Dell EMC OpenManage Enterprise Version 3.7

Release Notes

July 2021
Rev. A00

Notes, cautions, and warnings

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

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

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

Contents

1

Topics:

Dell EMC OpenManage Enterprise Version 3.7 Release Notes

This document describes the new features, enhancements, known issues, and fixed issues in Dell EMC OpenManage Enterprise version 3.7.

Release type and definition

Dell EMC OpenManage Enterprise

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

- Discover devices in a data center environment.
- View hardware inventory and monitor health of devices.
- View and manage alerts received by the appliance and configure alert policies.
- Monitor firmware / driver versions and Manage firmware / driver updates on devices with firmware baselines.
- Manage remote tasks (such as power control) on devices.
- Manage configuration settings across devices using configuration templates.
- Manage virtual identity settings across devices using intelligent identity pools.
- Detect and remediate configuration deviations across devices using configuration baselines.
- Retrieve and monitor warranty information for devices.
- Group devices into static or dynamic groups.
- Create and manage OpenManage Enterprise users.

Version

3.7

Release date

July 2021

Previous version

3.6.1

Previous minimum version required

3.5

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 or may not apply to your environment.

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

What is supported

For a complete list of supported devices, operating systems, and web browsers, see the *Dell EMC OpenManage Enterprise Version 3.7 Support Matrix* at Delltechcenter.com/OMEnt or Dell.com/OpenManageManuals.

New in this release

- CloudIQ plugin support — Device group(s) can be selected to send data to CloudIQ for monitoring.

Enhancements

- Ability to view devices that have been disconnected due to Authentication failure from All-Devices page.
- Text User Interface (TUI) capabilities to selectively enable or disable debug logging for appliance and plugin services.

Limitations

- Only the OpenSSH is supported for the discovery and inventory collection of Windows-based servers and Hyper-Vs. Other SSH protocol implementations, like Cygwin SSH, are not supported. [157991]
- OpenManage Enterprise version 3.6.x is unable to fetch the offline upgrade availability on NFS share. [203403]
- Filtering does not work as expected when the following special characters are used in the naming of groups, alert policies, profiles, templates, and other instances: **,**, ****, **_**, **%**, **#**, **'**, **+**, **)**, and **&**. The permissible special characters are : **/**, **?**, **.**, **>**, **<**, **"**, **:**, **;**, **|**, **]**, **}**, **{**, **[**, **-**, **=**, **~**, **`**, **(**, **^**, *, **$**, **@**, **!** [162539]
- For the Japanese locale of OpenManage Enterprise, the date format displayed is in US 'short' date format instead of the Japanese format. [163343]
- The naming of reports only allows the following special characters: '**_**' and '**-**'. A report's name cannot have special characters such as **,**, ****, **%**, **#**, **'**, **+**, **)**, and **&**. For example, a report with the name "OME3.4**@**NIC**^**Report" is not allowed. [164776]
- 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.
- After installing or upgrading to OpenManage Enterprise version 3.3.1 on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance. [152723]
- Firmware catalog management using Dell.com or a local network path is limited to only the Enterprise Server catalog. Other catalogs such as ESXi_Catalog.xml.gz are not supported.[159958]
- RAID secure attributes are not supported on target devices during template or profile deployment. [157218]

Known issues

Scope Based Access Control (SBAC)

Issue 1: Ownership information for device managers (AD/LDAP and OIDC) is lost on appliance upgrade.

Description: Post upgrade of OpenManage Enterprise from version 3.5 or earlier versions, the AD/LDAP and OIDC (PingFederate or KeyCloak) device managers would need to recreate all the previous-version entities such as jobs, alert policies, configuration templates, configuration baselines, profiles, firmware baselines, firmware catalogs, and reports as these entities are only available to the administrators post upgrade. [193698]

Issue 2: Alert policies and firmware baselines created by a device manager in 3.5 or earlier versions are only available to administrator users.

Description: Post upgrade of OpenManage Enterprise from version 3.5 or earlier versions, the alert policies from the previous appliance versions such as version 3.4 and version 3.5 are only assigned to the administrator users. Hence, these entities created by device managers prior to the upgrade would need to be recreated. [194142]

Issue 3: After upgrade, device managers can perform VLAN operation on in-scope proxied MX7000 sleds even when the chassis is out of scope.

Description: VLAN operation on in-scope 'proxied' MX7000 sleds is allowed for a device manager, even if the MX7000 chassis is out of scope. [192774]

Resolution: As the operations for the proxied sleds are routed through chassis, as a best practice the admin must assign both the chassis and the sleds in a device manager's scope.

Issue 4: Global search count is greater than the actual result count for scope-restricted device managers..

Description: When a 'scoped' device manager uses Global Search, the total search count exceeds the actual items displayed. [197629]

Issue 5: Run Inventory on Group is unavailable for Device Manager users.

Description: For the Device Manager users, **Run Inventory on Group** option under **Inventory** on the All Devices page is unavailable. [193441]

Discovery and inventory

Issue 1: Chassis Health State shows as disconnected for 10 minutes after the chassis administrator password is reset.

Description: When the Administrator password is reset on any discovered chassis (MX7000, M1000e, VRTX,and FX2), there is a disconnection of the chassis with the appliance for 600 seconds. During this interval, the Health State of the chassis on the All Devices page is displayed as 'Disconnected' and the tasks initiated on the chassis and sleds fail. [198434]

Issue 2: Post deletion of 8K devices, Onboarding task does not trigger during next discovery cycle.

Description: Post deletion of 8,000 devices from the appliance, the automatic onboarding task fails during the next discovery cycle. [200458]

Resolution: Restart the services from the Text User Interface (TUI) page.

Issue 3: Mismatch seen in CIQ data and OME device inventory for RaidControllerId.

Description: The *RaidControllerId* attribute in the *ServerRaidControllers* component in OpenManage Enterprise inventory and CIQ device data inventory have different values for the same device. [185745]

Issue 4: Duplicate entries displayed for third party devices when discovered using multiple protocols.

Description: For third party devices such as the HPE Proliant servers, you might see duplicate entries if they are discovered using multiple protocols. This duplication can be corrected by deleting the entries and rediscovering the device(s) using only the IPMI protocol. [180572]

Issue 5: Unable to retrieve hardware logs for HPE servers.

Description: For the discovered HP servers, the devices' Hardware Logs are not displayed as the third party library used by the appliance is unable to extract the hardware logs for HP iLO servers. [170550]

Issue 6: HPE servers display incorrect power supply data.

Description: For the discovered HP servers, the 'Power Supply' details are not displayed under the subsystem health section on the device's Overview page. This detail is missing as the third party API that is used to gather sensor health details, doesn't provide the 'Power Supply' data. [85153]

Issue 7: HPE servers do not display certain FRU fields.

Description: For the discovered HP servers, the following field-replaceable unit (FRU) details are not displayed under the device's Hardware page: Memory FRU details, BIOS - Part number and version, BMC controller - Part number. [75653]

Issue 8 : DIMM information is not available on Hypervisors.

Description: For the discovered Hyper-V servers, the Populated DIMM Slots and the Total DIMM Slots fields are displayed as '0' on the device's Overview page. [IT-84431]

Issue 9: MAC address not displayed for the discovered Windows servers.

Description:For the discovered Windows servers using Open SSH, the MAC address is not displayed on the device's Hardware > Device Management Info page. [181229]

Issue 10 : Few invalid IP range formats are not being validated when creating a Discovery job.

Description: While discovering devices, a few invalid IP and IP-range formats are not being rejected by the Create Discovery Job wizard, resulting in 'failed' Discovery jobs. [178692]

Resolution: Invalid IP or IP-range formats, as mentioned in the Context Help**(i)**, must not be used for device discovery.

Issue 11: Unclear error message on failure of Windows server discovery using SSH.

Description: Discovery of Windows server(s) using non-admin credentials fails with an error message '*Unable to connect to the device over SSH because a connection error occurred*.' This must be interpreted instead as '*Unable to perform the requested action because the device management endpoint authentication over SSH failed*'. [158088]

Issue 12: Guest Information for Hyper-V 2012 R2 is not available.

Description: The Guest information for the discovered Hyper-V 2012 R2 servers is not available on the device's Hardware page. [159535]

Issue 13: Windows Hyper-V guest information is missing when correlated with iDRAC during MX7000 discovery.

Description: The correlation of Windows Hyper-V post MX7000 chassis CCD, fails to give the Guest VM information under Device details page. [167935]

Resolution: The sled discovery need to be done out of the MX7000 chassis and managed separately to view the guest details.

Issue 14: Incorrect managed state is displayed for MX7000 chassis when discovered using lower privileged credentials.

Description: The Managed State of the previously 'Monitored' MX7000 chassis and sleds, on the All Devices page, is incorrectly displayed as 'Managed' post their rediscovery using the same lower privilege local or AD/LDAP credentials (Viewer or Device Manager) as before. [152154]

Issue 15: Managed state is not updated for devices when SNMP trap destination is manually set from iDRAC.

Description: If the SNMP trap destination is manually set in iDRAC as OpenManage Enterprise, the alerts are received and processed by the appliance. However, the device's Managed State displayed on the All Devices page remains the same as its initially discovered state of 'Monitored,' 'Managed,' or 'Managed with Alerts.' [158992]

Issue 16: Incorrect inventory data after moving sled from lead to member chassis.

Description: For the Multi-Chassis Management (MCM) group, a Chassis Refresh Inventory task for the 'lead' chassis does not fully update the sled inventory. A Chassis Refresh Inventory task is triggered in the appliance when a sled is removed from the lead chassis and added to a member chassis. [165191]

Resolution: To immediately update the sled inventory, trigger the refresh inventory of the sled manually. Otherwise, the sled inventory will be refreshed during the automatic daily inventory collection.

Issue 17 : Firmware compliance is executed on new device discovery.

Description: All the existing firmware compliance tasks will refresh automatically post device discovery. [146981]

Issue 18: Mismatch in device management IP for VxRail devices on Device Details and All Devices pages.

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 19: Servers reconfigured as VxRAIL post discovery, do not automatically group under HCI upon inventory refresh.

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 20: YX1X servers with iDRAC firmware version 1.98 or later show health status as 'unknown'.

Description: The All Devices page shows **Health Status** of the discovered YX1X servers with iDRAC firmware version 1.98 or later as **unknown**.

Issue 21: iDRAC virtual console launch point is unavailable for proxied sleds.

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

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

Issue 22: PowerVault MD3 storage arrays do not show the complete model numbers.

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]

Tasks

Issue 1

Description: For the failed alert-policy-triggered IPMI tasks, the task execution history on the Job Details page shows duplication of the error message. [204404]

Issue 2

Description: The IPMI CLI command `-I lanplus shell` doesn't end automatically and the jobs associated with such tasks would appear as 'In Progress' for a prolonged time on the Jobs page. [173061]

Resolution: You must run an Exit command to terminate such jobs.

Issue 3

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

Issue 4

Description: Configuration > **VLANs** page does not update automatically after importing VLAN definitions from file or from chassis. [153611]

Resolution: Refresh the **Configuration** > **VLANs** page or navigate to another page and return to view the newly-imported VLAN definitions.

Firmware and driver updates

Issue 1: Firmware compliance on multiple baselines logs CDEV9000 alerts for a single device with non associated firmware compliance baseline.

Description: When firmware compliance check is executed for multiple firmware baselines simultaneously, the warning alert —CDEV9000 - This device and several others has become non compliant after running compliance task: <Baseline Name>— is sometimes logged for these baselines on the Alerts page with any one random device in any of the firmware compliance baseline. Sometimes the firmware baseline is not associated with the device. [185315]

Issue 2: CDEV9000 non-compliance alert is logged for only one random device in the firmware baseline.

Description: When a firmware/driver baseline with many devices is checked for compliance, the warning alerts CDEV9000 on the Alerts page is logged for only one random non-compliant device from that baseline. [185312]

Issue 3 : In-band Windows servers driver update fails if their IP addresses are outside of the Restrict Allowed IP Range.

Description: Driver update task fails for the in-band Windows servers if their IP addresses are outside of the appliance's Restrict Allowed IP Range. [199725]

Resolution: Before initiating driver update tasks on the in-band Windows targets, ensure that their IP addresses are included in the Restrict Allowed IP Range (Application Settings > Security > Settings).

Issue 4

Description: For the discovered network switches with firmware version 10.5, the firmware version is displayed as 'NA' on the Device Overview page. [192087]

Issue 5

Description: Inventory collection and the firmware update on chassis storage sleds is not supported in OpenManage Enterprise if they are managed via chassis device management. [198981]

Issue 6

Description: In-band driver updates are only supported on Windows with OpenSSH. Driver updates on third party SSH hosted on Windows, such as the CygwinSSH, are not supported. [157887]

Issue 7

Description: For the family of network adapter drivers, the operating system installed version, as seen in the Device Manager, differs from the version available in the online catalog. [157824]

Issue 8

Description: PERC H730P controller driver is not listed in the Firmware/Driver compliance report as it is currently not included in the online firmware/driver catalog. However, as this driver is a part of the Windows' server inventory, it is listed in the Inventory report of the windows devices.[163175]

Issue 9

Description: The firmware or driver compliance status of network switches, modular IOAs, and Dell storage devices may show as "Compliant" (but unselectable) in the firmware/driver compliance reports even though update of these devices are not supported by the Dell catalog.

Resolution: It is recommended to perform individual firmware or driver updates for these devices using their respective individual Update package. To perform individual firmware or driver updates, select a device on the All Devices page, and click **View Details** > **Firmware/Drivers** and select the individual package option. For more information about the list of unsupported devices, refer the OpenManage Enterprise version 3.4 User's Guide (Firmware/driver compliance baseline reports—'false' compliant devices)

Issue 10

Description: AMD chipset driver update on the R6525 servers fails using OpenManage Enterprise Firmware/driver update feature. [159058]

Resolution: Windows (64-bit) driver updates for R6525 AMD chipsets must be done manually outside of the appliance.

Issue 11

Description: The firmware update task using the HTTP and HTTPS local shares fails, if these local shares were configured using proxy settings and are not listed in the proxy exception list. [151332]

Resolution: The HTTP and HTTPS local shares which are configured using the proxy settings, need to be listed in the proxy exception list before initiating any firmware update tasks using these shares.

Issue 12

Description: Firmware upgrade fails when iDRAC firmware versions older than 2.40.40.40 are upgraded directly to 2.63.60.61 with an error message **Unable to verify Update Package signature.** This failure happens as the firmware versions older than 2.40.40.40 cannot validate the latest SHA-256 digital signature of the Dell Update Packages. [146564]

Resolution: First upgrade the older iDRAC firmware versions to 2.40.40.40 before attempting an upgrade to iDRAC firmware version 2.63.60.61.

Issue 13

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

Issue 14

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

Issue 15

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

Issue 16

Description: When updating MX7000 chassis in the MCM mode, always make sure that the lead chassis is updated as the final step after updating all the member chassis. Also, chassis and sled firmware updates must be initiated separately. [168883]

Issue 17

Description: The Firmware Update task fails on the MCM member chassis with error message 'Syncing data with passive MM Task Failed. Completed With Errors'. [169333]

Configuration management

Issue 1: Improper alignment of compliance template attribute when the Upgrade notification bar is displayed.

Description: There is a misalignment of the compliance template attributes on the Template Details page when the Upgrade notification bar is displayed. [203837]

Issue 2: Duplicate log messages are seen in the task execution history of Create and Deploy template jobs.

Description: Duplication of log messages in the task execution history is seen for Create Template and Deploy Template jobs (Job Details page > View Details). [203788]

Issue 3: Template deployment fails if the reference server has a non-default port number.

Description: If a reference server has a non-default port number, then, the deployment of a template created using that reference server fails on target servers that have default port numbers. The template deployment fails with a 'Connection with server lost' error. [204048]

Issue 4 : VLAN attributes cannot be deployed using profiles unless deployed during template deployment.

Description: VLAN attribute changes fail on the target MX7000 sleds using profile redeployment, if the VLAN attributes were not initially deployed on the MX7000 sleds during template deployment using the 'Propagate VLAN settings immediately' option. [204044]

Resolution: Use the 'Propagate VLAN settings immediately' option every time VLAN changes are made during template deployment.

Issue 5: Redeployment of an unassigned profile on a new target is unsuccessful.

Description: Attempt to redeploy a profile to a new target, after the profile is unassigned from its earlier target, fails with a 'CGEN6008 -Unable to process the request.....' error. This error is exhibited even when the previous and new target are identical to each other. [204655]

Issue 6

Description: Deployment of a second template on a chassis is allowed even when a profile is already deployed on it. [204441]

Issue 7

Description: If only VLANs are assigned to a target device during profile deployment, then these VLANs are not reclaimed by the appliance when the profile is unassigned from the device. This behavior is not seen if other identities were assigned along with VLAN definitions during the profile deployment. [174360]

Issue 8

Description: User Password attributes can't be set on the MX7000 and the Chassis Management Controller Deployment templates. [200293]

Issue 9

Description: If only VLANs are assigned to a target device during profile deployment, then these VLANs are not reclaimed from the device when the profile is migrated to a new device. This behavior is not seen if other identities were assigned along with VLAN definitions during the profile deployment. [174576]

Issue 10

Description: Profile redeployment on FX2, VRTX, and M1000e chassis with edited VLAN configuration (tagged and untagged values), clears only those VLAN values which were set during the initial deployment of the profile. The other VLAN values on the ports that were not set during the initial deployment of the profile are not cleared during redeployment. [175692]

Issue 11

Description: Same inventory details can be present on two servers post migration, as the 'true' target-specific attributes are not reclaimed from the 'source' server as part of migration. [160622]

Issue 12

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

Issue 13

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 14

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

Issue 15

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 16

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 17

Description: If a chassis template is deployed with a new static IP address on the FX2, VRTX, and M1000e chassis, then these devices need to be re-discovered with the new IP for managing the device.

Issue 18

Description: The deployment task of an MX7000 chassis fails if proxy authentication is 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 19

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

Issue 20

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 21

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 22

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 23

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 24

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 25

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 26

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: AD group searches fail for an hour due to slow sync when AD/LDAP groups are added using the DNS option.

Description: Searching for an active directory group name in the Import Directory Group wizard immediately after adding the directory service using the DNS option could unsuccessful for up to one hour. This happens if there is a delay in synchronization of the newly-added domain controller. [203928]

Issue 2: Connection State of ESXi servers that are disconnected due to authentication failure are shown as 'Disconnected.'

Description: For the authentication-related disconnected ESXi servers, the Connection State on the All Devices page is displayed as 'Disconnected' instead of 'Disconnected (Authentication failure)'. [198421]

Issue 3: If Ping Identity is used for OIDC provider, the appliance can only be used with Administrator role.

Description: With OIDC provider PingFederate, it is observed that all the OpenID client policies associated with the OpenManage Enterprise Client IDs are reset to the policy marked as 'Default' when the appliance console gets re-registered with the OIDC provider. Re-registration of the appliance console with OIDC provider happens in the event of an appliance upgrade, change in network configuration, or change in SSL certificate. [193717]

Resolution: This is an issue with the OIDC provider, hence, the administrator must reconfigure all the OpenManage Enterprise Client IDs on the OIDC provider site to avoid any security concerns.

Issue 4: Manually setting the time to an earlier time on the VMware vSphere fails if periodic time synchronization is enabled in the VM.

Description: On VMware vSphere, changing the appliance's time to an earlier time than the system time fails if the periodic time synchronization in the VM is enabled. [198702]

Resolution: To set the appliance's time to an earlier time than the system time, disable the periodic time synchronization in the VM, by launching the vSphere Client, go to **Edit Settings** > **VM Options** > **VMware Tools** > **Synchronize Time with Host** and deselect the checkbox **Synchronize time periodically**.

Issue 5: Identity pool Usage page shows "CGEN1006" error on sorting for the first time.

Description: An error 'Error getting identity pool information (CGEN1006)' is displayed when sorting is done on an identity pool's Usage page fields. Also, the identity pool's Usage page turn blank when **View By** filter is applied. [200451]

Resolution: Return to the identity pool's Usage page after navigating to another page.

Issue 6

Description: Browser is unable to validate a Certificate Signing Request that is generated by providing IP address in the Subject Alternate Name (SAN) field on the Certificates section of the Application Settings > Security page and shows 'Your connection to this site is not secure' message. [204172]

Resolution: Provide a valid domain name in the SAN field and login with the appliance FQDN. The browsers will then be able to validate the certificate and show connection as secure.

Issue 7

Description: The traps forwarded from one OpenManage Enterprise console to another OpenManage Enterprise console are received as Miscellaneous category alerts with message "unknown trap received...," if the Trap Forwarding Format is set as "Original Format" in the former console. [188953]

Issue 8

Description: If SNMPv3 destination(s) is/are already added as alert forwarding destination(s) in the appliance, then in order to add and apply a new alert forwarding destination address, the appliance prompts only the first time to re-enter of all the previously entered SNMPv3 Authentication and Privacy passphrases before proceeding. [190690]

Resolution: Regardless of the appliance prompt, you must re-enter all the previously entered SNMPv3 Authentication and Privacy passphrases every time the SNMP community string or port is edited on Application Settings > Alerts > SNMP Alert Forwarding Configuration.

Issue 9

Description: For the discovered C9010 network switches, the Model field on the 'All Devices' and the 'Device Details' page is displayed as 'Unknown.' [188383]

Issue 10

Description: When a C9010 network switch is rebooted or reloaded, the alerts received in the appliance are being categorized as Miscellaneous with message 'Unknown trap received with enterprise OID...' [188382]

Issue 11

Description: When a Z9264 network switch is rebooted or reloaded, the alerts received in the appliance are being categorized as Miscellaneous with message 'Unknown trap received with enterprise OID....' [194718]

Issue 12

Description: Post addition of the disk space using the Configure Appliance Disk Size feature in the Text User Interface (TUI) , deletion or reduction of the appliance's console expanded disk space is not supported . [192976]

Resolution: To remove a newly-added disk or to reverse the increase in size of an existing disk, you must revert to prior VM snapshot that you are recommended to take as a backup before applying any disk configuration changes.

Issue 13

Description: For a logged-in AD user belonging to an imported child AD group, it is observed that multiple roles such as Device Manager and Viewer are displayed upon a mouseover on the username on the appliance masthead right-hand corner. This happens if the parent directory group and child directory group are imported with different privileges. For such AD users, the role with the maximum privilege will be applied. [195183]

Issue 14

Description: Console upgrade fails from version 3.4.1 to version 3.6, if there are a large number (more than 2,000) unreachable devices, in multiple discovery settings, in OpenManage Enterprise version 3.4.1. This happens as the long runtime of Discovery task exceeds the maximum wait-time limit of 48 hours set for the initiation of other post-upgrade tasks. [201178]

Resolution: To prevent upgrade failure, in such rare scenarios, you can manually cancel the Discovery task to allow the post-upgrade tasks to initiate and finish normally.

Issue 15

Description: An invalid audit log indicating 'console upgrade failure' is generated upon a successful upgrade of the appliance from version 3.4 to version 3.5. This audit log can be ignored. [173311]

Issue 16

Description: The Console Update Execution job's status is displayed as 'Failed' on the Jobs page, if the appliance upgrade takes more than 60 minutes. The 'Failed' status is due to a time out of the Console Update Execution job and can be ignored as this has no functional impact on the upgrade process. [170688]

Issue 17

Description: The built-in Virtual Disk report contains duplicate or empty values if the virtual disks and physical disks don't have any associations and are used individually. This issue is not observed if the VDs an PDs are being used together. [174851]

Resolution: It is recommended to use a custom report to get only the virtual disk data if the VDs and PDs are not associated.

Issue 18

Description: For Ubuntu devices, the **OS Version** under operating system information (from iDRAC/ISM) on the Device Overview page is not displayed. [171103]

Issue 19

Description: With the Japanese version of the appliance, it is observed that the PDF export of the Warranty page contains illegible characters. [176493]

Resolution: To get the PDF export of the Warranty page without the illegible characters, use the following workaround:

1. Export CSV report in Excel.
2. Change the encoding type to UTF-8.
3. Save it as PDF.

Issue 20

Description: When the appliance is configured to IPv6, it is unable to reach the targets like SMTP, syslog servers and share through FQDNs which is resolvable to both IPv4 and IPv6. [153980]

Resolution: When the features that use FQDN fail, it is recommended to check the interface and use the corresponding IP. For instance, if the primary network is enabled with only IPv6, and the FQDN expected to work on primary interface fails, user can use IPv6 address in the place of FQDN as a workaround. This applies for secondary interface as well.

Issue 21

Description: **Description**: The Text User Interface (TUI) screen is not displayed until the 'Enter' key is pressed after updating the appliance to version 3.4.1 on ESXi with large deployments involving 8,000 or more devices. [173206]

Issue 22

Description: When a Lead chassis retires and a backup chassis becomes the new lead on OpenManage Enterprise, the refresh inventory marks the original backup chassis and its associated devices to be invisible and not shown in the UI. [161300]

Resolution: Discover the new Lead on OpenManage Enterprise.

Issue 23

Description: The rack physical groups with long names consisting of more than 150 characters with no spaces, the appliance wizards experiences an 'overflow'. [164157]

Resolution: Limit the number of characters used to create names.

Issue 24

Description: If a Configuration Inventory task finds external identities that fall in an existing identity pool and that identity pool is later deleted and a new one with the same or overlapping identities is created, the new identity pool will not show those identities as assigned. [160888]

Issue 25

Description: Creation of templates using an MX7000 chassis that is configured to both IPv4 and IPv6 fails if the appliance is configured to use only IPv6. [167525]

Resolution: Ensure that both the appliance and the MX7000 chassis are configured to use the same protocol(s).

Issue 26

Description: For the YX3X servers, few of the Subsystem Health section details, available on the individual device's Overview page, such as the Storage, Temperature, and License details are displayed as 'No Data available,' even when their health status is 'OK.' [155425]

Issue 27

Description: The 'From' address used for all email actions, such as Reports, Update, Discovery and Alert Policies, is dependent on the SMTP server configuration. For some SMTP server configurations, the 'From' address is the Sender Email ID specified in the Application settings (**Application Settings** > **Console Preferences** > **Email Sender Settings** > **Sender Email ID**) and

for others it is the username used for SMTP server authentication (**Application Settings** > **Alerts** > **Email Configuration** > **SMTP Server Network Address**). [164204]

Issue 28

Description: There is currently a discrepancy between the actual number of MIBs imported and the MIB count displayed on the **Monitor** > **MIB** page. [160040]

Issue 29

Description: When NIC teaming is enabled on MX7000 chassis along with VLAN configuration, deploying of VLAN from the OpenManage Enterprise console will overwrite the NIC teaming configurations to 'No teaming'. The LACP or other teaming options would need to be reconfigured from MX7000.

Issue 30

Description: Appliance is unable to download the console upgrade from HTTP or HTTPS intranet share, when the intranet share address is blocked in proxy filtering. [152092]

Resolution: If the upgrade download has a problem connecting through proxy, uncheck the proxy settings and then download.

Issue 31

Description: After a fresh install or an upgrade to OpenManage Enterprise and configuration of network interface to DHCP, any prior static IP settings will not be retained. [148789]

Issue 32

Description: The **Timezone** and **NTP Server Address** fields added to the **Application Settings** > **Network** > **Time Configuration** section will remain blank and will not be displayed for a few minutes if the entered NTP server IP address is not reachable. [151221]

Issue 33

Description: Addition of a new network interface in hypervisors fails immediately after upgrading the OpenManage Enterprise from version 1.0 to version 3.3.1 (1.0>3.0>3.1>3.2>3.3.1). An error message "`Failed to reconfigure virtual machine Config-7 1.0 to 3.3.1. The attempted operation cannot be performed in the current state (Powered on)`" is displayed. [146752]

Resolution: Power off the virtual machine, add a new network interface, and then power on the virtual machine if the upgrade workflow is 1.0>3.0>3.1>3.2>3.3.1.

Issue 34

Description: Chassis health status shown in the chassis UI and the OMEnterprise console does not match. This happens because the chassis UI shows the chassis controller's health, whereas the OMEnterprise shows the overall health of the chassis. Hence, it is recommended to check the component-related health status for M1000e, FX2s and VRTX chassis. [85977]

Issue 35

Description: Emails for alert policies don't work when the same event is generated twice within 2 minutes. Email action for alerts containing the same message ID and content are triggered every 2 minutes to avoid many repeated/redundant alert messages in the inbox.[148407]

Issue 36

Description: While creating a customized device discovery job protocol for SNMP devices, the displayed default settings of 3 in the **Retries box** and 3 seconds in the **Timeout box** can be overlooked and should be customized as desired. [147416]

Issue 37

Description: When updating local shares for a manual upgrade for versions without any installed plugins (such as 3.1 and 3.2), the audit log displays warning entries such as 'Unable to retrieve the source file of type Plugin Catalog because the file does not exist' and 'The status of downloading the Plugin Catalog is Failed'. These error messages do not have any functional impact on the upgrade process and can be ignored. [144379]

Issue 38

Description: Clicking **Check Update** on OpenManage Enterprise version 3.2, where PowerManager plugin 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 39

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

Resolution: OpenManage Enterprise 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 40

Description: Post console update **Time interval** should be enabled manually in alert policy as it is disabled by default.

Issue 41

Description: Alert policies have been recategorized since OpenManage Enterprise version 3.3.1. The alert policies from appliance versions before 3.3.1 need to be recreated after the appliance upgrade.

Issue 42

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 43

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 44

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 45

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

Resolution: N/A

Issue 46

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

Resolution: Ignore or click **Dismiss**.

Issue 47

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 48

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 49

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 50

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

Resolution: N/A

Issue 51

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

Issue 52

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

Issue 53

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 54

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 55

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 56

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 57

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 58

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

Issue 59

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

Issue 60

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

Issue 61

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 62

Description: All the AD/LDAP groups imported from the OpenManage Enterprise versions before version 3.2, such as the version 3.1 and version 3.0, should be deleted and re-imported.

Issue 63

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 64

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 65

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 66

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 67

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 3.7 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 3.7:

Table 1. 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	32 GB	16 GB
Processors	8 cores total	4 cores total
Hard drive	400 GB	400 GB

Minimum system requirements for deploying OpenManage Enterprise version 3.7

Table 2. Minimum system requirements

Particulars	Minimum requirements

Supported hypervisors	• VMware vSphere versions:
	  ○ vSphere ESXi 5.5 Onwards
	• Microsoft Hyper-V supported on:
	  ○ Windows Server 2012 R2 Onwards
	• KVM supported on:
	  ○ Red Hat Enterprise Linux 6.5 Onwards

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 • Microsoft Edge version 41.16299 and later

Table 2. Minimum system requirements (continued)

Particulars	Minimum requirements
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.

Generic naming convention for Dell EMC PowerEdge servers

To cover a range of server models, the PowerEdge servers are now being referred to using the generic naming convention and not their generation.

This topic explains how to identify the generation of a PowerEdge server that are referred to using the generic naming convention.

Example:

The R740 server model is a rack, two processor system from the 14th generation of servers with Intel processors. In the documentation, to refer to R740, generic naming convention **YX4X** server is used, where:

- The letter **Y** (alphabet) is used to denote the following server form factors:
  - **C** = Cloud - Modular server nodes for hyper-scale environments
  - **F** = Flexible - Hybrid rack-based sleds for rack-based FX2/FX2s enclosure
  - **M** or **MX*** = Modular - Blade servers for the modular enclosure MX7000, M1000e and/or VRTX
  - **R** = Rack-mountable servers
  - **T** = Tower Servers
- The letter **X** (digit) denotes the class (number of processors) of the server.
- The digit **4** denotes the generation of the server.
- The letter **X** (digit) denotes the make of the processor.

Table 3. PowerEdge servers naming convention and examples

YX3X servers	YX4X systems
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540

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.