Dell EMC Update Manager 1.2

User's Guide

October 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

Introduction

Dell EMC Update Manger plug-in is an integrated solution for Dell EMC OpenManage Enterprise(OME) that allows IT administrators to create and manage repositories for PowerEdge devices that are managed in OpenManage Enterprise, which run iDRAC or Windows operating system. For more information about the supported PowerEdge devices, see the OpenManage Enterprise support matrix.

A repository consists of system bundles and their associated Dell Update Packages (DUP). A system bundle is a software collection that can be grouped to arrange the related updates that are applicable to same target platform and having the same format. A DUP is a self-contained executable file in a standard package format that updates a specific software element on Dell server or storage such as the BIOS, a device driver, firmware, and other similar software updates. These bundles and repositories allow the deployment of multiple firmware updates simultaneously. The Update Manager plug-in(UMP) supports DUPs in .exe format.

To update the systems with the latest firmware and software using Update Manager, do the following:

- Ensure that the repositories are up-to-date.
- Enable manual or automatic updates of the catalog present in the repositories.
- Customize a repository by importing or deleting update packages.
- Enable the option to view the baseline compliance report of the repository that is used to update the firmware of the components in the repository.

Topics:

Role-based privileges for Update Manager

The following table lists the permissions of the user roles for Update Manager:

Table 1. Role-based privileges for Update Manager

Functions	Administrator	Device Manager (DM)	Viewers
Install or uninstall Update Manager	Allowed	Not Allowed	Not Allowed
Enable or disable Update Manager	Allowed	Not Allowed	Not Allowed
Configure proxy	Allowed	Not Allowed	Not Allowed
Configure preferences	Allowed	Not Allowed	Not Allowed
Create repository	Allowed	Allowed	Not allowed
Import update package	Allowed	Allowed (owned by DM)	Not allowed
Delete repository or bundles or update packages	Allowed	Allowed (owned by DM)	Not allowed
Repository refresh	Allowed	Allowed (owned by DM)	Not allowed
View repository dashboard	Allowed	Allowed (owned by DM)	Allowed
View repositories	Allowed	Allowed (owned by DM)	Allowed
View or edit baseline compliance report from the **Repository** page.	Allowed	Allowed (owned by DM)	Not allowed

Role-based privileges for OpenManage Enterprise

The following table lists the OpenManage Enterprise features required for Update Manager users:

Table 2. Role-based privileges for OpenManage Enterprise

Functions	Administrator	Device Manager	Viewers
Update firmware with baseline compliance report	Allowed	Allowed (owned by DM)	Not allowed
Update Settings	Allowed	Not allowed	Not allowed
Create alert policy	Allowed	Allowed (owned by DM)	Not allowed

2

Install Update Manager

Update the Dell EMC OpenManage Enterprise(OME) settings to detect Update Manager plug-in in the OpenManage Enterprise console. You can download and install the Update Manager. Enables you to creates and maintain repositories of components along with their respective updates.

Topics:

Update OpenManage Enterprise settings for Update Manager

This section describes the updates that are performed on Dell EMC OpenManage Enterprise . You can update or install the supported plugins in Dell EMC OpenManage Enterprise.

Prerequisites

- Dell EMC OpenManage Enterprise 3.8 is installed.
- Internet connection is stable if the online source is selected for the updates.
- Download the **OpenManage_Enterprise_UpdateManager_1.2_A00.zip** file from dell.com if a network share is used as a source for the updates.

About this task

To configure the updates and detect the UMP plug-in, do the following:

Steps

1. Log in to the Dell EMC OpenManage Enterprise console.
2. Go to **Application Settings** > **Consoles and Plugins**.
3. Click **Update Settings**.
4. Select **Manual**. This option allows the manual check of updates from a specified source.

   NOTE: Automatic update is not supported for detecting Update Manager.

5. Select the source from where the updates must be applied:
   - **Dell.com**(online)—Checks for the availability of updates directly from https://downloads.dell.com/openmanage_enterprise.
   - **Network Share** (offline)—Checks for updates from a specified NFS, HTTP, or HTTPS path that contains the update package.
6. Click **Test Now** to validate connection to the specified network share.
7. Click **Apply**.
   Update Manager plug-in is detected.

   NOTE: Update Manager plug-in must be installed manually once detected.

Install Update Manager

Install the Update Manager plug-in in the Dell EMC OpenManage Enterprise console to create and maintain the repositories of components with their respective updates.

Prerequisites

Ensure you update OME settings for Update Manager through **consoles and plugins** tab.

About this task

To install Update Manager, perform the following steps:

Steps

1. Launch Dell EMC OpenManage Enterprise.
2. In **Application Settings**, click **Console and Plugins**.
3. In the **Plugins** section, click the **Install** option for Update Manager.
   The **Install Plugin** window is displayed.
4. Check for the latest available versions of update manager.
5. Click **Download Plugin**.
   Wait for the plug-in to download. The plug-in is downloaded, and the status of the download is displayed on a green color band on the top-right corner.
6. Click **Install Plugin**.
   Capture a snapshot of the OpenManage Enterprise appliance VM.
7. On the **Confirmation** wizard, select the checkbox to confirm that the snapshot is captured.
   The **Confirm Install** tab is enabled.
8. Click **Confirm Install** to start the installation.
   The Dell EMC OpenManage Enterprise appliance restarts. The restart pauses the scheduled job or the jobs in progress for few minutes and resumes once the appliance is active.
9. The Update manager plug-in is installed.

Next steps

Log in to the Dell EMC OpenManage Enterprise again and the **Update Management** is displayed under new navigation **Plugins**.

Upgrade Update Manager

Upgrade the Update Manager plug-in to the latest available version in the Dell EMC OpenManage Enterprise console.

Prerequisites

- Update manager version 1.2 is available on the OpenManage Enterprise version 3.8.
- Upgrade path of Update manager from version 1.1 to 1.2 or 1.0 to 1.2 are supported.
- Update manager version 1.1 is available on OpenManage Enterprise version 3.6 or 3.7 and OpenManage Enterprise is upgraded to OpenManage Enterprise version 3.8.
- Update manager version 1.0 is available on OpenManage Enterprise version 3.5 and OpenManage Enterprise is upgraded to OpenManage Enterprise version 3.8.
- Clear the browser cache and cookies before starting the upgrade process.

About this task

Perform the following steps to upgrade the Update Manager plug-in from previous version to the latest version:

Steps

1. From OpenManage Enterprise console, go to**Application Settings** > **Consoles and Plugins**.
2. Click **Update Settings**, and select the required fields. For more information, see Configure OME settings for Update Manager.

NOTE: Automatic update is not supported for detecting Update Manager.

3. Go to the Update Manager section on the **Consoles and Plugins** page, and click **Update Available**.
4. Click **Download Update**.
   The appliance restarts. The plug-in is updated and is in a disabled state.
5. Click **Enable** to enable the plug-in. For information, see Enable Update Manager.
   The update manager plug-in is upgraded to the latest version.

Next steps

NOTE: All the repositories and its associated content created using Update Manager version 1.0 are still available for use.

NOTE: When you migrate from UMP v1.0/OME v3.5 or UMP v1.1/OME v3.6, v3.7 to UMP v1.2/OME v3.8, the repository must be refreshed to use the latest catalog if the created repositories have PowerEdge servers supported with Windows server 2019 or above. Modifications are done in OpenManage Enterprise 3.8 to accommodate the new Microsoft build number system used in Windows Server 2019 or above.

NOTE: Update Manager version 1.1 and above supports SBAC functionality. Users with device manager privileges can view or edit repositories that are defined in the **User Scope**, during the creation of the device manager user. For more information about SBAC functionality, see **Dell EMC OpenManage Enterprise Version 3.6 User's Guide**.

NOTE: Only users with administrator privileges can see the repositories that are created by Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) users.

3

Configure Update Manager

This chapter describes that how you configure the Update Manager, or edit a proxy. You can manage the alerts, create alert policies and then manage the alert policies. You can view the running jobs, job types, and its details.

Topics:

Configure Update Manager preferences

About this task

The version limit of a repository and the storage space used by the plugin can be configured in the **Preferences** page.

Steps

1. From the OpenManage Enterprise home page, select **Plugins** > **Update Management** > **Settings**.
2. Click **Preferences**.
   The **Preferences** page is displayed.
3. In the **Versioning** option, select **Unlimited**, or **Maximum number of version** to set the maximum number of versions of a repository that can be stored.
   - **Unlimited**: This default option enables unlimited versions of a single repository to be stored.
   - **Maximum number of version**: Enter the maximum number of versions of a repository that can be stored. If the number of repository versions exceeds this value, the oldest version is automatically deleted.
4. **Storage Space Available** displays the total storage space that is dedicated for the Update Manager plugin. The value that is displayed is 20 percent of the total available storage in OpenManage Enterprise. **Storage Space Used** displays the total storage spaced used by the plugin.

   The **Storage Space Used** is only updated after any repository operation is complete.
5. In **Set Storage Limit** enter any whole number ranging from 10 GB to the value displayed in **Storage Space Available** to set the storage limit for the update manager plugin. Ensure that the value entered in **Set Storage Limit** is not lower than the value in **Storage Space Used**.

   It is recommended to not use the complete **Storage Space Available** when configuring this limit.

   An alert is generated if the **Storage Space Used** exceeds 80 percent of this configured limit. If the **Storage Space Used** exceeds this limit, a critical alert is generated and any repository operation in progress fails.

   The default value for this field is 25 GB.
6. Click **Apply**.

   If you want to restore the preferences to the previous values, click **Discard**.

Configure or edit a proxy

About this task

The Update Manager plugin allows the configuration of an OpenManage Enterprise proxy. If a proxy is configured on OpenManage Enterprise, it can be edited here, and then be used by OpenManage Enterprise.

Steps

1. From the OpenManage Enterprise home page, click **Plugins**, then **Update Manager** and then **Settings**.
   The **Network** page is displayed.
2. Click **Configure Proxy** or **Edit Proxy**.
3. Select **HTTP Enable Proxy settings** and enter the information in the **Proxy Address** and **Port Number** fields.
4. If the proxy requires authentication, select **Enable Proxy Authentication**, and then enter the credentials of the proxy.
5. Click **Apply**.

Transfer of ownership of Device Manager entities

Administrators can transfer entities such as repositories, baselines, jobs, firmware and configuration templates and baselines, and alert policies that are created by one device manager to another device manager. Administrators can initiate a transfer of ownership when a device manager leaves the organization.

Prerequisites

- No Update Manager specific jobs are in progress before the transfer of ownership of device manager entities, or before modifying the user scope of a device manager .
- Ensure you have the administrator user privileges to perform this task on OpenManage Enterprise.

About this task

If any repository refresh, create, import, or delete operation is in progress during the transfer of ownership, the baselines and jobs associated with the repositories will not be available to the user to which they have been transferred to.

NOTE:

- 'Transfer of ownership' transfers only the entities and not the device groups (scope) owned by a device manager to another.
- Before a transfer of ownership of entities is initiated, the administrator must first reassign the device groups owned by the former device manager to the device manager who will be taking over.
- If the ownership of the entities is transferred to an Active Directory user group, then the ownership is transferred to all the members of that AD group.

To transfer the ownership of entities such as jobs, baselines, firmware or configuration templates and baselines, and alert policies from one device manager to another, do the following:

Steps

1. From OpenManage Enterprise, go to **Application Settings** > **Users**.
2. Select the device manager user, and click **Transfer Ownership**.
3. From the **Source User** drop-down list, select the device manager from where the ownership of entities must be transferred.

   NOTE: The Source User lists only the local, active directory, OIDC, or deleted device managers with entities such as jobs, FW or configuration templates, alerts policies, and profiles associated with them.

4. From the **Target User** drop-down list, select the device manager where the entities are transferred to.
5. Click **Finish** and click **Yes** at the prompt message.

Results

All the owned entities such as repositories, baselines jobs, firmware or configuration templates, and alert policies are transferred from the **source** device manager to the **target** device manager.

Manage alerts

Alerts are generated when a repository is refreshed and when the repository storage exceeds the configured limit. Email alerts can also be configured for a repository refresh task.

View alert log

From OpenManage Enterprise, go to **Alerts**, and then click **Alert Logs** to view the generated alerts. By default, only the unacknowledged alerts are displayed.

Information about the alerts is provided in the following columns in the **Alert Logs**:

- **Alert**: Severity of an alert.
- **Acknowledge**: If the alert has been acknowledged a tick mark appears under **ACKNOWLEDGE**. Click between the square bracket under **ACKNOWLEDGE** to acknowledge or unacknowledge an alert.
- **Time**: The time at which the alert was generated.
- **Source name**: The source name is displayed as **N/A** for any alert generated by Update Manager.
  NOTE: The source name for an undiscovered device or an internal alert is IP address of the device that generated the alert. In this case, the alert cannot be filtered based on the source name.
- **Category**: The category indicates the type of alert, for audit, configuration or updates.
- **Message ID**: The ID of the generated alert.
- **Message**: The generated alert.
- The box on the right provides additional information such as the detailed description and recommended action for a selected alert.

Click any of these column headings to sort the alerts.

Filter the alerts by using **Advanced Filters**. The following additional information can be used to filter the alerts:

- **Start Date** or **End Date** of when the alert was generated.
- **Subcategory**: Subcategory of the alert.
  NOTE: To filter the alerts generated for a repository refresh task, select **Updates** in the **Category** drop-down list and then **Refresh Repository** in the **Subcategory** list.
- **User**: Allows to filter the alerts which have been acted upon by users with Administrator privileges.

Create an alert policy

About this task

Perform the following steps to create an alert policy for a repository refresh task:

NOTE: Alert policies created by any DM user in Update Manager version 1.0, are not accessible to the same Device Manager(DM) users after upgrading to Update Manager latest version. However, these alert policies are accessible to the Administrators only.

Steps

1. Go to **Alert** and click **Alert Policies**, and then click **Create**.
2. Enter a name and description for the alert policy and click **Next**. The **Enable Policy** check-box is selected by default.
3. Select **Update Manager** and click **Next**.
4. Select **Any Undiscovered Device** and click **Next**.
5. Specify the duration for when the alert policy is applicable by selecting the required values for **Date Range**, and **Days**, and then click **Next**.

   NOTE: This step is optional.

   NOTE: A time interval cannot be set for alert policies that are created for Update Manager.

6. Select the severity of the alert and click **Next**.
7. Select **Email** and specify the information in the fields and click **Next**.
   This option sends an email to the designated recipient. Update manager only supports email notifications.
   NOTE: Emails for multiple alerts of the same category, message ID, and content are triggered only once every 2 minutes to avoid repeated or redundant alert messages in the inbox.
8. Review the details of the created alert policy and click **Finish**.

Manage alert policies

After alert policies have been created on the Alert Policies page, they can be edited, enabled, disabled, and deleted. In addition, OpenManage Enterprise provides integrated alert policies that trigger associated actions when the alert is received. These integrated alert policies cannot be edited or deleted, but can be enabled or disabled.

To view the created alert policies go to **Alerts**, and then click **Alert Policies**. To select or clear all the alert policies, select the check box in the header of the table. Select one or multiple check boxes next to the alert policy to perform the following actions:

- **Edit**: Select an alert policy, and then click **Edit** to edit the required information in the Create Alert Policy dialog box.
- **Enable**: Select one or more alert policies, and then click **Enable**. A check mark appears under the **Enabled** column when an alert policy is enabled. The **Enable** button is deactivated for an alert policy that is already enabled.
- **Disable**: Select one or more alert policies, and then click **Disable**. The alert policy is disabled, and the check mark in the **ENABLED** column is removed. The **Disable** and **Edit** buttons are deactivated for an alert policy that is already disabled. Alert policies can also be disabled by clearing the **Enable** check box during alert policy creation.
- **Delete**: Select one more the alert policies, and then click **Delete**.

View Update Manager specific jobs

This section describes the different job types for Update Manager and how to view them.

View job lists

From OpenManage Enterprise, go to **Monitor** and then click **Jobs** to view the list of existing jobs. Information about the jobs is provided in the following columns:

- **Job Status**: Execution status of the job.
- **State**: If the job is enabled or disabled.
- **Job Name**: Name of the job.
- **Job Type**: The type of job. For more information, see Job Types.
- **Description**: Description of the job.
- **Last Run**: Date and time of when the job was last run.

Click any of these column headings to sort the jobs.

Filter the jobs by using **Advanced Filters**. The following additional information can be used to filter the jobs:

- **First run**: Filters all the jobs run after the specified date.
- **Source**: Select either **All**, **User generated**, or **System generated** jobs.

Job Types

Table 3. Job types in OpenManage Enterprise

Job Type	Description
UMP_Delete_Task	Displays the DUP and catalog delete jobs.
UMP_Download_Task	Displays the DUP and catalog download jobs for a created repository.
UMP_Import_Task	Displays import DUP jobs.
UMP_Update_Task	Displays DUP and catalog downloads for refresh jobs.

View individual job details

To view the details of a specific job, select a job and then click **View Details**. The following information is displayed:

- **Job Details**:

    - Provides the name, type, description, and status of the job.
    - Click **Restart Job** if the job status is **Stopped**, **Failed**, or **New**.
- **Execution History**:
    - Displays the time and duration of the job, and its percentage completion.
    - Filter the jobs by the status or the name of the target system in the **Advanced Filters** section.
- **Execution Details**: Lists the repositories on which the job was run and the time that is taken for the job.

The right side of the page displays the **Result** of the job and the **Messages** associated with it.

View audit logs

Audit logs list the actions that were performed on the devices that are monitored by OpenManage Enterprise. Log data can be used to help you or the Dell EMC support teams in troubleshooting and analysis. See Auditing and Logging for more information on the EEMI messages specific to Update Manager 1.1 and above.

To view the audit logs click **Monitor** and then **Audit Logs**. The details of each audit log are displayed in the following columns:

- **Severity**: The severity of the information in the log.
- **Time stamp**: The date and time when the action in the log is performed.
- **User**: The user who performed the actions recorded the log.
- **Message ID**: The ID of the generated log.
- **Source Address**: The IP address of the system which generated the log.
- **Category**: There are two categories of audit logs.
    - **Audit**: Generated when a user logs in or out of the OpenManage Enterprise appliance.
    - **Configuration**: Generated when any action is performed on a target device.
- **Description**: Description of the log.

Click any of the column headings to sort the audit logs.

Filter the audit logs by using **Advanced Filters**. The **Start Time** and **End Time** can be used to filter the audit logs generated during a specified period.

4

Create and view repositories

Topics:

Use an SUU ISO file to create a repository

About this task

This section describes how to use a Server Update Utility(SUU) ISO file to create a repository. If you do not want to use an SUU-based catalog, go to create a repository.

Steps

1. Download the required SUU ISO file from https://www.dell.com/support/. For more information, see *DELL EMC OpenManage Server Update Utility User's guide*.
2. Save the file to a network share. The supported network share types are NFS, CIFS, HTTP, and HTTPS.
3. Right-click the ISO image file, and extract it to the same network share using any extraction utility.
4. From the repository folder, copy the folder path of the **Catalog.xml** file.

   NOTE:
   - The version number of the **Catalog.xml** file is not displayed.
   - The filename of the **Catalog.xml** file cannot be changed.

5. In the Create Repository workflow, set **Base Catalog** to **Network Share** and enter the required information for **Share Address** and **Catalog File Path**.

   NOTE: The **Test Connection** option confirms whether OpenManage Enterprise has access to the location.

Create a repository

Prerequisites

- Ensure that you use either an online catalog or offline catalog generated from DRM v3.3.2 or above or SUU v 21.09.00 or above as latest base catalog, while creating a repository of device drivers from Dell devices, managed in-band with supported Operating System Windows server 2019 or above.
- The supported PowerEdge devices are discovered and managed in the OpenManage Enterprise.
- Internet connection is stable to access **downloads.dell.com**. If required, configure the proxy for OpenManage Enterprise.
- To use a SUU-based catalog, download the SUU ISO file to a network share, and extract the ISO file in the same location. For more information, see Use an SUU ISO file to create a repository.

NOTE: Repositories or baselines that are created by Active Directory(AD) or Lightweight Directory Access Protocol (LDAP) user in Update Manager version 1.0 are accessible only to the Administrators after upgrading to Update Manager version 1.1 and later.

Steps

1. From the OpenManage Enterprise home page click **Plugins**, and select **Update Management** > **Repository**.

2. Click **Create Repository** .
   The **Create Repository** window is displayed.
3. In the **General** section, provide the following details and click **Next**.

- **Name**: Provide a unique repository name within the 255 character limit and ensure that it has no special characters.
- **Description**: Provide a description for the repository and ensure that it does not exceed the 1024 character limit.
- **Baseline Name**: The baseline name is autopopulated with the name that is provided for the repository. It is recommended to change the baseline name as required.
- **Baseline Description**: The baseline description is autopopulated with the description that is provided for the repository. You can change the baseline description as required. Ensure that the description does not exceed the 500 character limit.
- **Base catalog**: Select either **Enterprise Server Catalog**, **Index Catalog** or **Network share** from the drop-down list.
  - **Enterprise Server Catalog**: Contains all the latest BIOS, drivers, and other firmware of the Dell Update Packages for Dell EMC PowerEdge servers and chassis. The latest version of the enterprise server catalog is selected by default.
  - **Index Catalog**: You can access solution-specific catalogs such as ESXi and MX Validated Stack, and also older versions of all Enterprise server catalogs. Select the type of catalog from the **Catalog Group** drop-down list. The latest version of the catalog is selected by default. The **Catalog** drop-down list shows the older versions of the selected catalog group. Select the version of the catalog required for the repository.
  - **Network Share**: This option allows you to select any custom Enterprise catalog from any offline network path. Select a catalog from a local network share from the **Share Type** list. The supported share types are NFS, CIFS, HTTP, and HTTPS.

    NOTE:
    - If the Dell update packages (DUPs) are present in same network share location as the custom catalog and you want the DUPs to be downloaded from offline share instead of **dell.com**, then ensure that the base location for the corresponding custom catalog is empty.
    - Catalogs with updatable components that are created using Dell EMC Repository Manager or Dell EMC Server update utility (SUU) based catalogs can also be used.
    - The supported formats for **Share Address** are IPv4, IPv6, and hostname. The supported format for **Catalog File Path** is `/directory/subdirectory/file` or `directory/subdirectory/file`. A schema validation is performed by selecting **Test Now**. To ensure that the file is well formed and there is no unwanted or corrupted data. Enter the values in the authentication options and select **Test Now** to test the network share connection.
    - The appliance may become unresponsive if the selected catalog fails to download. Refresh the browser to reload OpenManage Enterprise again.
- **Update catalog**: You can update the selected catalog manually or automatically.

  Set weekly or daily automatic updates using the **Update Frequency** drop-down list. Select the day, and time in the **HH:MM** field to specify the time for the automatic update.

  NOTE: Ensure that automatic updates are set to begin 24 hours after the repository is first created.

4. Select the devices or groups you require in the repository in the **Devices/Groups** section, and click **Next**. Users with device manager privileges can only view or select the groups that are selected by the administrator in the **User Scope** when creating that user. A lock icon is displayed next to the group name, for groups that are not accessible to the user with device manager privileges.
   - **All Devices**—Selects all the devices in the selected catalog.
   - **Device**—Selects the devices from a list of devices in the selected catalog. Click **All selected devices** to view the devices you have selected, and click **OK**.
   - **Groups**—Select a group or groups of devices available in the selected catalog and click **Ok**.

   The PowerEdge devices and the groups in which they are arranged is displayed on the left side of the **Select Device** and **Select Group** window. To refine your search, use **Advanced Filters**.
5. The **Summary** section provides the summary of previously entered information. Click **Finish** to create the repository.

Results

The created repository appears in the **Repository** and **Overview** pages. The **UMP_download_Task** job is triggered, which downloads the catalog and its associated DUPs of the repository. The downloaded catalog and DUPs are displayed in the **Messages** section of the job details page. The repository is unavailable until this download job is completed. The baseline appears in the **Firmware/Driver Compliance** page under **Configuration**.

The catalog version is displayed as **Network** in the **Overview** and the **Repository** page if the repository is created using a network share. The catalog versions are not displayed if the repository is created using a SUU catalog.

View repository details

The repositories are listed in the **Repository** page under **Update Management**. Users with administrator or viewer privileges can view all the repositories. Users with device manager privileges can only view the repositories that are created by the user.

NOTE: Repositories or baselines that are created by Active Directory(AD) or Lightweight Directory Access Protocol(LDAP) user in Update Manager version 1.0 are accessible only to the Administrators after upgrading to Update Manager version 1.1 and above. For more information see Transfer of Ownership Device Manager entities.

Expand the repository to view the device bundles and components present in the repository. Details of the repository are displayed in the following columns :

- **Name**: Name of the repository
- **Version number**: Repository version number.
- **Size**: Total size of the DUPs in the repository.
  NOTE:
  - The combined size of all the repositories may appear to exceed the total available storage. However, only one copy of a DUP is stored even if it is present in multiple repositories.
  - If an ESXi catalog is selected when creating the repository, the repository size is displayed as 0.

  .
- **Date modified**: Date and time at which the repository was modified.
- **Label**: Displays of importance of updates for each component. Expand the device bundles to view the components in each bundle.
  - **Critical**- The components must be updated immediately.
    NOTE: OpenManage Enterprise categorizes **Urgent** DUPs as **Critical**.
  - **Optional**- Component update is optional.
  - **Recommended**- Component update is recommended.
- **Description**: The description provided to the created repository.

Click **Name**, **Version**, or **Date Modified** to arrange the repositories according to the column headings.

Additional information for a selected repository is displayed on the right side of the page:

- **View Report** launches the compliance report of the components in the devices and bundles of the repository with its associated baseline in the **Firmware/Driver compliance** page. For more information, see check for firmware or driver updates for a device..
- **Edit**: Allows you to change the name, description, baseline name and baseline description of the repository. It is recommended to not edit the name of the baselines created using the update manager plugin from the **Firmware/Driver compliance** page.
- A doughnut chart summarizes the level of importance of the component updates.
- The number of components in the repository.
- The number of devices selected when creating the repository. Click the information icon next to **Devices** to view the name, IP address, and model of all the devices. Any devices that are added or removed after repository creation are not reflected in the **Devices** field.
- **Catalog Versions**: Version of the catalog from which the repository was created.
- **Available Catalog Version**: The latest available version of the catalog.
- All the versions of the repository.
- **Owner**: The user that created the repository.
- **Last Modified By**: The last user that made changes in the repository.

You can filter the repositories according to any of the following components using the **Advanced Filters** section:

- **Name**: Enter the name of device or component.
- **Criticality**: Select the importance of the component update from the drop-down menu.
  NOTE: OpenManage Enterprise categorizes **Urgent** DUPs as **Critical**.
- **Category**: Select the category of the component.
- **Type**: Select the type of update.

Expand the repositories once the filters are applied to view the filtered components. If the device bundle in any of the repositories does not satisfy the filtered criteria, a red bar is displayed below it.

The **Repository** page also supports the following functions:

- Delete one or multiple repositories and repository versions.
- Delete one or multiple repository bundles and update packages.
- Import an update package .
- Update the catalog associated with the repository.

View the repository dashboard

The Update Management **Overview** page contains the dashboard which displays all the existing repositories. Users with administrator or viewer privileges can view all the repositories. Users with device manager privileges can only view the repositories that are created by the user.

The following details of the repositories are displayed:

- The repository name.
- **Current version**: Displays the current repository version number. Click the version number to view the list of versions for a specific repository.
- The number of devices in the repository.
- The version of the catalog present in the repository.
- The number of components in the repository and the level of importance of their updates.

Click **View Repository** to view detailed information about the selected repository in the **Repository** page.

Check for firmware or driver updates for a device

About this task

This section describes how to check the compliance of each device in a baseline with its associated catalog. To check the compliance of the baseline created by Update Manager, perform the steps that are given below.

Steps

Select the repository and click **View Report**.

NOTE: The baseline compliance report is only generated for the latest version of the repository.

You are redirected to the **Firmware/Driver Compliance** page where the baseline compliance report is displayed with the following information:

- **COMPLIANCE LEVEL**: Indicates the compliance level of the firmware of a device with the associated baseline catalog.
  - **OK** —The firmware or driver version of a component in the device is the same as its associated baseline catalog.
  - **Critical** —The firmware or driver version of a component in the device is not compliant with the baseline catalog, and so it must be updated immediately.
  - **Warning** —The firmware or driver version of a component in the device is not compliant with the baseline, and so it must be upgraded.
  - **Downgrade** —The firmware or driver version of a component in the device is newer than the baseline version.
- **TYPE**: Type of device for which the compliance report is generated.
- **DEVICE NAME/COMPONENTS**: By default, the service tag of the device is displayed. Click the device name to view the list of components and their compliance with the latest catalog.
  NOTE: For all the devices (except the MX7000 chassis) which are compliant with their associate firmware baseline, the device name is not displayed.
- **SERVICE TAG**: Click the service tag number to view complete information about the device on the **<device name>** page.
- **REBOOT REQ**: Indicates if the device must be restarted after updating the firmware.
- **Info** : The icon corresponding to every device component is linked to the support site page from where the firmware/driver can be updated.
- **CURRENT VERSION**: Indicates the current firmware version of the device.
- **BASELINE VERSION**: Indicates the corresponding firmware and driver version of the device available in the associated catalog.

To search for a device or component, select or enter the information in the **Advanced Filters** section.

Results

This baseline compliance report can be used to update the firmware and drivers of devices and components that are associated with the baseline. For more information, see *Dell EMC OpenManage Enterprise Version 3.6 User's Guide*.

NOTE: The view report option is disabled, or might produce an inaccurate baseline compliance report in the following scenarios:

- If the baselines created using the update manager plugin are modified or deleted.
- If a baseline has the same name as another repository containing another catalog.

NOTE: If the baselines are edited in the **Fimrware/Driver Compliance** page, then the changes are not reflected in the Update Manager plugin. The repository functions will not work for the repositories that contain the edited baseline.

Update firmware and drivers using a baseline compliance report

Prerequisites

- If HTTP and HTTPS shares were configured using the proxy settings, ensure that these local URLs are in the proxy exception list before initiating any update tasks.
- Only one update task can be initiated on the target machine at a given time.

About this task

A baseline compliance report can be used to update the firmware or drivers of a device or component associated with the baseline.

Steps

1. Click **View Report** for the baseline containing the device to be updated.
2. Check the compliance level of one or more devices or components, and then select the corresponding check boxes.
   If required, use **Advanced Filters** to specify the device or component. To select all of the check boxes, select the check box in the column heading.
3. Click **Make Compliant**.
4. Under **Schedule Update** select either:
   - **Update Now**: To apply the firmware or driver updates immediately.
   - **Schedule Later**: To specify a date and time when the firmware or driver version must be updated. This mode is recommended if you do not want to disturb your current tasks.
5. Under **Server Options** select either:
   - **Reboot server immediately**: Reboots the server after firmware or driver update.
   - **Stage for next server reboot**: Updates the firmware or driver when the server reboots next time.
     NOTE: If the firmware/driver update jobs are created using this option, then the inventory and baseline check must be performed manually after the package is installed in the remote device.
6. Select **Reset iDRAC** to initiate a reboot of iDRAC before the update job is initiated.
   NOTE: This function is not supported for updating the drivers.
7. Select **Clear Job Queue** to delete all the jobs on the target device, before the update job is initiated.
8. Click **Update**.

5

Manage repositories

The following repository functions are supported by Update Manager:

- Import update packages to repositories or device bundles.
- Delete repositories
- Delete device bundles and update packages.
- Refresh a repository.

No other operations are allowed when the jobs for any of these functions are in progress.

Repository versioning- Any of the above actions, except for repository deletion, results in the creation of a new version of the repository with the version number incremented by 0.01. Refresh the browser or go to another page if the repository version is not updated. The number of versions any repository can have depends on the limit configured in update management preferences.

Ensure that no Update Manager specific jobs are in progress before the transfer of ownership of device manager entities, or before modifying the user scope of a device manager.

NOTE: The change in repository version number is not reflected in the Audit logs. To see the latest version of the repository go the **Overview** or **Repository** page.

Topics:

Import an update package

About this task

An update package can be imported only from a local path to one or multiple repositories or device bundles. Update packages only with the file format .EXE are supported.

Steps

1. From OpenManage Enterprise, go to **Update Management**, and then click **Repository**.
2. Select the repository or bundle to which the update package must be imported and click **Import**.
   - To select all the repositories, select the check box to the left of **Name**.
   - To select one or more repositories, select the check box next to a repository.
   - To select one or more bundles, expand the repository and select the check box next to the device.
3. Click **Browse** and select the update package from the local system.

   If an update package is not applicable to a device or repository, then an error message is displayed.

   NOTE:
   - The import operation is not successful if the update package does not have a valid signature.
   - It is recommended to not change the file name of the DUP to be imported.
   - The import of DUP fails if you create repository for a PowerEdge server, and later delete all the devices of the supported PowerEdge server from Dell EMC OpenManage Enterprise (OME).
4. Click **Finish** after the import job is completed.

Results

After the import job is successfully completed, the baseline and catalog of the repository are also updated. The repository is updated and its version is incremented by 0.01.

If the same type of update package is present in the repository, it is replaced with the imported update package. If the update package is exactly the same as another update package in the repository, then no changes are made to the repository.

Delete a repository

About this task

Perform the following steps to delete a repository.

Steps

1. From **Plugins**, go to **Update Management** and then click **Repository**.
2. Select one or multiple repositories and click **Delete**.
3. Select the specific versions of the repository to be deleted or select **All Versions**.
4. Click **Delete**.

Results

Once the delete job is successful, the repository is deleted and is no longer displayed in the **Overview** or **Repository** page. The baselines and catalogs that are created using the repository are also deleted from the **Firmware/Driver Compliance** page.

Delete device bundles or update packages

About this task

Perform the following tasks to delete device bundles or update packages from a repository.

Steps

1. From **Plugins** go to **Update Management** and then click **Repository**,
2. Select the device bundles or update packages.
   - Select one or multiple device bundles by expanding the repository and selecting the check box next to the bundle.
   - Select one or multiple update packages by expanding the device bundle and selecting the check box next to the component.
3. Click **Delete**.
4. Select the check box in the **Delete** window to delete the update packages from all the existing bundles.
5. Click **Delete**.

Results

The device bundles or update packages are deleted from the repository. The repository is updated and its version is incremented by 0.01.

Refresh a repository

A repository refresh task replaces the catalog present in the repository with the latest available version. For a user with device manager privileges, the refresh task will also update the devices or groups present in the repository, based on the user scope assigned to the user. A repository refresh task replaces the catalog present in the repository with the latest available version.

Prerequisites

Ensure that the repository has sufficient storage space. See delete repository or component to manage repository storage space.

About this task

A repository must be refreshed in any one of the following scenarios:

NOTE: Only the latest version of a repository can be refreshed.

- When the base catalog is refreshed to a new catalog version.
- When Dell devices are added or removed from the groups, used for repository creation.
- When any of the groups used for repository creation is removed from repository owner's scope.
- When the scope is changed for a user with device manager privileges.
- When Dell devices are added or removed from the **Devices** section in OpenManage Enterprise.

You can refresh the catalog automatically or manually. Select the automatic refresh schedule when a repository is created. When the automatic refresh task is complete, the **Last Run Date/Time** and **Next Run Date/Time** display on the jobs page for the selected refresh job.

To manually refresh a repository, perform the following steps:

Steps

1. From **Plugins** go to **Update Management** and the click **Repository**.
2. Select the check box next to the repository.
3. Go to the right side of the page and click on the icon next to **Last Updated**.

   The date and time of the last catalog update is displayed if the catalog was previously updated.

Results

The catalog that is associated with the repository is updated to the latest available version at the default repository location in OpenManage Enterprise. The catalog version is also updated in the **Catalog Management** page under **Firmware/Driver** compliance. The latest baseline and update packages are used to generate a baseline compliance report. The repository is updated and its version increments by 0.01.

- If any device bundles or update packages were previously deleted, the repository refresh job updates the repository along with the deleted bundles and update packages. The new version of the generated catalog contains the details of the deleted components, and the same catalog is used to generate the compliance report.
- If you add or remove devices from a group, or components from a device in OpenManage Enterprise before the refresh operation, the changes are reflected in the repository after it is refreshed.
- The repository does not refresh successfully if there is insufficient storage space, and the respective alert and audit logs are generated.
- If all the groups or devices associated with a repository are removed from the repository owner's scope, then the refresh job task fails with an error message, **No devices found to perform refresh**. No new versions get created as there is no data available for this repository. The older versions of repositories will still be retained, and can be deleted manually.
- If an administrator changes the role of Device manager (DM) to Viewer, then the demoted user loses access to all owned entities like repositories and baselines. Since, the repository owner has become a Viewer, the subsequent refresh task on that repository fails.

NOTE: For users with device manager privileges, if any groups present in the repository are removed from the **User Scope** by the administrator, they will not reflect in the repository after it is refreshed.

NOTE: Scope changes made to a device manager user is only reflected on the latest version of the repository.

NOTE: If all the device groups are removed from the assigned scope for a device manager user, the repository refresh job fails.

6

Maintain update manager

Topics:

Disable Update Manager

Steps

1. Click **Application Settings** and then **Consoles and Plugins**.
2. Go to the **Update Manager** section and click **Disable**.
3. Click **Disable Plugin**.
4. Select the check box in the **Confirmation** window and then click **Confirm Disable**.

Results

The appliance restarts and no longer contains **Update Management** under the **Plugins** section. The baselines created by Update Manager are available for use even when the plugin is disabled.

Enable Update Manager

About this task

Once the plugin is disabled, it can be enabled by performing the following steps:

Steps

1. Click **Application Settings** and then **Consoles and Plugins**.
2. Go to the **Update Manager** section and click **Enable**.
3. Click **Enable Plugin**.
4. Select the check box in the **Confirmation** window and then click **Confirm Enable**.

Results

The appliance restarts, and **Update Management** now appears under the **Plugins** section.

Uninstall Update Manager

Steps

1. Click **Application Settings** and then **Consoles and Plugins**.
2. Go to the **Update Manager** section and click **Uninstall**.
3. Click **Uninstall Plugin**.
4. Select the check box in the **Confirmation** window and click **Confirm Uninstall**.

Results

The appliance restarts and **Update Management** no longer appears in the **Plugins** section. Once the plugin is uninstalled, all the catalogs and baselines created by the plugin are cleared and are no longer available for use.

7

Auditing and logging

Update Manager lists all the actions that are performed on the monitored devices in audit logs. Use the OpenManage Enterprise console to generate the audit logs with all the relevant information. You can export the audit log files to a CSV file format. The following table lists all the EEMI message details that are used in Update Manager.

Table 4. EEMI messages in Update Manager

Message ID	Message Description
CUMP0001	The repository <repoName> is refreshed successfully.
CUMP0002	Unable to refresh the repository <repoName>.
CUMP0003	Repository has exceeded the configured storage limit.
CUMP0004	Unable to create the repository <repoName>.
CUMP0005	Unable to delete the repository <repoName>.
CUMP0008	Unable to import the update package into the repository <repoName>.
CUMP0011	The repository <repoName> is created successfully.
CUMP0012	The repository <repoName> is updated successfully.
CUMP0013	The repository <repoName> is deleted successfully.
CUMP0014	The configuration data is successfully updated.
CUMP0015	An update package is available for the selected catalog.
CUMP0016	An update package is unavailable for the selected catalog.
CUMP0017	The catalog <catalogName> is updated successfully.
CUMP0018	Unable to update the catalog <catalogName>.
CUMP0019	The storage space has reached or exceeded 80% of the configured value.
CUMP0020	Unable to create the repository version because the maximum number of versions are already created.
CUMP0021	The repository version <version number> of repository <repository name> is deleted successfully.
CUMP0022	The repository bundle(s) or component(s) of repository <repository name> is deleted successfully.
CUMP0023	The repository version <version number> of repository <repository name> is created successfully after performing the <task name> operation.
CUMP0024	The repository <repository name> is edited successfully.