Rev. 1
October 2021

Dell EMC OpenManage Enterprise 3.8 Release Notes

Describes the new features, changed features, resolved issues, known issues, and limitations in OpenManage Enterprise.
Release Type: Major (MA)

Topics:

Revision history

This section provides a description of document changes.

Table 1. Document Revision history

Document Revision	Date	Description of changes
01	October 2021	Initial release in new template

Product description

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. OpenManage Enterprise's system management and monitoring is best suited for enterprise LANs and is not recommended for usage over WANs. For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

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 deployment 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.

Some of the security features of OpenManage Enterprise are:

- Role-based access that limits access to console settings and device actions.

- Scope based access control allows administrators to restrict the device groups that device managers can access and manage.
- Hardened appliance with Security-Enhanced Linux (SELinux) and an internal firewall.
- Encryption of sensitive data in an internal database.
- Use of encrypted communication outside the appliance (HTTPs).
- Create and enforce firmware and configuration-related policies.
- Provision for configuring and updating the bare-metal servers.

New features

The following table describes the features that are introduced in OpenManage Enterprise version 3.8.

Feature name	Feature description
HTTPS support	Ability to configure the internal appliance share to furnish content through HTTPS or CIFS (default).
Windows 2022 support	Deployment of appliance on Windows Server 2022 is supported.
Easier way to create and download a console log archive from the Graphical User Interface (GUI)	You can now create a console log archive and then download it from the **Monitor** > **Audit Logs** > **Troubleshoot** submenu rather than the Text User Interface (TUI) when the Field Service Debug (FSD) is enabled.

Known issues

Table 2. Known issues

Issue ID	Functional area	Description	Workaround/Resolution
210858	Alert Management	If several alerts are received at once by the lead chassis, in a multi-chassis management (MCM) environment, then the display and processing of those alerts in OpenManage Enteprise is delayed.	
204404	Alert Management	For the failed alert-policy-triggered IPMI tasks, the task execution history on the Job Details page shows duplication of the error message.	
190690	Alert Management	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.	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.
188953	Alert Management	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.	
164204	Alert Management	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**	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
		ID) and for others it is the username used for SMTP server authentication (**Application Settings** > **Alerts** > **Email Configuration** > **SMTP Server Network Address**).	
160040	Alert Management	There is currently a discrepancy between the actual number of MIBs imported and the MIB count displayed on the **Monitor** > **MIB** page.	
148407	Alert Management	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.	
132915	Alert Management	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.	
124596	Alert Management	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.	
122657	Alert Management	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.	
111854	Alert Management	When an already imported MIB is renamed and parsed through API the trap status is reported as 'Existing' instead of 'Imported'.	
121158	Appliance Deployment	While programmatically deploying the OpenManage Enterprise from Linux shell, if the argument provided for *--name=* in the command line begins with a "**$**" then the argument is ignored and appliance is deployed with the name OPENMANAGE ENTERPRISE.	The *--name=* argument, which begins with "**$**" in the command line must be enclosed in single quotes, for example, *--name=* **'$OME-VM'**.
198702	Appliance Settings	Manually setting the time to an earlier time on the VMware vSphere fails if periodic time synchronization is enabled in the VM. 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.	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**.
192976	Appliance Setting	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.	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.

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
151221	Appliance Setting	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.	
209489	Appliance Upgrade	Upgrading of a PMP-installed OpenManage Enterprise appliance to version 3.8 might take longer. Appliance upgrade time might be between 1 and 10 hours depending on the number of devices being monitored by Power Manager.	
209000	Appliance Upgrade	Upgrade of the appliance may fail if initiated post deletion of devices. If an upgrade of the appliance is initiated post deletion of devices, the Off-boarding tasks may fail or run endlessly resulting in upgrade failure and a console reboot with the previous working state of the appliance.	Restart the services from the Text User Interface (TUI) page
208040	Appliance Upgrade	When upgrading an appliance that is supporting 8,000 devices to v3.8, the Console Update Execution job's status may be displayed as 'Failed' on the Jobs page. When upgrading an appliance that is supporting 8,000 devices to v3.8, the Console Update Execution job's status may be displayed as 'Failed' on the Jobs page. This Failed status of the Console Update Execution task is seen 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.	
201178	Appliance Upgrade	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.	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.
200458	Appliance Upgrade	Post deletion of 8K devices, Onboarding task does not trigger during next discovery cycle. Post deletion of 8,000 devices from the appliance, the automatic onboarding task fails during the next discovery cycle.	Restart the services from the Text User Interface (TUI) page.
173206	Appliance Upgrade	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.	
170688	Appliance Upgrade	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.	
146752	Appliance Upgrade	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`	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
		`cannot be performed in the current state (Powered on)` " is displayed.	
144379	Appliance Upgrade	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.	
114683	Appliance Upgrade	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.	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.
108055	Appliance Upgrade	After upgrading to the latest version of OpenManage Enterprise, the existing job IDs are changed.	
173311	Audit Log	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.	
132601	Configuration Deployment	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.	Select 'BIOS' attributes only for deployment.
113576	Configuration Deployment	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.	
108779	Configuration Deployment	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'.	
108484	Configuration Deployment	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.	
107230	Configuration Deployment	After deploying an MX7000 chassis template, you cannot log in to the MX7000 chassis with LDAP credentials.	Manually update the LDAP Bind password to log in.
	Configuration Deployment	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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
	Configuration Deployment	The directory service details in an MX7000 chassis are overwritten after the device configuration template is deployed.	
	Configuration Deployment	After a chassis is removed from the MCM group, you must rediscover the lead and member chassis to create and deploy a configuration template.	
	Configuration Deployment	Template Deployment with iDRAC Management IP option "Set as DHCP" fails, and the task has to be tracked from iDRAC for final status.	
204655	Configuration Management	Redeployment of an unassigned profile on a new target is unsuccessful. 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.	
204048	Configuration Management	Template deployment fails if the reference server has a non-default port number. 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.	
203837	Configuration Management	Improper alignment of compliance template attribute when the Upgrade notification bar is displayed. There is a misalignment of the compliance template attributes on the Template Details page when the Upgrade notification bar is displayed.	
175692	Configuration Management	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.	
174576	Configuration Management	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.	
174360	Configuration Management	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.	
160888	Configuration Management	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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
129049	Configuration Management	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.	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.
107376	Configuration Management	The **Migration Profile** task fails if the user is not configured on the target device with the error: 'User Name is not configured'.	
105156	Configuration Management	The changed VLAN name and IDs are not updated on the target MX7000 chassis after a stateless deployment task is run.	
98511	Configuration Management	The Reclaim Identities and Profile Migration features are not supported for Emulex OneConnect Cards.	
212253	Device Grouping	If a device under any chassis group (MX7000, M1000e, VRTX, and FX2) is deleted, the group for the chassis also gets deleted.	Rediscover the chassis.
210064	Device Grouping	Any scheduled tasks, such as Blink device, Power Control, Remote Command, and Change Virtual console, on hierarchical static groups continue to run on the groups even after the groups are removed from hierarchy.	
209637	Device Grouping	When a new device is added to a group associated to a Configuration baseline, the Baseline Compliance status of the group in the Compliance report is displayed as 'Unknown' (?).	
164157	Device Grouping	The rack physical groups with long names consisting of more than 150 characters with no spaces, the appliance wizards experiences an 'overflow'.	Limit the number of characters used to create names.
116913	Device Grouping	Servers that are reconfigured as VxRAIL do not automatically group under HCI upon refreshing the inventory.	After a server is reconfigured as a VxRAIL, rediscover the device in the Discovery page. After rediscovery, the device is correctly grouped under HCI.
86481	Device Grouping	A query group with switch and device power state together is not working as expected.	Exclude switch power state while creating a query group.
212646	Device Management	For the servers discovered using read-only user credentials, the **Launch Virtual Console** button on the device's Overview page remains enabled. Clicking the button displays an error- 'Error launching Virtual Console: An unknown error has occurred. Please try again'.	
198434	Device Management	Chassis Health State shows as disconnected for 10 minutes after the chassis administrator password is reset. 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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
173061	Device Management	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.	
170550	Device Management	Unable to retrieve hardware logs for HPE servers. 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.	
158992	Device Management	Managed state is not updated for devices when SNMP trap destination is manually set from iDRAC. 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'.	
136816	Device Management	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.	
102887	Device Management	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.	
91653	Device Management	Mismatch in device management IP for VxRail devices on Device Details and All Devices pages. 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.	
81207	Device Management	In the **Execution Details** section, data must be manually sorted in the table every time after moving to a new page.	Sort information of a single page at a time.
	Device Management	The iDRAC virtual console management launch point is unavailable in the All Devices page for sleds with a 'Proxied' onboarding state.	
99821	Device Monitoring	Currently, the health status including PSU and temperature data is not displayed for the storage devices.	
198421	Device Monitoring	Connection State of ESXi servers that are disconnected due to authentication failure are shown as 'Disconnected'. For the authentication-related disconnected ESXi servers, the Connection State on the All Devices page is displayed as 'Disconnected' instead of 'Disconnected (Authentication failure)'.	
192087	Device Monitoring	For the discovered network switches with firmware version 10.5, the firmware version is displayed as 'NA' on the Device Overview page.	
181229	Device Monitoring	MAC address not displayed for the discovered Windows servers. For the discovered Windows servers using Open SSH, the MAC address is not displayed	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
		on the device's Hardware > Device Management Info page.	
180572	Device Monitoring	Duplicate entries displayed for third party devices when discovered using multiple protocols. 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.	
171103	Device Monitoring	For Ubuntu devices, the **OS Version** under operating system information (from iDRAC/ISM) on the Device Overview page is not displayed.	
167935	Device Monitoring	Windows Hyper-V guest information is missing when correlated with iDRAC during MX7000 discovery. The correlation of Windows Hyper-V post MX7000 chassis CCD, fails to give the Guest VM information under Device details page.	The sled discovery need to be done out of the MX7000 chassis and managed separately to view the guest details.
159535	Device Monitoring	The Guest information for the discovered Hyper-V 2012 R2 servers is not available on the device's Hardware page.	
157824	Device Monitoring	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.	
155425	Device Monitoring	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'.	
153611	Device Monitoring	**Description: Configuration** > **VLANs** page does not update automatically after importing VLAN definitions from file or from chassis.	Refresh the **Configuration** > **VLANs** page or navigate to another page and return to view the newly-imported VLAN definitions.
152154	Device Monitoring	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.	
99821	Device Monitoring	Currently, the health status including PSU and temperature data is not displayed for the storage devices.	
85977	Device Monitoring	An individual Chassis Management Controller (CMC) health may not be correctly displayed in the device drill-down operation.	Always consider the CMC rollup health status.
85977	Device Monitoring	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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
85153	Device Monitoring	HPE servers display incorrect power supply data. 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	Device Monitoring	Discovery of an HP server by using IPMI command may not reflect the correct rollup health status.	View the lower-level sensor health data.
75653	Device Monitoring	HPE servers do not display certain FRU fields. 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.	
	Device Monitoring	The All Devices page shows health status of the discovered YX1X servers with iDRAC firmware version 1.98 or later as unknown.	
211345	Discovery	Listing of a standalone switch, that was discovered using SNMP, is deleted from the All Devices page if it rediscovered during the FX2, VRTX, and M1000e chassis discovery. The All Devices page stops displaying the listing of a standalone switch that was discovered using SNMP, after a rediscovery of the same switch using the **Disover IO Modules with chassis option** during chassis discovery. This is applicable to the FX2, VRTX, and M1000e chassis switches.	To relist the switch on the All Devices page, rediscover the switch using it chassis or as a standalone.
178692	Discovery	Few invalid IP range formats are not being validated when creating a Discovery job. 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.	
158088	Discovery	Unclear error message on failure of Windows server discovery using SSH. 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*'.	
147416	Discovery	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.	
128842	Discovery	The **Schedule** advanced filter in the **Monitor > Discovery** page incorrectly displays even those discovery jobs which have completed their initial scheduled run.	
210644	Firmware/Driver Management	When managed sleds get discovered via chassis using chassis credentials, the Rollback of the firmware version is not working. This issue exists on a newly-installed OpenManage Enterprise appliance as well.	Download the DUPs and do the single DUP update manually.

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
211090	Firmware/Driver Management	On the Firmware/Driver Compliance Report page, the filter based on Component Type in the Advanced Filters drop down is not working. On the Firmware/ Driver Compliance Report page, if a device has both driver (OS components) and firmware components for update and if the user select one of the components from the Component Type in the Advanced Filters drop down followed by the Select All(checkbox) components, then, updates are triggered for both the driver and firmware components.	It is recommended to select individual components checkbox (either Firmware or Driver) when only one component type update is required.
209750	Firmware/Driver Management	If an MX7000 chassis firmware is downgraded, then, the associated job's status and details must be checked on the respective MX7000 as they are not available in OpenManage Enterprise.	
209728	Firmware/Driver Management	Baseline Version field in the Compliance report using local firmware catalogs shows as 'Update file not in catalog.' For the firmware catalogs generated using DRM versions lower than 3.3.2 and hosted on network shares with Windows 2019 and above, the Baseline Version field in the Compliance report using such catalog shows as 'Update file not in catalog'.	For local network shares using Windows 2019 and later, catalogs must be generated using Dell Repository Manager (DRM) version 3.3.2 and later.
208758	Firmware/Driver Management	OpenManage Enterprise supports UI internationalization, however, it is recommended that the functional content such as the file names and catalog content are entered only in English. Firmware compliance catalog with Japanese catalog file name in the path fails the connectivity test and fails to create catalog across CIFS , NFS , HTTP and HTTPS shares.	
185315	Firmware/Driver Management	Firmware compliance on multiple baselines logs CDEV9000 alerts for a single device with non associated firmware compliance baseline. 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.	
185312	Firmware/Driver Management	CDEV9000 non-compliance alert is logged for only one random device in the firmware baseline. 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.	
163175	Firmware/Driver Management	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.	
159958	Firmware/Driver Management	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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
159058	Firmware/Driver Management	AMD chipset driver update on the R6525 servers fails using OpenManage Enterprise Firmware/driver update feature.	Windows (64-bit) driver updates for R6525 AMD chipsets must be done manually outside of the appliance.
157887	Firmware/Driver Management	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.	
152092	Firmware/Driver Management	Appliance is unable to download the console upgrade from HTTP or HTTPS intranet share, when the intranet share address is blocked in proxy filtering.	If the upgrade download has a problem connecting through proxy, uncheck the proxy settings and then download.
151332	Firmware/Driver Management	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.	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.
146981	Firmware/Driver Management	All the existing firmware compliance tasks will refresh automatically post device discovery.	
146564	Firmware/Driver Management	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.	First upgrade the older iDRAC firmware versions to 2.40.40.40 before attempting an upgrade to iDRAC firmware version 2.63.60.61.
136820	Firmware/Driver Management	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.	
116172	Firmware/Driver Management	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.	
108218	Firmware/Driver Management	The **Update Firmware** button remains enabled even when there are no firmware catalogs available for upgrade or downgrade.	
	Firmware/Driver Management	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.	
165191	Inventory	Incorrect inventory data after moving sled from lead to member chassis. 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.	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.

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
160622	Inventory	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.	
75653	Inventory	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.	
	Jobs	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.	
161300	Multi-Chassis Management	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.	
168883	Multi-Chassis Management	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.	
161300	Multi-Chassis Management	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.	Discover the new Lead on OpenManage Enterprise.
153980	Networking	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.	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.
148789	Networking	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.	
102153	Networking	From the **All Devices** page, you cannot launch the iDRAC application interface with IPv6 addresses.	
	Networking	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.	
	Networking	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.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
	Networking	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.	
174851	Reports	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.	It is recommended to use a custom report to get only the virtual disk data if the VDs and PDs are not associated.
133201	Reports	Export of large firmware compliance reports, containing more than 200,000 elements, fails and the appliance displays an **Application timeout** error.	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.
194142	Scope Based Access Control	Alert policies and firmware baselines created by a device manager in 3.5 or earlier versions are only available to administrator users. 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.	
193698	Scope Based Access Control	Ownership information for device managers (AD/LDAP and OIDC) is lost on appliance upgrade. 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.	
210645	Scope Based Access Control (SBAC)	Any scheduled tasks must be rescheduled by the new Device Manager after transfer of ownership. After a transfer of ownership is executed, the new Device Manager must reschedule any tasks, such as the tasks for firmware updates, deployment of templates, alerts policies that were previously scheduled by the former Device Manager.	
197629	Scope Based Access Control (SBAC)	Global search count is greater than the actual result count for scope-restricted device managers. When a 'scoped' device manager uses Global Search, the total search count exceeds the actual items displayed.	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
194142	Scope Based Access Control (SBAC)	Alert policies and firmware baselines created by a device manager in 3.5 or earlier versions are only available to administrator users. 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.	
193698	Scope Based Access Control (SBAC)	Ownership information for device managers (AD/LDAP and OIDC) is lost on appliance upgrade. 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.	
193441	Scope Based Access Control (SBAC)	Run Inventory on Group is unavailable for Device Manager users. For the Device Manager users, **Run Inventory on Group** option under **Inventory** on the All Devices page is unavailable.	
192774	Scope Based Access Control (SBAC)	After upgrade, device managers can perform VLAN operation on in-scope proxied MX7000 sleds even when the chassis is out of scope. VLAN operation on in-scope 'proxied' MX7000 sleds is allowed for a device manager, even if the MX7000 chassis is out of scope.	
204172	Security	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.	
	Security	OpenManage Enterprise could be impacted by the Linux TCP SACK vulnerability (CVE-2019-11477).	
195183	User Management	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.]	
203928	User Management	AD group searches fail for an hour due to slow sync when AD/LDAP groups are added using the DNS option. 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.	
193717	User Management	If Ping Identity is used for OIDC provider, the appliance can only be used with Administrator role. With OIDC provider PingFederate, it is observed	

Table 2. Known issues (continued)

Issue ID	Functional area	Description	Workaround/Resolution
		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.	
210771	Warranty Management	In a pure IPv6 setup, the appliance is unable to retrieve the warranty issues from the support site.	Consider enabling IPv4 for routing purpose before initiating Warranty jobs.
176493	Warranty Management	With the Japanese version of the appliance, it is observed that the PDF export of the Warranty page contains illegible characters.	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.

Limitations

Table 3. Limitations

Functional area	Limitation
Appliance Localization	For the Japanese locale of OpenManage Enterprise, the date format displayed is in US 'short' date format instead of the Japanese format.
Appliance Upgrade	In a pure IPv6 network (without IPv4), the availability of any new upgrade version from dell.com, using online method, is not displayed on the **Console and Plugins** page.
Appliance Upgrade	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.
Configuration Management	When the internal share uses HTTPS, then, template creation, template deployment, Boot to Network ISO, and firmware updation are not supported on FX2, VRTX, and M1000e chassis.
Configuration Management	When the internal share uses HTTPS, then, template creation and deployment, and firmware updates are not supported on the CCD-discovered MX7000 sleds.
Configuration Management	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.
Configuration Management	RAID secure attributes are not supported on target devices during template or profile deployment.
Configuration Management	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.
Device Discovery	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.

Table 3. Limitations (continued)

Functional area	Limitation
General	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 : **/**, **?**, **.**, **>**, **<**, **"**, **:**, **;**, **|**, **]**, **}**, **{**, **[**, **-**, **=**, **~**, **`**, **(**, **^**, *****, **$**, **@**, **!**.
Inventory	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.
Reports	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.
Reports	Export of large firmware compliance reports, containing more than 200,000 elements, fails and the appliance displays the Application timeout error.

Environment and system requirements

For information about the environmental and system requirements for OpenManage Enterprise, see the *Dell EMC OpenManage Enterprise User's Guide* or the *Dell EMC OpenManage Enterprise Support Matrix*.

Support deprecation

OpenManage Essentials has reached both the End of Life as of December 2015 and End of Software Maintenance as of December 2018. The last release of OpenManage Essentials is version 2.5.

Dell EMC recommends managing your devices by using Dell EMC OpenManage Enterprise - the “next generation” of the OpenManage Essentials console. This ensures the latest features, best performance as well as the latest security updates and bug fixes.

Installation and upgrade considerations

For instructions on installing and upgrading of OpenManage Enterprise, see the *Dell EMC OpenManage Enterprise User's Guide*.

Where to get help

Dell Technologies maintains support pages for all products at www.dell.com/support.

The product support pages provide important information about the products. This information includes product and user documentation, knowledge base articles, drivers and other software installation packages downloads, advisories, knowledge base articles, and more.

A valid support contract and registration may be required to access all the information available on the product support sites.

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.