

# MX7000 Firmware Update

## Revisions

Date	Description
Jan 2019	Initial release

## Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Author: Dahir Herzi, Anoop Alladi, Zoheb Khan and Murali Anumolu

# Table of contents

Revisions.....	2
Acknowledgements.....	2
Introduction .....	4
Catalog Management.....	4
Baseline Report and Compliance Summary.....	6
How a baseline report is generated:.....	6
Firmware update using the Compliance report.....	8
DUP Based update .....	9
Rollback Firmware .....	10
Firmware update for NWIOM.....	10
Firmware update for SAS IOM and Storage.....	12

## Introduction

The Purpose of this white paper is to describe the new and improved features for the firmware update workflow. This technical white paper describes the following features:

- Catalog Management
- Baseline Report and Compliance Summary
- Firmware update using the Compliance report
- DUP based update. (Single DUP upload and update)
- Rollback updated firmware
- Firmware update for IOMs and Storage components

Firmware update is one of the most the critical features for any deployed hardware. This allows users to keep the devices compliant with the hardware manufacturer recommendations. New Firmware often fixes defects, contains new features or protects from security vulnerabilities. MX7000 Chassis allows users to regularly check for compliance of the chassis Sleds, IOMs, and other components then provides the recommendations for a firmware update.

**Configuration**

Firmware Deploy Identity Pools Networks

Baseline Compliance

- ✖ Critical: 0
- ⚠ Warning: 0
- ⬇ Downgrade: 0
- ✔ Ok: 1

Create Baseline Delete Check Compliance Catalog Management

COMPLIANCE	NAME	JOB STATUS
✔	System BaseLine	✔ Completed

1 item(s) found, 1 item(s) selected. Displaying items 1 - 1.

Figure 1 MX7000 Check Compliance

## Catalog Management

MX7000 Chassis allows a user to add a Catalog from Dell online (<http://downloads.dell.com/Catalog>), which is the Catalog from Dell software repository site (PDK Catalog). The chassis already has been configured with the Dell repository as the default site, and user will not need to enter the URI for any of the Dell repositories. Moreover there is an option to use a validated stack Catalog which contains only MX7000 specific bundles. Another option is entering a Network Path for a custom Catalog to be utilized if there is a need to use a Catalog generated by Dell repository manager. The Catalog will contain firmware component details like firmware version, criticality of the update and the location of the DUP.

Here are the steps needed to create a Catalog:

- From Configuration -> Firmware Menu, select Catalog management and Click on Add
- A popup is displayed to add a firmware Catalog. By default Dell Online Catalog is selected.
  - The user has to option to select Dell online Catalog (aka PDK Catalog).

- Also an option to select a validated stack Catalog which is the NGM Catalog that contains only the MX7000 bundles.
- Finally there is an option for a Network path for location of a custom Catalog.

Figure 2 MX7000 Catalog creation wizard

Select one of the following Catalog sources:

- Newest validated stacks of chassis firmware on Dell.com —this is the Catalog that contains latest validated bundle of the Dell EMC 14G MX7000 chassis.
- Latest component firmware versions on Dell.com — this Catalog includes all Dell software components for supported hardware. (aka PDK Catalog)
- Network Path — a folder where a Catalog and optionally associated updates have been placed by generating the Catalog using Dell EMC Repository Manager or a Dell online Catalog placed the share.

Supported Share Type:

- NFS
- CIFS
- HTTP
- HTTPS

Options	Description
Share Address	Enter the address of the Catalog file location. The share address can have a maximum length of 255 characters. The address must have a valid host name, IPv4 address, or IPv6 address. (IP-Address or FQDN)
Catalog File Path	Enter the path of the Catalog file location. A Catalog file path can have a maximum length of 255 characters.( For example: file-path/Catalog.xml)
Domain	This option is available only if the Share Type is CIFS. The domain can have a maximum length of 255 characters.
User Name	This option is available only if the Share Type is CIFS or HTTPS. The user name can have a maximum length of 255 characters.

Password	This option is available only if the Share Type is CIFS or HTTPS. The password can have a maximum length of 255 characters.
Certificate Check	Select the check box to check the security certificate authentication. This option is enabled only if the Share Type is HTTPS

Once the Catalog creation is complete, MX7000 chassis displays the information of the Catalog such as the remote repository location, Release date, and number of bundles present in the Catalog. If the user configures a baseline using the Catalog a list all the baselines associated with the Catalog will be shown on the page (See Figure 3). Association of Catalog and baseline is discussed in following section.

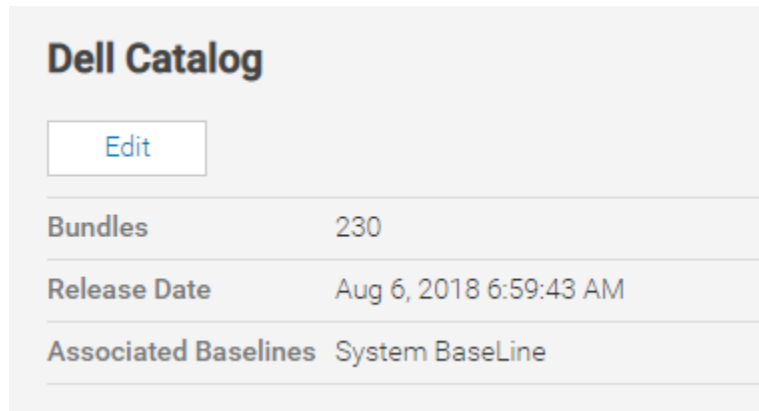


Figure 3 MX7000 Catalog Details

Catalog Management also allows to edit the Catalog, update the Catalog and delete the Catalog. Internally when a Catalog is updated and a baseline is associated, the report is regenerated.

## Baseline Report and Compliance Summary

Baseline report displays the compliance of the devices/groups selected. Compliance is an indication of the drift between Catalog component version and the device inventory, if a device inventory is older than the Catalog content then this device is none-complaint. The compliance specifies if an action is required, such as device that require an upgrade and the criticality of the upgrade. A Baseline report displays the following details at the high level:

- Compliance state
- Associated Catalog
- Compliance pie chart with number of devices in critical, warning, downgrade and compliant state with the Catalog.

## How a baseline report is generated:

The user selects a Catalog and selects the devices/groups then generate a report. Internally OME-M uses the “Dell Update Engine for Consoles” library (DUEC) to generate the compliance report. OME-M provides device software inventory details and a Catalog source to the DUEC library. The DUEC library takes the input and returns a compliance report.

Here are the steps to create a baseline report and view the compliance details:

How a baseline report is generated:

- Under Configuration->Firmware, click Create baseline. In the popup, select a Catalog, Baseline report name, description and Devices/Groups that needs to be part of this baseline report.

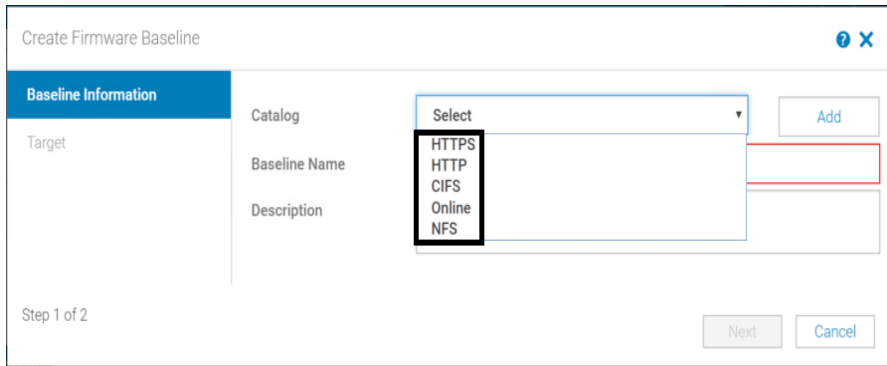


Figure 4 shows the 'Create Firmware Baseline' dialog box. The 'Catalog' dropdown menu is open, displaying options: HTTPS, HTTP, CIFS, Online, and NFS. The 'Add' button is highlighted. The 'Baseline Name' and 'Description' fields are empty. The 'Next' and 'Cancel' buttons are at the bottom right.

Figure 4 MX7000 Baseline creation

Choose devices or groups for the baseline:

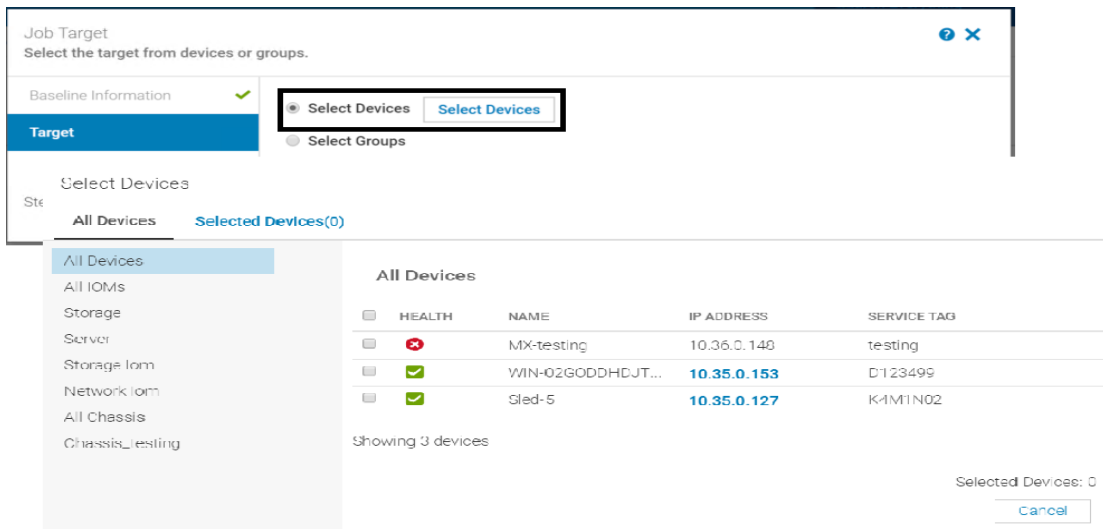


Figure 5 shows the 'Job Target' dialog box. The 'Target' tab is selected. The 'Select Devices' button is highlighted. Below, a table lists devices with columns: HEALTH, NAME, IP ADDRESS, and SERVICE TAG. The table shows three devices: MX-testing (10.36.0.148), WIN-02GODDHDJT... (10.35.0.153), and Sled-5 (10.35.0.127). The 'Selected Devices: 0' indicator is at the bottom right.

HEALTH	NAME	IP ADDRESS	SERVICE TAG
	MX-testing	10.36.0.148	testing
	WIN-02GODDHDJT...	10.35.0.153	D123499
	Sled-5	10.35.0.127	K4M1N02

Figure 5 MX7000 Baseline target selection

Click finish to create a baseline

- Once the baseline is created, a new record is displayed on the baseline reports page with the Compliance summary details:

## Firmware update using the Compliance report

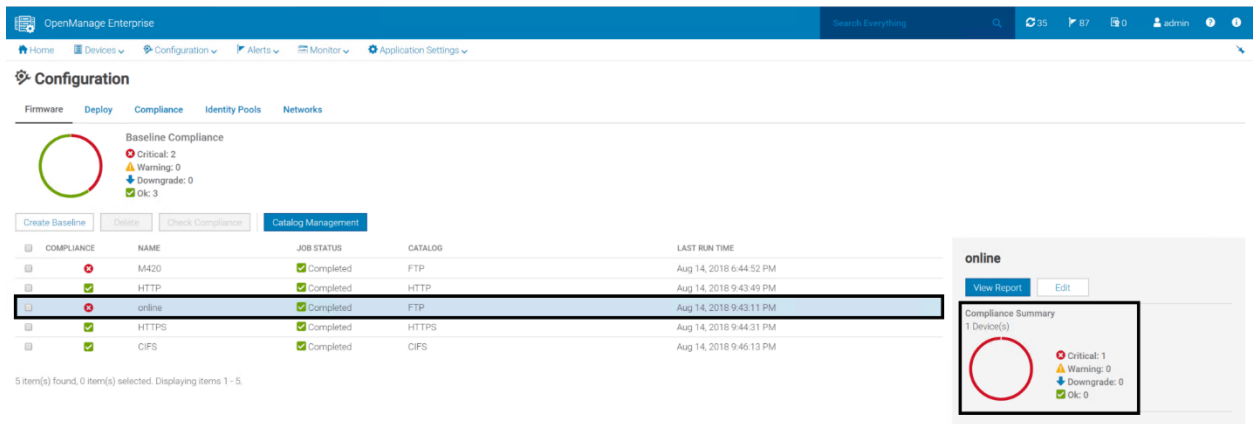


Figure 6 MX7000 Baselines

- Click on View report to view the Device level compliance report and also the software component compliance report for the device. This report provide the list of all the updatable components.

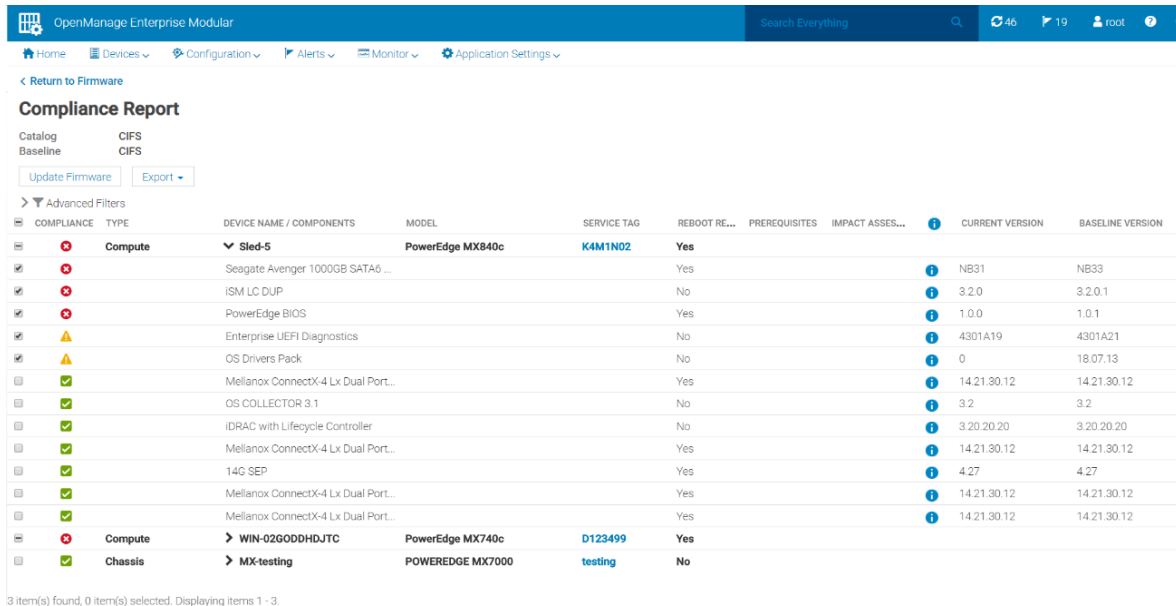


Figure 7 MX7000 Baseline report

## Firmware update using the Compliance report

Once the compliance report is generated, User can view the Device level compliance details and also Component level details. User can see the criticality of the component and also the Component name and has the option to update the component. When the Firmware Update button is clicked a popup will display to schedule the Job to Run now or Schedule it at later time. Also there is an option to stage the jobs. If option "Stage for next reboot" is selected, the firmware jobs are staged on the remote device (only applicable to server devices). Below is the firmware update schedule window:



## Schedule Update

Please Note: Firmware updates may take up to 45 minutes per server.

### > Additional Information

**Update Now**

Firmware updates will apply immediately. If a server is selected, it may cause the server to reboot.

To stage the firmware updates for next server reboot, select the option below.

This option only applies to servers. Firmware updates will apply immediately for all other devices.

**Stage for next server reboot.**

**Schedule Later**

Firmware updates will apply at a selected date and time and then reboot the server(s).

Figure 8 MX7000 Update scheduler

## DUP Based update

This feature allows user to manually choose a DUP (Dell Update Package) from local directory to be applied to the chassis components or device in the chassis. Before applying the DUP is validated for compliance and signature. A DUP level report is displayed, information on the version being applied and details on criticality of the DUP plus the devices that require an update. Below are the steps for DUP based updates.

- Go to All devices, or Respective device page then select device(s) to update. Click the firmware update button.

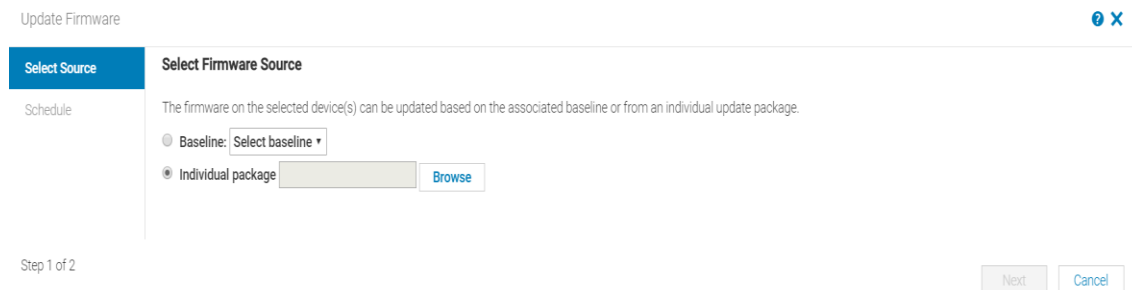


Figure 9 MX7000 DUP selection

- Select individual package then Browse to the DUP location and upload a DUP. Once the DUP is uploaded, the DUP is validated and compliance check will done with the software inventory of the device. Compliance report for the DUP is displayed as below:

Update Firmware i X

Select Source

Select Firmware Source

The firmware on the selected device(s) can be updated based on the associated baseline or from an individual update package.

Baseline: Select baseline

Individual package iDRAC-with-Lifecycle-Cont Browse

Version: 3.20.20.20  
Date: 2018-06-22 10:00:00.000

	COMPLIANCE	DEVICE NAME	SERVICE TAG	COMPONENT	CURRENT VERSION	REBOOT REQUIR...	PREREQUIL...	IMPACT A...
<input type="checkbox"/>	✔	WIN-02GODD...	D123499	iDRAC with Li...	3.20.20.20	No		
<input type="checkbox"/>	✔	Sled-5	K4M1N02	iDRAC with Li...	3.20.20.20	No		

2 item(s) found, 0 item(s) selected. Displaying items 1 - 2.

Step 1 of 2

Next
Cancel

Figure 10 MX7000 Target selection

- Select the devices and click next to schedule the firmware update job.

## Rollback Firmware

The Rollback Firmware window enables you to roll back a firmware update to the previous version. If the user is unhappy with a recent firmware update, they can request a rollback of the firmware to the previous version prior to the update. The rollback is enabled if MSM has access to the firmware package corresponding to the previous version. The access could be enabled either by

- The device has a rollback or N-1 version.
- The imported Catalog contains a reference to the previous version.
- You browse for a firmware package, which has the previous version

## Firmware update for NWIOM

MSM supports DUP update for Dell managed advanced IOMs: Dell EMC MX9116n Fabric Engine / Dell EMC MX5108n Ethernet Switch. At high level the DUP upgrade process for NWIOM is identical to other devices. However, there is added flavor of Fabric / Full Switch mode. Note, NWIOMs are utilized to formulate a Fabric and are managed as part of a single entity. Therefore, when a NWIOM is in Fabric mode, meaning part of Fabric, it will lead to FW upgrade of all the IOMs in the Fabric. However, this behavior is not applied for the Full Switch mode IOMs.

IOM Upgrade for the Full Switch Mode IOM:

# Firmware update for NWIOM

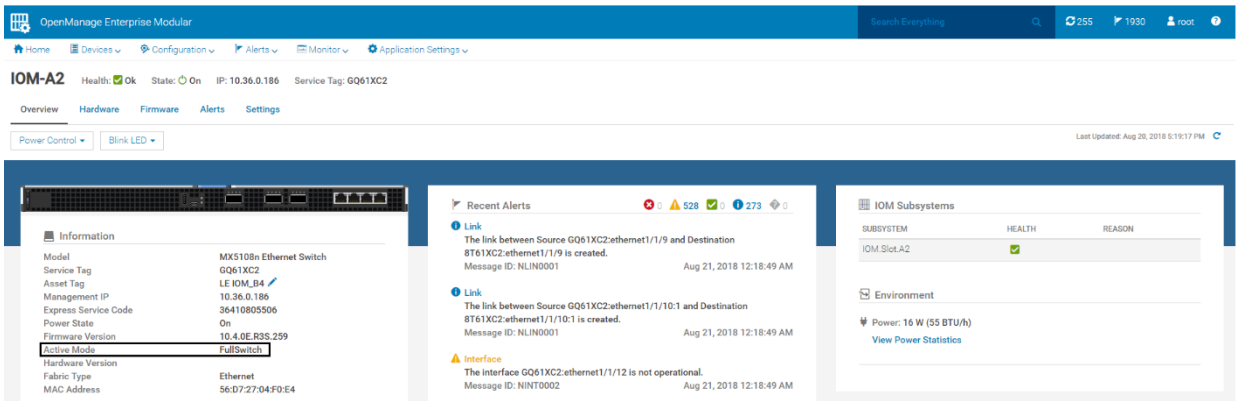


Figure 11 MX7000 IOM in Full Switch Mode

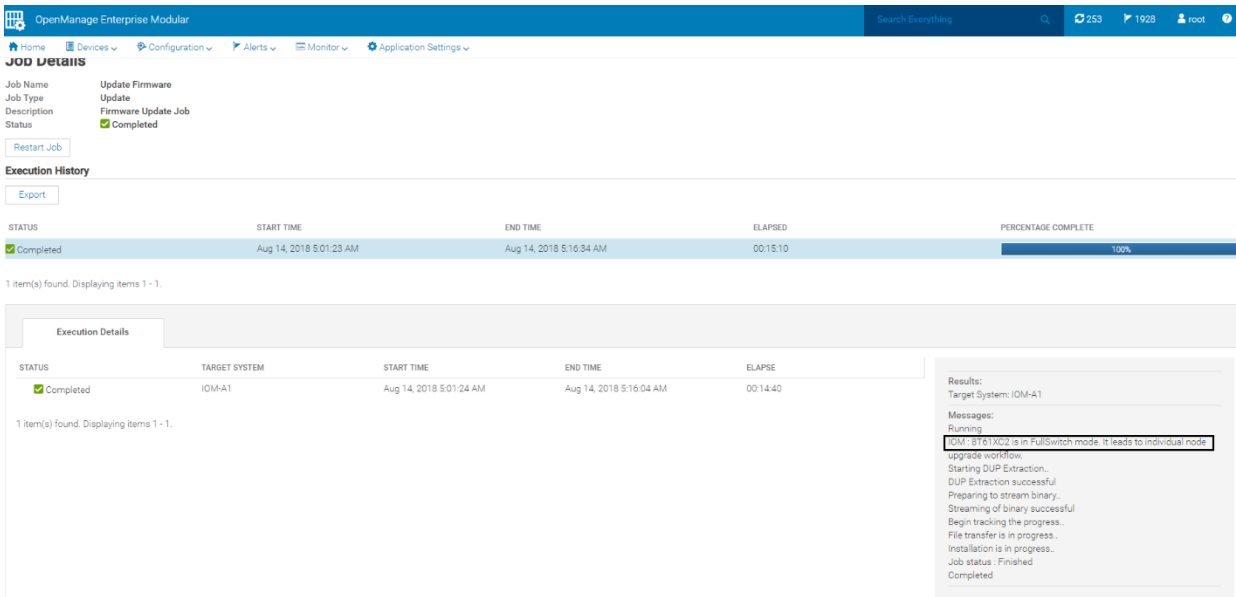


Figure 12 MX7000 IOM in IOM in Full Switch Mode update

## IOM Upgrade for the Fabric Mode IOM:

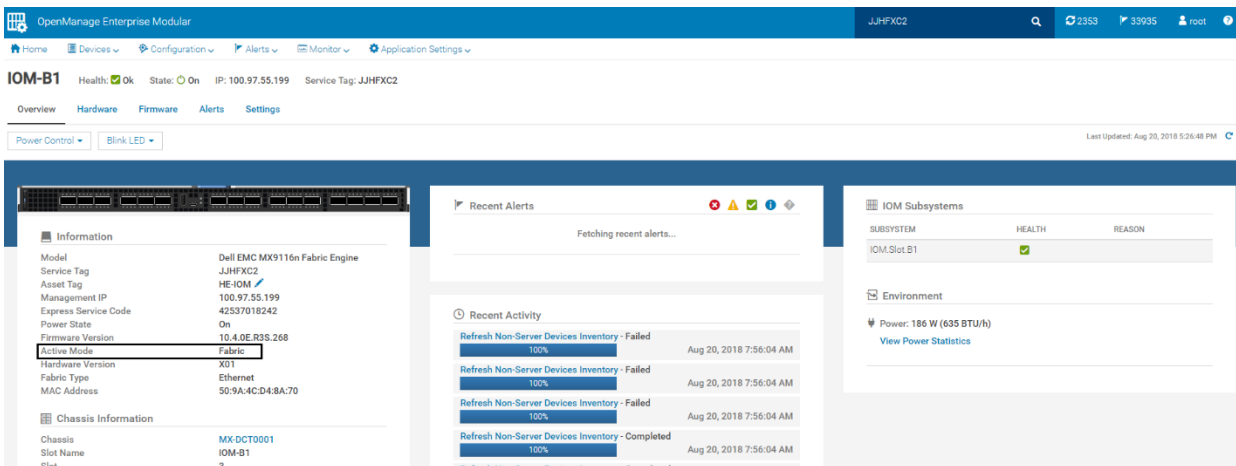


Figure 13 MX7000 IOM in Fabric Mode

# Firmware update for SAS IOM and Storage

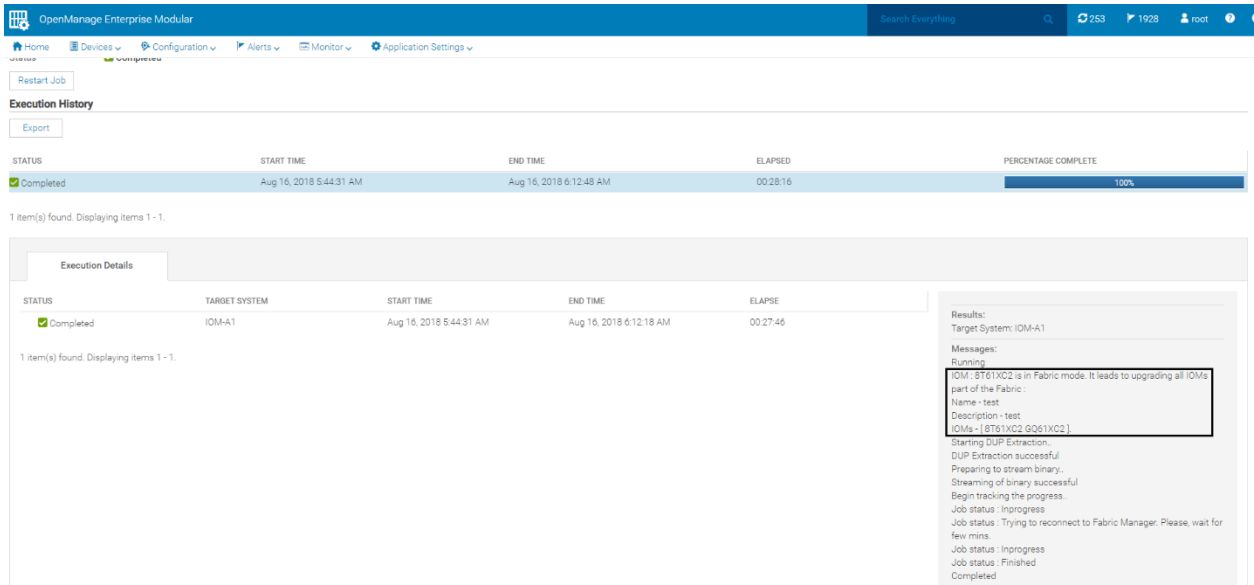


Figure 14 MX7000 Fabric Mode IOM upgrade status update

## Firmware update for SAS IOM and Storage

MSM supports the Firmware update of SAS IOM (Dell EMC PowerEdge MX5000s) and Storage (Dell EMC PowerEdge MX5016s) devices by using either Compliance report or DUP based update.

Based on the pre-requisite information of the firmware update it is required to power off the compute sleds which has storage assignments before triggering the firmware update.

- Pre-requisites in Compliance Report

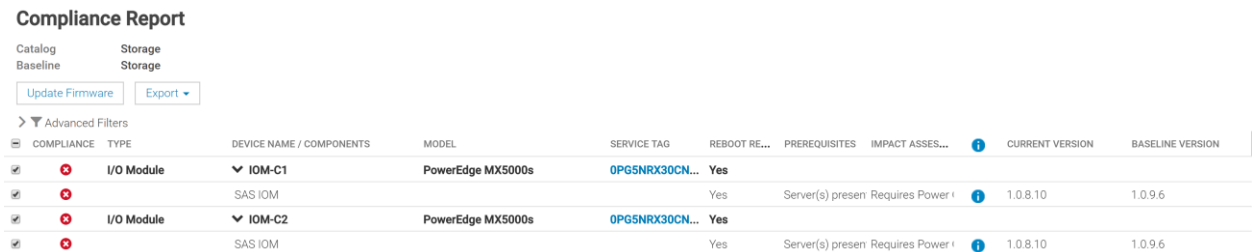


Figure 15 MX7000 SAS IOM Storage baseline report

### Pre-requisites in DUP Update

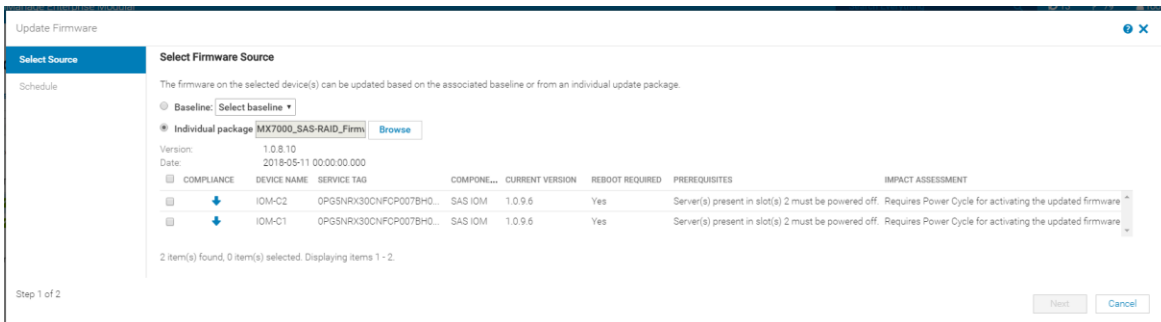


Figure 16 MX7000 SAS IOM and storage single update