 25 devices per page to perform operations such as refresh inventory, refresh status, and add devices to groups on the All Devices page. [98194]
- The appliance fails to identify locally shared folders if the folder names have spaces in them. For example, the appliance fails to retrieve files from an offline NFS source folder named D____K (with 4 spaces between 'D' and 'K'). This happens as the appliance ignores the spaces and interprets the name as DK. [115310]
- Export of large firmware compliance reports, containing more than 200,000 elements, fails and the appliance displays the **Application timeout** error.

Fixed issues

Table 1. Issues fixed in this release

Issue Reference	Summary
135343	Fixed the issue to retrieve warranty information of managed devices when the appliance is configured using authenticated proxy settings.
130453	Fixed the issue with setting up push notification for OpenManage Mobile where an error message "Hostname can't be null - Code 1002" would appear.
141847	Fixed the upgrade to 3.2.1 from any supported upgrade path when the user had a pre-canned template cloned in 1.0.
139446	Fixed the issue with Intel XXV710 based NICs not being listed in the Device Firmware Compliance Page.
141224	Fixed the issue with DNS names not being displayed for chassis on the All Devices page.
142237	Fixed the issue with the Firmware Compliance report not listing components that have Component ID as 0 or Null.

Known issues

Discovery and inventory

Issue 1

Description: The management IP on the **Device Details** page of the discovered VxRail devices does not match the management IP displayed on the **All Devices** page. [91653]

Issue 2

Description: If the onboarding state of the lead chassis and member chassis in an MCM group is in monitored state, the inventory task might fail if the MCM group is configured with more than 10 chassis. [108962]

Issue 3

Description: The exported inventory file lists values for component status and URL of the chassis is not listed. [108056]

Issue 4

Description: Servers that are reconfigured as VxRAIL do not automatically group under HCI upon refreshing the inventory. [116913]

Resolution: After a server is reconfigured as a VxRAIL, rediscover the device in the Discovery page. After rediscovery, the device is correctly grouped under HCI.

Issue 5

Description: The All Devices page shows **health status** of the discovered 11G servers with iDRAC firmware version 1.98 or later as **unknown**.

Issue 6

Description: The iDRAC virtual console management launch point is unavailable in the All Devices page for sleds with a 'Proxied' onboarding state.

Resolution: Ensure the sleds are in a 'Managed' state.

Issue 7

Description: For the discovered PowerVault MD3 series storage arrays, the complete model numbers are not displayed by the appliance in the All Devices page. For these devices, the model numbers as returned from the SNMP walk are displayed.[119881]

Issue 8

Description: In order to support discovery with domain credentials, OpenManage Enterprise 3.2 and later uses SSH instead of WSMAN. Hence, All the Windows and Hyper-V devices discovered prior to updating the appliance have to be deleted and re-discovered using their SSH credentials.

Issue 9

Description: While creating sever discovery jobs with the **Host OS** option in the **Create Discovery Job** wizard, the check box **Discover using SSH (Linux)** in the Additional Settings dialog box is misleading and should be interpreted instead as **Discover using SSH (Linux, Windows, and Hyper-V)**.

Tasks

Issue 1

Description: After upgrading to the latest version of OpenManage Enterprise, the existing job IDs are changed. [108055]

Firmware updates

Issue 1

Description: The **Update Firmware** button remains enabled even when there are no firmware catalogs available for upgrade or downgrade. [108218]

Issue 2

Description: The firmware rollback on PowerEdge MX7000 is not supported. Also, rollback on sleds is not supported when the onboarding state of the sleds is Proxied.[116172]

Issue 3

Description: A job for firmware rollback on PowerEdge MX7000 sleds, though allowed in the appliance, would fail. This happens due to the fact that the firmware rollback is not supported on MX Series sleds discovered as part of MX7000 chassis discovery or in proxied state. [136820]

Configuration management

Issue 1

Description: The Reclaim Identities and Profile Migration features are not supported for Emulex OneConnect Cards. [98511]

Issue 2

Description: If the MX7000 chassis is in the 'monitored' state during stateless deployment, the deployment job fails because the user does not have necessary privileges. Only the server configuration profile is imported. However, this information is not displayed in the Task Execution section. [108484]

Issue 3

Description: The changed VLAN name and IDs are not updated on the target MX7000 chassis after a stateless deployment task is run. [105156]

Issue 4

Description: If the IP setting is not configured on the discovered PowerEdge MX740C and PowerEdge MX840C, the Boot to Network ISO operation is not run during the template deployment. [102887]

Issue 5

Description: After deploying an MX7000 chassis template, you cannot log in to the MX7000 chassis with LDAP credentials. [107230]

Resolution: Manually update the LDAP bind password to log in.

Issue 6

Description: The deployment task of an MX7000 chassis fails if proxy authentication in enabled in the configuration template with error: 'Unable to complete the request because the input value for Password is missing or an invalid value is entered'. [108779]

Issue 7

Description: The directory service details in an MX7000 chassis are overwritten after the device configuration template is deployed.

Issue 8

Description: After a chassis is removed from the MCM group, you must rediscover the lead and member chassis to create and deploy a configuration template.

Issue 9

Description: The **Migration Profile** task fails if the user is not configured on the target device with the error: 'User Name is not configured '. [107376]

Issue 10

Description: If the IP configuration of a discovered device is changed during template deployment (from DHCP to Static or vice versa), the Boot to Network ISO operation fails. This happens as the appliance is unable to ping the target post template deployment.[113576]

Issue 11

Description: Unable to set Target iSCSI IQN on BIOS-iSCSI via reference server template deployment, as it fails with `Invalid AttributeValue` error. The default iSCSI Target IQN format of the iSCSI controllers of devices such as PowerVault ME4012 array and Equallogic PS array, is not accepted as a valid IQN format for deployment with IDRAC version 3.34.34.34. [132601]

Resolution: Select 'BIOS' attributes only for deployment.

Issue 12

Description: Creation of a chassis template from a reference M1000e chassis which has Firmware versions 6.10 or later fails if SMBv1 is disabled in the appliance. [129049]

Resolution: Enable SMBv1 in the appliance using **Application Settings** > **Console preferences** > **SMB settings** to create chassis templates from M1000e chassis with firmware versions 6.10 or later.

Issue 13

Description: Template Deployment with iDRAC Management IP option "Set static IP for each device" fails with error message "connection lost" with IPV6 IP (Legacy(3.1)). It works with IPV4.

Issue 14

Description: Template Deployment with iDRAC Management IP option "Set as DHCP" fails, and the task has to be tracked from iDRAC for final status.

Others

Issue 1

Description: Clicking **Check Update** on OpenManage Enterprise version 3.2, where PowerManager extension is not installed, an error **CGEN1003**- Unable to complete the operation because an empty payload is not allowed for this request is displayed.

Resolution: This error can be ignored as it is for information purpose only. There is no functional impact of this error and the user can go ahead with the upgrade.

Issue 2

Description: OpenManage Enterprise could be impacted by the Linux TCP SACK vulnerability (CVE-2019-11477).

Resolution: OMEnterprise 3.2.1 includes CentOS kernel patches for the TCP SACK Panic issues and carries the updated kernel-3.10.0-957.21.3.el7.x86_64.rpm including fixes for the CVE-2019-11477 vulnerability.

Issue 3

Description: A query group with switch and device power state together is not working as expected. [86481]

Resolution: Exclude switch power state while creating a query group.

Issue 4

Description: The management IP is incorrectly indicated if the server is discovered by using both the IPv4 and IPv6 addresses. [86196]

Resolution: Manually start the iDRAC Graphical User Interface (GUI).

Issue 5

Description: The target IP address is incorrectly listed in the task history of an alert policy that is created by running a remote script. [86424]

Resolution: N/A

Issue 6

Description: Not all scheduled jobs are displayed in the Recent Tasks list. [86488]

Resolution: Go to the Jobs page to view the latest and complete list of jobs.

Issue 7

Description: Discovery operation fails by using IPMI commands on the CISCO server if a KG key is used. [78545]

Resolution: KG key is not supported for this device discovery.

Issue 8

Description: When a device is turned off, the console takes a few moments to display the updated health status. [86146]

Resolution: Refresh the browser, or wait for a few moments.

Issue 9

Description: An individual Chassis Management Controller (CMC) health may not be correctly displayed in the device drill-down operation. [85977]

Resolution: Always consider the CMC rollup health status.

Issue 10

Description: Certain SNMP alerts are undefined for the S4810 networking switch. [85016]

Resolution: N/A

Issue 11

Description: An unknown Error message occasionally displayed in the SNMP alert console. [84894]

Resolution: Ignore or click **Dismiss**.

Issue 12

Description: In the SNMP alert console, some alerts from OMSA correctly show the Message ID field, while others show N/A. [83579]

Resolution: N/A

Issue 13

Description: Discovery of an HP server by using IPMI command may not reflect the correct rollup health status. [85153]

Resolution: View the lower-level sensor health data.

Issue 14

Description: In the **Execution Details** section, data must be manually sorted in the table every time after moving to a new page. [81207]

Resolution: Sort information of a single page at a time.

Issue 15

Description: Currently, the health status including PSU and temperature data is not displayed for the storage devices. [99821]

Resolution: N/A

Issue 16

Description: : The rollback features is not supported on the MX7000 chassis. Also, the rollback operation fails on the M1000e, FX2, and FX2s chassis. [110239]

Resolution: For M1000e, FX2, and FX2s chassis, create and associate a new baseline with the necessary firmware version to roll back.

Issue 17

Description: Currently, the alerts are not received by OpenManage Enterprise if the alerts are associated with the devices' IP address. However, alerts are successfully received when associated with the device Service Tag. [106369]

Issue 18

Description: Invalid host names are displayed under the **Source Name** column and are also available for selection in some of the OpenManage Enterprise tasks. [68214]

Issue 19

Description: Authentication by one-way and two-way trusts of AD users is not supported by the appliance.

Issue 20

Description: From the **All Devices** page, you cannot launch the iDRAC application interface with IPv6 addresses. [102153]

Issue 21

Description: When PCIe cards are mapped to the FX2/FX2s chassis, migration of identities is not supported on the sleds in the same FX2s chassis since the FQDDs differ.

Issue 22

Description: Console Upgrade from 3.0 through NFS Share fails. Also, console Upgrade through HTTPS (internal Share) fails when upgrading from versions 3.0 and 3.1. [114683]

Resolution: Use the online method for updating, or use the HTTPS method. Ensure that the security certificates are signed by a trusted third-party certificate authority while using the HTTPS method of update.

Issue 23

Description: The selected target devices or device groups while creating an alert policy in OpenManage Enterprise-Tech Release are cleared when the appliance is updated. [115698]

Resolution: After updating the appliance, edit the alert policy and select the target devices or device groups to receive the group-specific alerts.

Issue 24

Description: After you update the appliance from OpenManage Enterprise-Tech Release, the Syslog server messages do not retain the standard format of `<timestamp><hostname>_<Alert_Message>`. The alerts are displayed as `"EEMI@123_[id]":Alert_Message.` [115699]

Issue 25

Description: Few alerts from the PowerEdge R240, R340, T140, T340, and R740xd2 servers are received with unknown severity in the OpenManage Enterprise appliance. [112404]

Issue 26

Description: While programmatically deploying the OpenManage Enterprise from Linux shell, if the argument provided for --*name=* in the command line begins with a "**$**" then the argument is ignored and appliance is deployed with the name OPENMANAGE ENTERPRISE. [121158]

Resolution: The --*name=* argument, which begins with "**$**" in the command line must be enclosed in single quotes, for example, --*name=* **'$OME-VM'**.

Issue 27

Description: The Severity status in the Alert log for the alerts received from the PowerVault ME4 storage arrays is being reported as **Unknown** by the appliance. This defect is due to the unavailability of the precanned MIBs for the PowerVault ME4 storage arrays in the appliance console. [122657]

Issue 28

Description: After the console is upgraded, there is a delay of approximately 15 minutes in the initiation of the **Post Upgrade** task by the appliance. [130142]

Issue 29

Description: When an already imported MIB is renamed and parsed through API the trap status is reported as 'Existing' instead of 'Imported.'[111854]

Issue 30

Description: Ignore alert policy created for warranty, firmware compliance, configuration compliance alert will be ignored only if alert is generated from the same device from which ignore policy was created. In other cases, alert will be received and not ignored. [124596]

Issue 31

Description: SSH Private key can be applied while adding a remote script in the Script Execution page. [129366]

Issue 32

Description: The **Schedule** advanced filter in the **Monitor > Discovery** page incorrectly displays even those discovery jobs which have completed their initial scheduled run. [128842]

Issue 33

Description: In order to leverage performance improvements made in the Active Directory login, users have to delete and re-import the user groups in OpenManage Enterprise version 3.2.

Issue 34

Description: The .CSV files, that record the deleted alerts from the Alert log, fail to capture the **Device Name** and the **Device IP** details of the alerts received from the undiscovered devices.[132915]

Issue 35

Description: Export of large firmware compliance reports, containing more than 200,000 elements, fails and the appliance displays an **Application timeout** error. [133201]

Resolution: When exporting large firmware compliance reports, the following workarounds can be employed :

- Allocate more memory to the appliance while installing.
- Before exporting large reports, ensure that other jobs are not running.
- Use the Firmware Compliance per Component or the Firmware Compliance per Device Report instead of exporting.
- Use filters to derive a smaller result set before exporting.

Issue 36

Description: A "Connection to server failed" error is displayed by the failed Power Action Tasks. Power Action tasks fail when they encounter servers where no power state change is required. This error message, though misleading, does not mean that the appliance is unable to establish contact with the server. [136816]

Issue 37

Description: Expect a delay while deleting a large number of devices by selecting the "Across all pages" option. This delay in completion of the job is due to the deboarding of the already onboarded devices by the appliance before their deletion. [136847]

Issue 38

Description: With this release, context-sensitive help on Power Manager plugins is currently not available. [136300]

Issue 39

Description: The **Monitor** > **Jobs** > **View Detail Execution History** page incorrectly displays **Could not set alert destination on the target** under **Messages**, even for the successfully-completed jobs created for setting of trap destinations for the MX7000 chassis.

Issue 40

Description: Deleting a device from the **All Devices** page would fail if there are active jobs involving the device.

Resolution: Before deleting a device from the **All Devices** page, ensure there are no jobs in the 'running' status involving the device.

Installation

Dell EMC OpenManage Enterprise is provided as an appliance that you can deploy on a hypervisor and manage resources to minimize downtime. The virtual appliance can be configured from the application web console after initial network provisioning in the Text User Interface (TUI). For steps to view and update the console version, see the *Dell EMC OpenManage Enterprise User's Guide* on the support site.

ⓘ **NOTE: For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.**

Installation prerequisites and minimum requirements

For a list of supported platforms, operating systems, and browsers, see the *Dell EMC OpenManage Enterprise Version 3.2 Support Matrix* on the support site and Dell TechCenter.

To install OpenManage Enterprise, you must have the local system administrator rights and the system you are using must meet the criteria. See the *Dell EMC OpenManage Enterprise User's Guide* on the support site and Dell TechCenter.

Recommended minimum hardware configuration for OpenManage Enterprise version 3.2.1:

Table 2. Minimum recommended hardware

Minimum recommended hardware	Large deployments	Small deployments
Number of devices that can be managed by the appliance	Up to 8000	1000
RAM	16 GB	16 GB
Processors	8 cores total	4 cores total
Hard drive	250 GB	50 GB

Minimum system requirements for deploying OpenManage Enterprise version 3.2.1

Table 3. Minimum system requirements

Particulars	Minimum requirements

Supported hypervisors	• VMware vSphere versions:
	  • vSphere ESXi 6.7
	  • vSphere ESXi 6.5
	  • vSphere ESXi 6.0
	  • vSphere ESXi 5.5
	• Microsoft Hyper-V supported on:
	  • Windows Server 2019
	  • Windows Server 2016
	  • Windows Server 2012 R2
	• KVM supported on:
	  • Red Hat Enterprise Linux 7.2
	  • Red Hat Enterprise Linux 7.0
	  • Red Hat Enterprise Linux 6.5

Particulars	Minimum requirements
Network	Available virtual NIC which has access to the management networks of all the devices which is managed from OpenManage Enterprise.
Supported browsers	• Internet Explorer (64-bit) 11 and later • Mozilla Firefox 52 and later • Google Chrome 58 and later
User interface	HTML 5, JS based

ⓘ **NOTE: For the latest update about the minimum system requirements for OpenManage Enterprise, see the *Dell EMC OpenManage Enterprise Support Matrix* on the support site.**

Contacting Dell

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

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

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