DELL Technologies

Whitepaper

Performing System Update using Dell EMC OpenManage integration for Microsoft System Center Configuration Manager and System Center Virtual Machine Manager

Abstract

OMIMSSC is an extension for Microsoft System Centre suite of products like SCCM and SCVMM that enables complete lifecycle management of Dell EMC devices. This whitepaper explains how OMIMSSC can help you schedule, and update firmware of components present in remotely managed Dell devices. This solution can be used for infrastructure built on certified Dell EMC PowerEdge Servers, Modular systems, Storage Spaces Direct Ready Nodes, and Microsoft System Centre for Virtual Machine Manager (SCVMM) or Configuration Manager (SCCM).

August 2020

Revisions

Date	Description
August 2020	Initial draft created.
August 25 2020	Editorial review by IDD.

Acknowledgments

This whitepaper was authored by:

- Sharu Sharma

Table of contents

Executive Summary

Firmware is the software program or set of instructions that provides low-level control for specific hardware, like RAID controllers, NIC adaptors, ethernet controllers, BIOS, power supply units, etc. To maintain optimum performance of these devices, it is necessary to keep their firmware up to date or use the recommended version. Updating firmware in a datacenter is a challenge as the IT administrator needs to manually perform the update on a large number of devices.

System Update updates firmware for various components like iDRAC, RAID, NIC, and BIOS on a Dell EMC device. Systems Management consoles like OMIMSSC help the administrator to update firmware remotely on multiple devices at the same time. OMIMSSC abstracts the process by automating the firmware update with simplified workflows and thereby reducing the solution downtime.

This document provides detailed information about the solution deployment workflows available in OMIMSSC.

1. Introduction to OMIMSSC

OMIMSSC is a virtual appliance that provides complete lifecycle management of Dell devices like servers, chassis, modular systems, and networking switches in a cloud environment when managed by Microsoft System Center.

OMIMSSC offers feature like operating system deployment, storage spaces direct cluster creation, hardware patching, firmware update, and maintenance of devices.

OMIMSSC can be downloaded from Dell support site (https://www.dell.com/support). For information on OMIMSSC download, installation, and setup instructions refer product manuals referred in resource section A.1

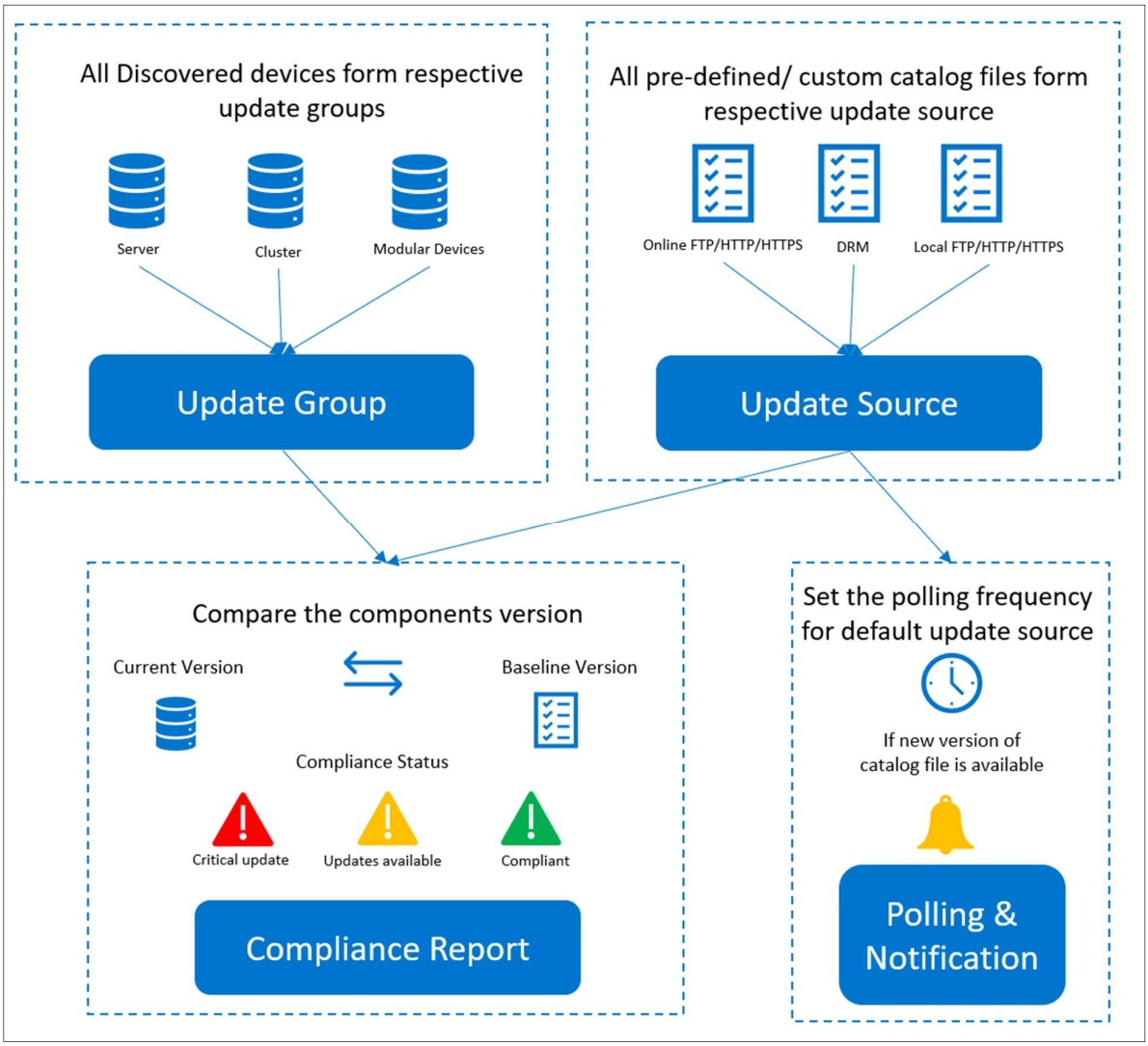
For information about SCCM and SCVMM, see the Microsoft documentation in the reference section A.

1.1. Solution Prerequisite

Components	Version
Management Application	Dell EMC OMIMSSC Appliance version 7.0 or later
Microsoft Consoles (Management System)	• SCVMM (2012, 2016, 2019) • SCCM (2012, 1902) etc.
Managed Node (Server Models)	• Dell EMC PowerEdge Server • Dell EMC MX Series • Dell EMC PowerEdge Storage Spaces Direct Ready Nodes

2. System Update Architecture

To relate to the remote system update, following terminologies will help you to understand various components used in the flow.



- **Update Sources**: Sources of the latest firmware for your discovered devices. This also acts as baseline for future updates.
  - Online: FTP, HTTP, or HTTPS
  - Offline: Local network FTP, HTTP, or HTTPS share, DRM
- **Update Groups**: Groups of devices created for bulk firmware updates.
  - Predefined Update Group - a read-only **Update** group which cannot be modified, created, or deleted.
  - Custom Update Group - a custom group which can be created, modified, and deleted by the user.

The following groups are created after a fresh installation of OMIMSSC:

- Default Host Group – servers that are running Windows or are synchronized with a registered Microsoft console.
- Default unassigned Group – all the unassigned, or bare-metal servers.
- Default non-windows host group – servers that are running operating systems other than Windows.
- Chassis Update Group – one group created for every modular server.
- Cluster Update Group – one group created for every windows failover cluster which contains all their nodes.

Recommendation: Performing updates on a batch of servers could be for a site-based maintenance or maintenance of specific systems. You need to create custom group for these batch of servers and perform non-complaint update remediation on individual groups.

- **Compliance Report:** The statistical report comparing the components in the Update Source to your discovered devices. The Available Updates icon indicator color is based on the criticality of the update. OMIMSSC has defined three colors for the same:
  - **Red:** One or more critical update required in a server or selected update group.
  - **Yellow:** No critical updates but few recommended updates available.
  - **Green:** All firmware versions are up to date.

Polling & Notifications: To identify whether there is any latest update source being published by Dell EMC.

2.1. Understanding the Solution

OMIMSSC uses WSMAN command to connect with remote systems, ensure the require outbound ports are open on your system.

You can schedule your update task or run it immediately. Time required to finish this update task depends upon number of devices in upgrade group and total number of components for these devices. Make use of **Jobs & Logs** page to view the progress of the specific update task. Once the task finishes, refresh the inventory to see the latest compliance.

Other key points:

- While updating certain components the server requires intermittent restart which is internally handled by the iDRAC and the DUP (Dell Update Package)
- Firmware update job will FAIL if the operation fails on even one device of the update group.

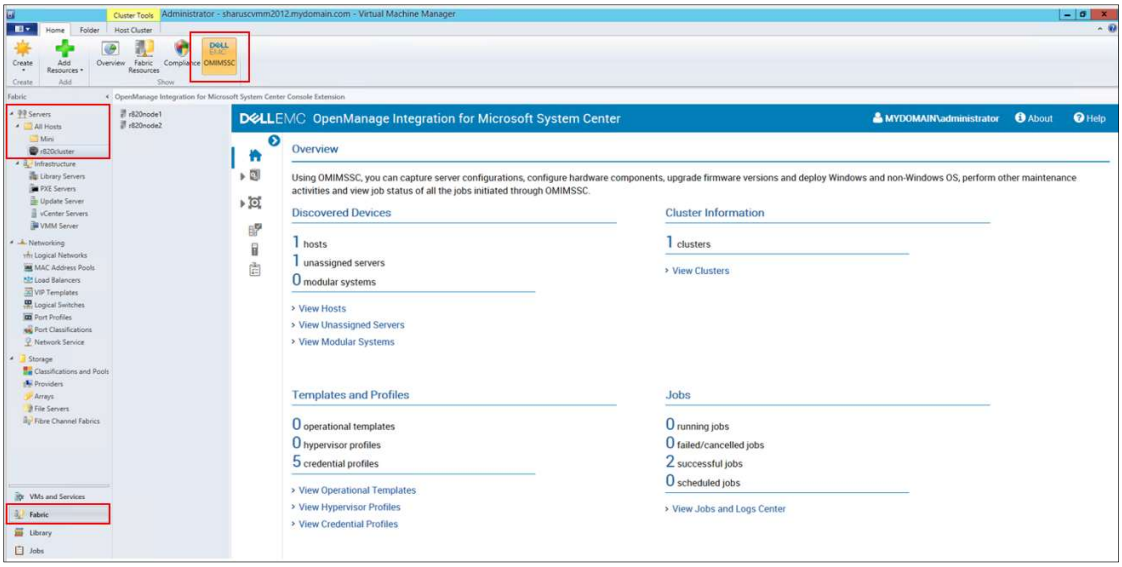
3. Configure the OMIMSSC appliance in SCCM &SCVMM

You can access the OMIMSSC console from SCCM or SCVMM.

3.1 Access the OMIMSSC Appliance

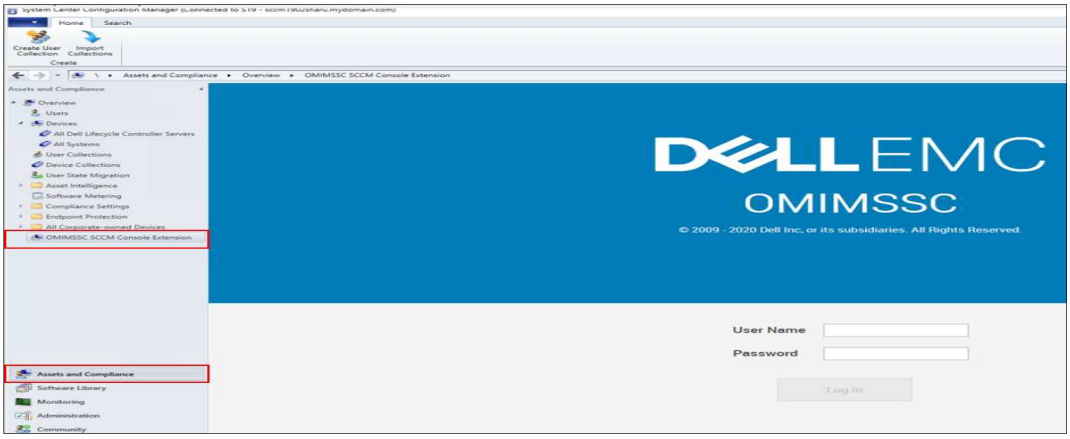
3.1.1. In SCVMM

Ensure you have the OMIMSSC's SCVMM extension installed and configured in your instance of SCVMM. You will see a new icon on the top header for **All Hosts** under the **Fabric** section. Click on the **Dell EMC OMIMSSC** icon to launch this integrated console.



3.1.2. In SCCM

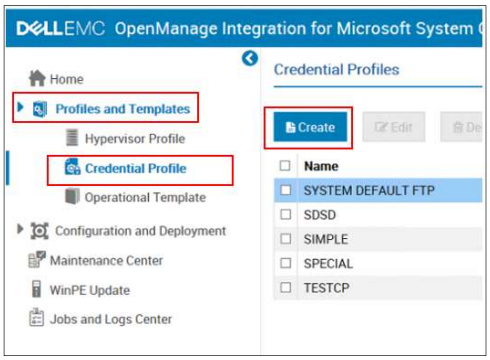
Ensure you have the OMIMSSC's SCCM extension installed and configured in your instance of SCCM. You will find **OMIMSSC SCCM Console Extension** option under **Assets and Compliance** section.



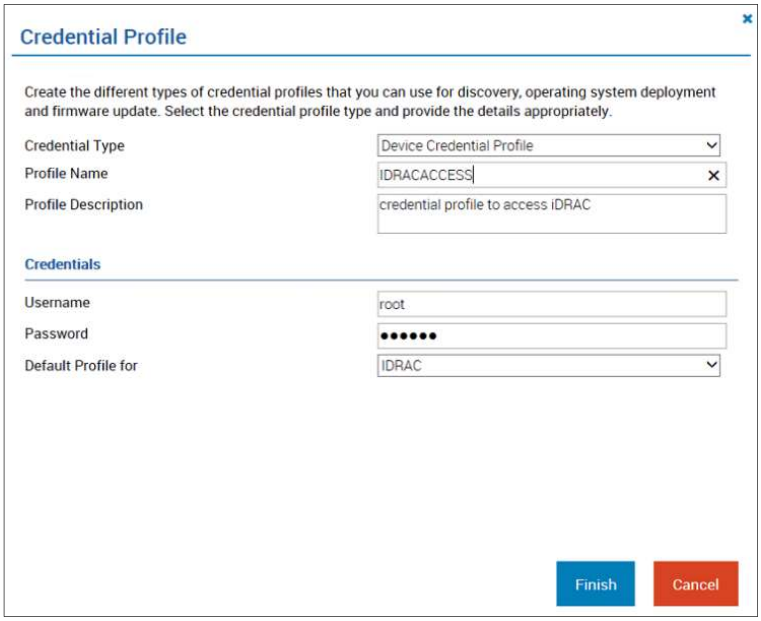
3.2 Configure Credential Profile

You will have to create a Credential Profile to discover your remote devices. A Credential Profile contains the username and password that are used to access a system or device. Create a Device credential profile that is applicable to remote iDRAC(s). Perform the following steps:

1. Expand **Profiles and Templates** tab in the OMIMSSC Appliance left menu
2. Click **Credential Profile**
3. Click **Create**



4. Fill up the form and click **Finish**.

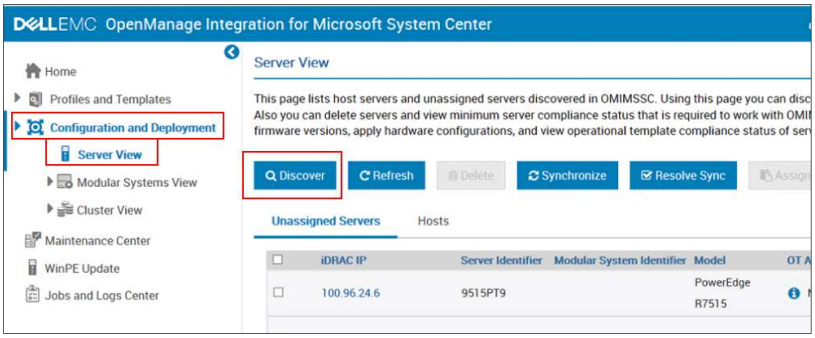


3.3 Discover the devices to be managed (Servers and Modular System)

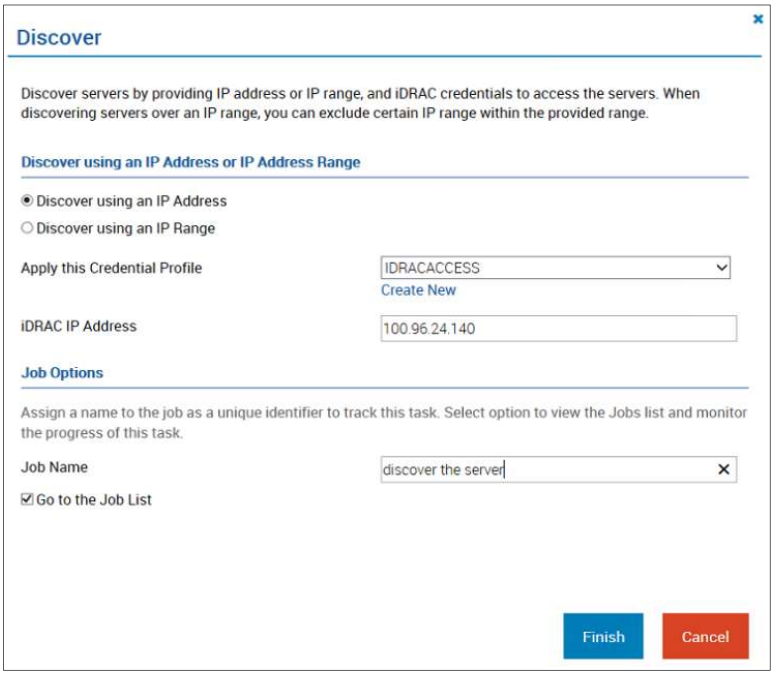
Use iDRAC IP address of the devices to discover systems that need to be managed. To discover a server or modular system perform the following steps:

1. In the left menu, expand **Configuration and Deployment** tab

2. Click **Server View** (when you want to discover a server) or **Modular System View** (when you want to discover a Modular system).
3. Click **Discover**

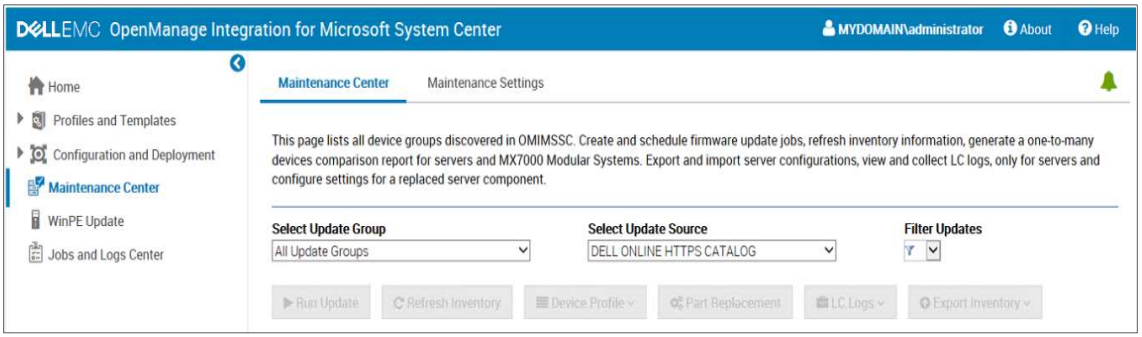


4. Fill in the form. You have an option to discover a single server or a sequence of servers and then click **Finish**.



3.4 Maintenance Settings

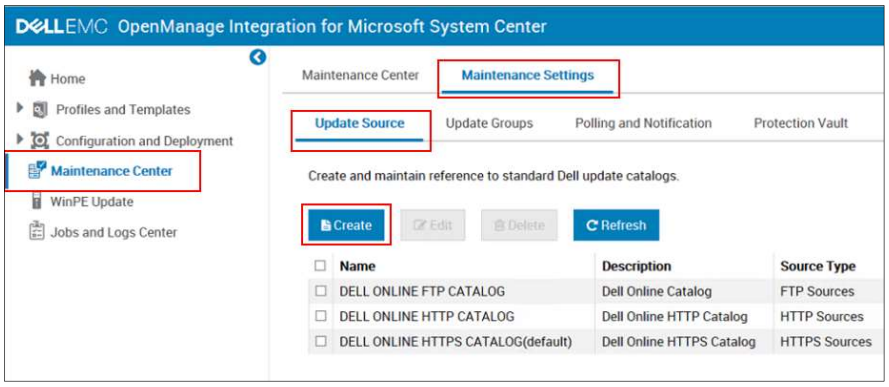
This page has a separate tab for Maintenance Settings where the Update Groups, Update Source, Pooling and Notification configurations will be available.



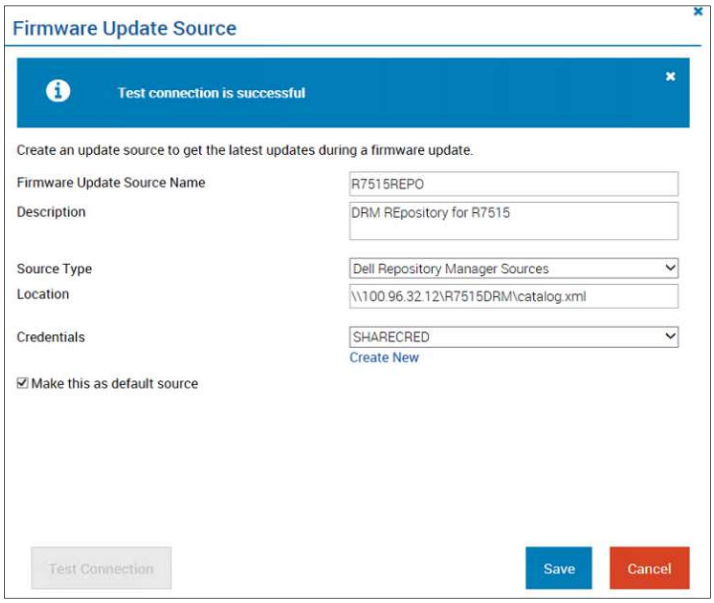
3.4.1 Configure the Update Source

Under Maintenance Settings you can either create a new update source or edit the existing available update sources. Let us create a new DRM update source in this section. Perform the following steps:

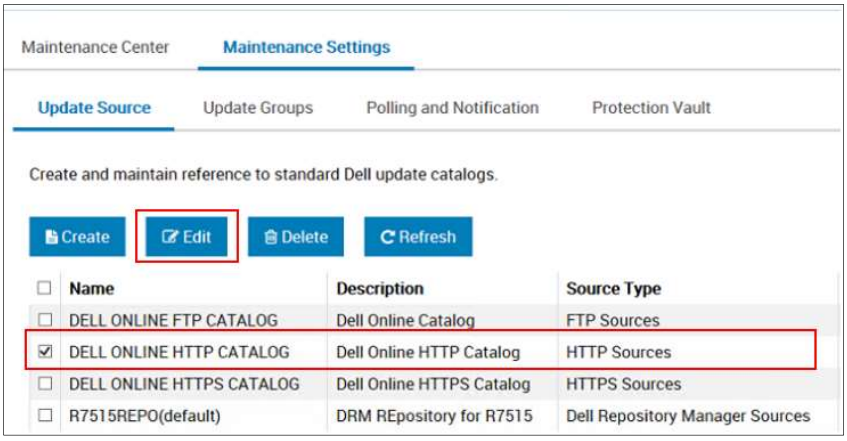
1. Switch to **Maintenance Settings** Tab
2. Under **Update Source** subcategory, click **Create**.



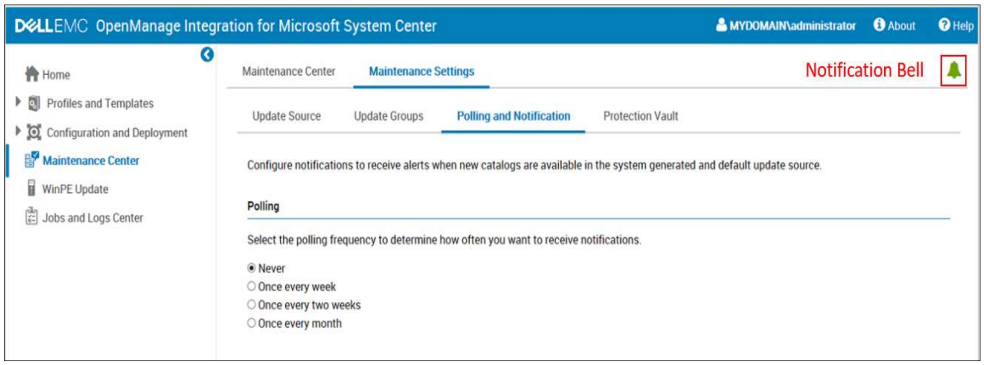
3. For creating a DRM update source, select the **Source Type** as Dell Repository Manager Sources.
4. In **Location**, provide the windows share location for DRM. For FTP or HTTP or HTTPS provide the URL of the update source.
5. In **Credentials**, select the credential profile that has access to the update source. For Source Type as HTTP or HTTPS or FTP, if proxy is required to access its location add the **Proxy Credential.**
6. If you wish to configure the Polling and Notification feature for this update source, you need to select the **Make this as default source** check box**.**
7. To verify that the location of the update source is reachable by using the mentioned credentials, click **Test Connection,** and then click **Save.**



Note: Before **viewing** the Compliance Report, it is recommended to **Edit** the update source and run **Test Connection** on the selected update source.



8. **Configuring Polling Frequency** for the **Default Update** source to receive alerts when there is a new catalog file available. The color of the notification bell changes to **Orange** when there is a new catalog file available. Click the bell icon to refresh the inventory. **Green** notification bell signifies an updated or latest catalog file.

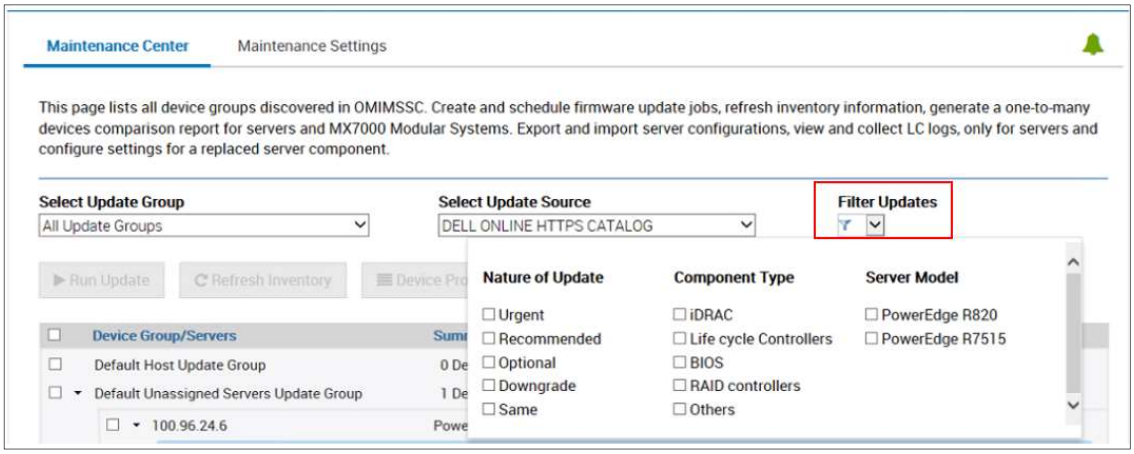


OMIMSSC gives you the following time frequency for the polling:

- **Never –** (Default) never receives any updates.
- **Once a Week –** receives updates about new catalogs every week.
- **Once every 2 Weeks –** receive updates about new catalogs every two weeks.
- **Once a month –** receive updates about new catalogs every month.

3.4.2 View Compliance Report

Let us check the component level compliance report of the server against the newly created DRM update source. After expanding the server level details, we have an option to either select the entire update group or to select a server. We can also select only those components where the updates will be applied.

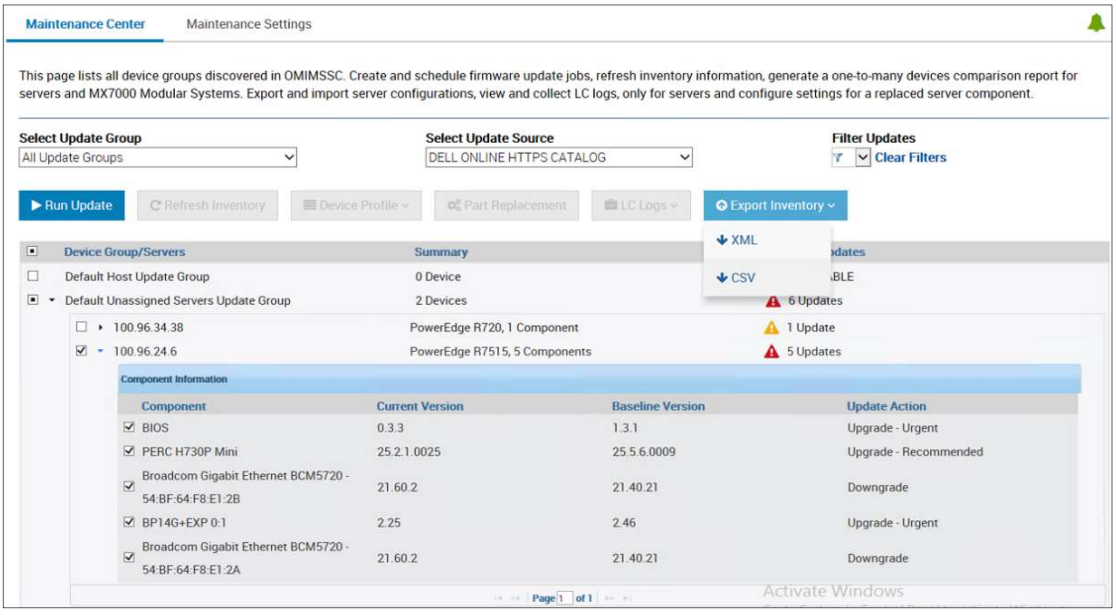


OMIMSSC supports three kind of filters:

- **Nature of the Update –** filter based on type of updates.
- **Component Type –** filter based on different components present in the servers discovered by the appliance.
- **Server Model –** filter based on the model of the servers discovered by the appliance).

Example: If you wish to install only the critical BIOS firmware updates on all your R820 servers, then select 'Urgent' as the Nature of Update, 'BIOS' as Component Type and 'PowerEdge R820' as Server Model.

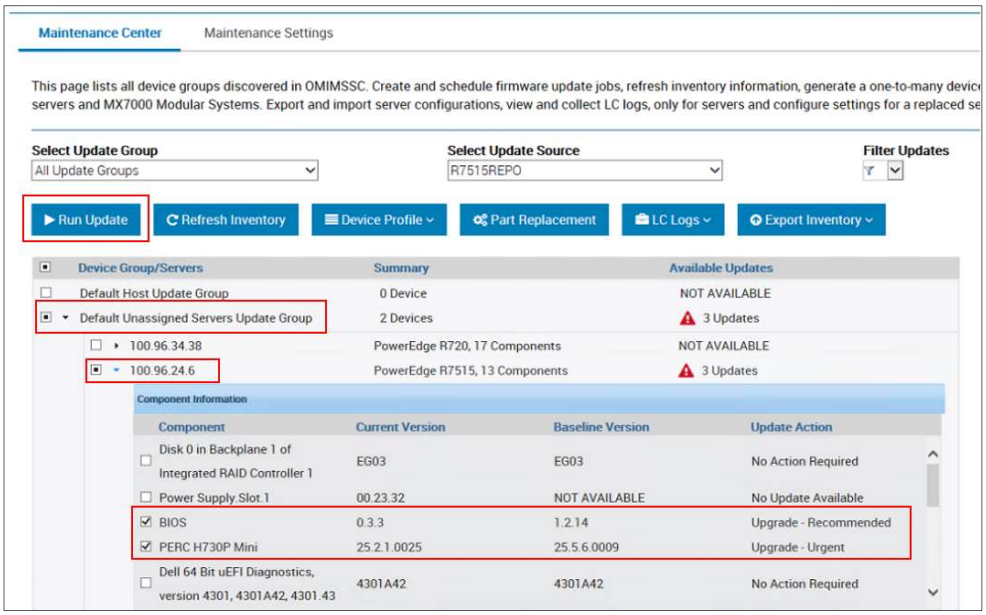
Best Practice: To plan your update, add a filter to select only the Urgent, Recommended, Optional, and Downgrade. Next, select the user group or the server, and then click **Export Inventory.** Then select either CSV or XML.



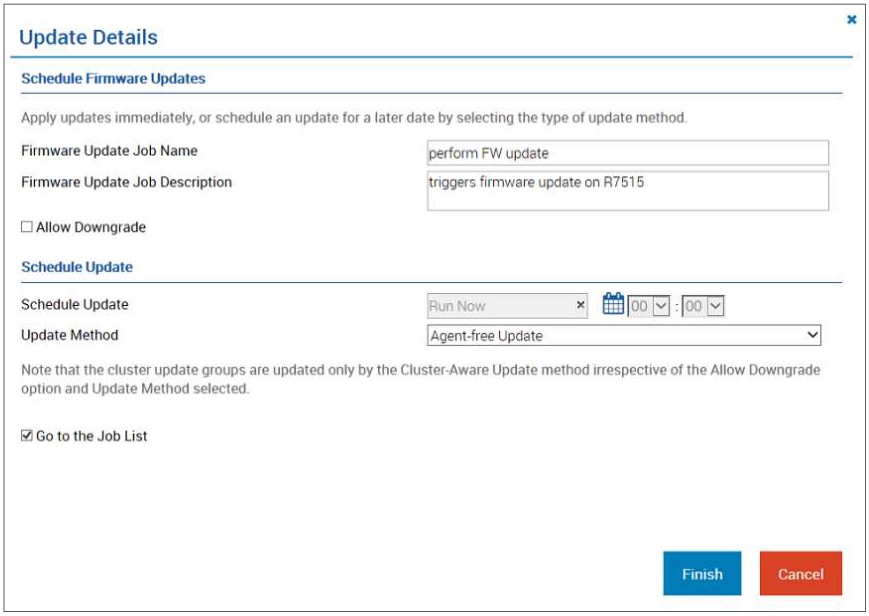
3.4.3 Run the Firmware Update Job

The final step is to trigger the Firmware Update Task from OMIMSSC Maintenance Center page. Perform the following steps:

1. Select the server or modular system update group, and an Update Source, then click **Run Update.**

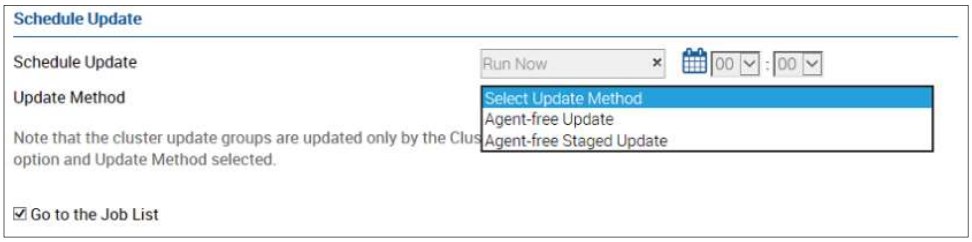


2. In **Update Details,** provide the firmware update job name and description.



3. It's not recommended to downgrade a given firmware version but if there are unavoidable reasons, you can select **Allow Downgrade** checkbox. If this option is not selected, then no action is performed on the component that requires a firmware downgrade.

4. In **Schedule Update**, select one of the following:
   - Run Now – to apply the updates immediately
   - Schedule – to apply the updates at a selected date and time.
5. Select the required update method:
   - **Agent-Free Staged Update –** In this method, the updates that do require any restart are applied first, and the updates that require a restart are applied when the system restarts.
   - **Agent-Free Update** – In this method, all the updates are applied together, and then the system restarts.



6. Click **Finish**

4. Troubleshooting tips

This section has all the troubleshooting information related to update sources, update groups, repositories and inventory after update.

- Failure of creation of update source

  When the Domain Name System (DNS) network configuration of the appliance is changed, creation of HTTP or HTTPS or FTP type update source fails.

  Resolution: Restart the appliance, and then create the update source.

- Failure to connect to FTP using default update source.

  After setting up and configuring, upgrading, or migrating when you try to access the FTP site using the default update source Dell Online Catalog it may fail if proxy credentials are required.

  Resolution: Edit the update source to add the proxy credentials.

- Failure of test connection for local update source

  After providing the details of a local update source, the test connection may fail as the required files may be not accessible.

  Resolution: Ensure that catalog.gz file is present in the following folder structure:

  For local **HTTPS**: *https:\\IP address\catalog\catalog.gz*

  For local **FTP**: *ftp:\\IP address\catalog\catalog.gz*

  For local **DRM**: *\\IP address\catalog\<catalogfile>.gz*

- Failure to create DRM update Source

  Creating DRM update source on management server running on Windows 10 Operating System (OS) may fail, displaying the following error message: *Failed to reach location of update source. Please try again with correct location and/or credentials.*

  Refer the dlciappliance_main **log** in Admin portal, if the error message displayed is: Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.

  Resolution: see to the following KB article: support.microsoft.com/en-us/help/4034314

- Failure of firmware update because of job queue being full

  Firmware update job submitted from OMIMSSC to iDRAC fails, and the OMIMSSC main log displays the following error: *JobQueue Exceeds the size limit. Delete unwanted JobID(s).*

  Resolution: manually delete the completed jobs in iDRAC and retry the firmware update job.

- Failure of firmware update when using DRM update source

  Firmware update job may fail if you are using DRM update source with insufficient access to the share folders. If the windows credential profile provided while creating DRM update source is not a part of domain administrator group or the local administrator group, the following error message is displayed: *Local cache creation failure*.

  Resolution:

  1. After creating the repository from DRM, right-click on the folder, click **Security** tab, and then click **Advanced**.

2. Click **Enable inheritance** and select the Replace all child object permission entries with inheritable permission entries from this object option, and then share the folder with **Everyone** with read-write permission.

- Firmware update on components irrespective of selection

  The same components on identical servers get updated during a firmware update irrespective of the selection of components made on these individual servers. This behavior is observed for 12th and 13th generation of PowerEdge servers with Enterprise license of iDRAC.

  Resolution:

  1. First apply updates for common components on identical servers, and
  2. then apply updates for specific components on individual servers.

  Note: Perform staged updates with planned outage time to accommodate the firmware update.

- Failure to delete a custom update group

  After scheduling any job on a server belonging to a custom update group, if the server is deleted from Microsoft console and you synchronize registered Microsoft console with OMIMSSC, the server is removed from the custom update group and the server is moved to a predefined update group. You cannot delete such custom update group, because it is associated with a scheduled job.

  Resolution: Delete the scheduled job from Jobs and Logs page, and then delete the custom update group.

A. Technical Support and Resources

- Dell.com/support is focused on meeting customer needs with proven services and support.
- Firmware update in OMIMSSC provides expertise that helps to ensure customer success on Dell EMC OMIMSSC
- Microsoft System Center Configuration Manager
- Microsoft System Center Virtual Machine Manager

A.1 Related Resources

OMIMSC Interactive Demo

OMIMSSC User Guide

A.2 Terms and Definitions

Terms	
OMIMSSC	Dell EMC OpenManage Integration for Microsoft System Center Appliance
SCVMM	Microsoft System Center Virtual Machine Manager
SCCM	Microsoft System Center Configuration Manager
iDRAC	Integrated Dell Remote Access Controller
DRM	Dell EMC Repository Manager
DUP	Dell Update Package