



Updating Dell Server Hardware with Dell OpenManage Essentials

This Dell technical white paper provides information about the maintenance and enforcement of hardware revision baseline within a datacenter environment using Dell OpenManage Essentials.

Dell Engineering
September 2015

Revisions

Date	Description
August 2013	Initial release
September 2015	Updates with the OpenManage Essentials version 2.1 release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2015 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge are trademarks of Dell Inc. Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.



Table of contents

Revisions.....	2
Executive summary	6
1 Introduction.....	7
2 Obtaining the latest version of update packages	8
2.1 Dell Server Update Utility DVD	8
2.2 Dell online catalog (recommended).....	9
2.3 Dell Repository Manager	10
3 In-Band System Updates.....	11
3.1 Updating the hardware at your convenience	12
3.2 Supported models for system update	15
3.3 Dell OpenManage Server Administrator (OMSA).....	15
3.4 Updating systems.....	15
3.5 Agent Free In-Band System Update	18
4 Out-Of-Band System Updates (iDRAC).....	19
5 System updates on correlated devices – servers and iDRACs	26
6 In-band system update task (Linux) using sudo users	27
6.1 Configuring a sudo user in Linux	27
7 System update using the guided wizard.....	30
8 System Update – Run Option	33
9 Initiating firmware and driver inventory.....	35
9.1 Creating the firmware and driver inventory task from the Remote Tasks portal	35
9.2 Creating the firmware and driver inventory from the System Update portal	47
10 Performing system update.....	50
10.1 Linux system update as a “sudo” user	51
10.2 Scheduled Firmware & Driver Inventory collection task after update.....	52
11 Difference between managing a server with or without OMSA.....	53
12 Updating the inventory collector component in OpenManage Essentials	54
A Additional resources (optional)	56



Table of figures

Figure 1	Select a catalog source	8
Figure 2	Importing the latest Dell FTP catalog	9
Figure 3	Software Inventory Information table.....	12
Figure 4	Default reboot target server setting	13
Figure 5	Create (in-band) system update task	14
Figure 6	Advanced settings preferred update in-band mode	15
Figure 7	Non-Compliant Systems.....	16
Figure 8	Create In-band delivery mode system update task	17
Figure 9	System Update Task (OMSA) Execution Status	18
Figure 10	Advanced Settings preferred update mode iDRAC	20
Figure 11	iDRAC Non-Compliant Report.....	21
Figure 12	Create out-of-band system update task	22
Figure 13	Out-of-band (iDRAC) system update task execution status	23
Figure 14	Out-of-band (iDRAC) - cancel iDRAC jobs	24
Figure 15	Creating a Linux user.	27
Figure 16	Editing the sudoers file	28
Figure 17	Logging in as a sudo user.....	28
Figure 18	System update task – Enable Sudo	29
Figure 19	System update wizard.....	30
Figure 20	System update wizard – Non-Compliant Systems	31
Figure 21	System update wizard – Applicable Packages	31
Figure 22	Credentials page of the system update wizard	32
Figure 23	Running a system update task.....	33
Figure 24	Running the Import Catalog for System Update task	34
Figure 25	Remote Task – Firmware & Driver Inventory Task - launch point	35
Figure 26	Firmware & Driver Inventory Task – Task Name	36
Figure 27	Firmware & Driver Inventory Task – Filter devices based on the operating system	37
Figure 28	Firmware & Driver Inventory Task – Select the Operating System	38
Figure 29	Firmware and Inventory task – Show OMSA based targets.....	39
Figure 30	Firmware & Driver Inventory Task – Select Target.....	41
Figure 31	Firmware & Driver Inventory task – Select a query	42
Figure 32	Firmware & Driver Inventory task – Enable All option for OMSA based targets	43



Figure 33	Firmware & Driver Inventory Task –Set schedule.....	44
Figure 34	Firmware & Driver Inventory Task – Run now	45
Figure 35	Firmware & Driver Inventory Task – Credentials	46
Figure 36	System Update Portal – Non inventoried Systems	47
Figure 37	System update portal – Select the servers	47
Figure 38	System update portal – Run inventory	48
Figure 39	System update portal – Firmware & Driver inventory wizard.....	49
Figure 40	System update portal – Non-Complaint Systems tab.....	50
Figure 41	System update portal – Linux server select packages	51
Figure 42	System update portal – Linux sudo.....	51
Figure 43	Scheduled F/W& Driver inventory Task	52
Figure 44	Dell Solutions tab showing Inventory Collector Component	54
Figure 45	Update link for inventory collector component	55



Executive summary

This white paper describes the process of maintaining and enforcing a firmware and drivers revision baseline within the Dell PowerEdge server environment using OpenManage Essentials.

This document explains the process to update servers without forcing an unplanned shutdown. Using OpenManage Essentials, IT administrators can keep the servers up-to-date without affecting the production environment. You can use a single console to update multiple Dell servers.



1

Introduction

IT administrators face several challenges today, which include managing system updates (BIOS, firmware, driver) in a datacenter. Administrators find it challenging to keep track of new versions of firmware and drivers, which are released at frequent intervals.

This white paper explains how an IT administrator can use Dell OpenManage Essentials to overcome the challenges associated with managing system updates. This document covers the following topics:

- Deploying system updates along with the OMSA agent
- Obtaining the latest versions of drivers, firmware, and BIOS
- Determining the servers that should be updated and their respective packages (DUPs)
- Updating the hardware at your convenience
- Updating the hardware using the Guided System Update Wizard
- Agentless system update



2 Obtaining the latest version of update packages

To obtain the latest version of drivers, firmware, and BIOS, you must import the latest **catalog.cab** file. You can import the catalog file from three different sources provided by Dell:

- Dell Server Update Utility (SUU) DVD
- Dell FTP
- Dell Repository Manager (RM)

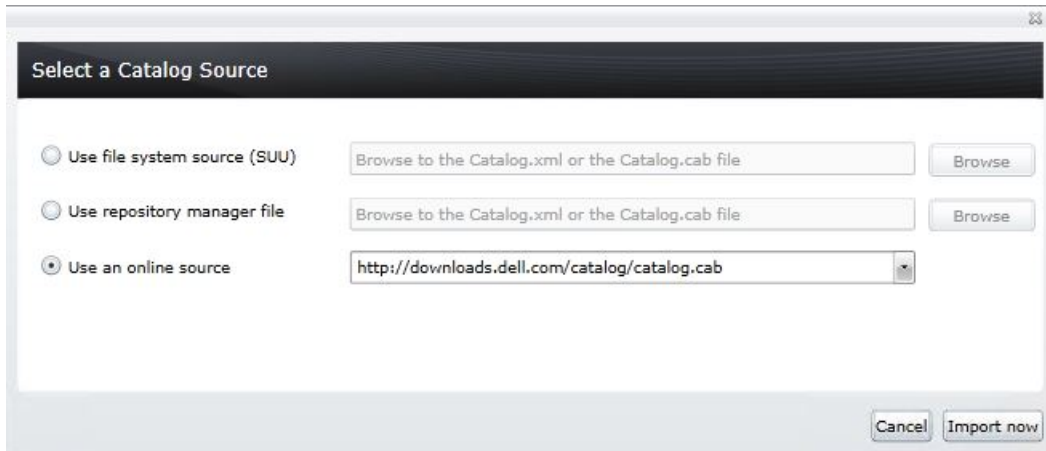


Figure 1 Select a catalog source

2.1 Dell Server Update Utility DVD

Note: You can obtain the latest version of Dell SUU from dell.com/support.

Dell recommends using the Server Update Utility when internet access is not available on the server where OpenManage Essentials is installed.

To import the catalog using the SUU DVD or iso image:

1. Mount the SUU DVD or iso image.
2. Open the OpenManage Essentials console.
3. Click **Manage** → **System update**.
4. Click **Select a catalog source**.
The **Select a catalog source** window is displayed.
5. Select the **Use file system source (SUU)** option
6. Click **Browse** and navigate to the location where SUU is available.
7. Select the **catalog.xml** or **catalog.cab** file located in the SUU repository folder.
8. Click **Import now** to import the catalog.

2.2 Dell online catalog (recommended)

Dell recommends using the Dell online catalog as the source when the internet is accessible from the server running OpenManage Essentials. Dell uploads the latest releases of firmware, drivers or BIOS at **downloads.dell.com** or **ftp.dell.com** such that the latest catalog is always available.

To obtain the latest catalog:

Note: If the system on which OpenManage Essentials is installed connects to the internet through a proxy server, ensure that the proxy settings are configured in the **Settings** page in OpenManage Essentials.

1. Open the OpenManage Essentials console.
2. Click **Manage**→ **System update**.
3. Click the **Summary** tab.

Note: The **Get the Latest** button is enabled only when a new version of the catalog is available on the Dell FTP site.

4. Click **Get Latest**.

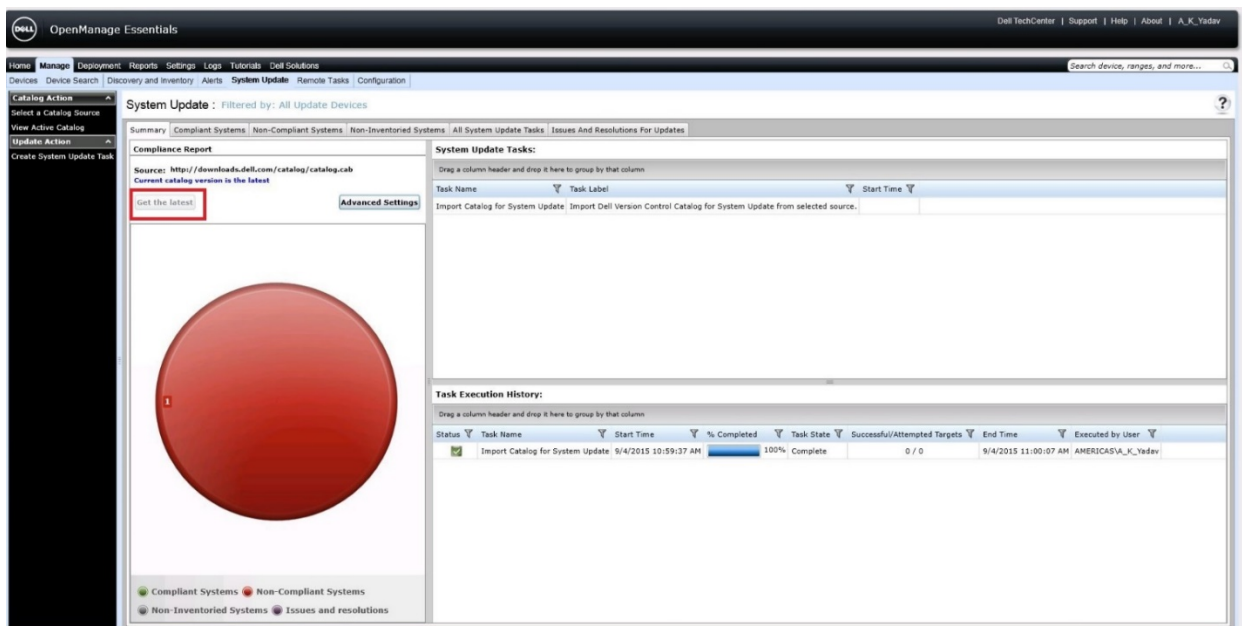


Figure 2 Importing the latest Dell FTP catalog

2.3 Dell Repository Manager

Dell Repository Manager is a separate tool that you can install from the OpenManage Essentials installation package. Repository Manager allows you to create a custom repository for the required server model, operating system, and components that you want to update.

To create a custom repository:

1. Perform discovery and inventory of the servers and iDRAC (using the appropriate protocols) in OpenManage Essentials.
2. Launch Dell Repository Manager (server).
3. Click **Create** and select **Dell OpenManage Essentials Repository**.
4. Type a name and description and click **Next**.
5. Select Dell online repository and click **Next**.
Repository Manager obtains the OpenManage Essentials inventory and all the devices are displayed in Repository Manager.
6. Click **Next**.
7. Select save and download repository and click **Finish**.
8. Select a location to save the catalog and DUPs.



3 In-Band System Updates

In-band system updates rely on the operating system (Windows/Linux) environment to update Dell PowerEdge servers. OpenManage Essentials can update Dell servers that either have or do not have Dell OpenManage Server Administrator (OMSA) installed on them.

To identify the servers that may require updates in your datacenter, perform a discovery and inventory of the servers in OpenManage Essentials. If the server has OMSA installed, you must discover the server using SNMP/WMI protocol. If the server does not have OMSA installed, you must discover the servers with WMI/SSH protocol and run the **Create F/W & Driver Inventory Task** to gather the inventory information. The discovered servers should be classified under **Servers** node in the **All Devices** tree of the **Devices** portal.

After the discovery and inventory, you must import the baseline catalog. During a catalog import, the installed version of server packages is compared with the available version of packages in the baseline catalog to determine the updatable packages for each server. A comparison report is generated and the servers are classified as follows:

- **Compliant Systems** – Servers in this category have the same versions of BIOS, drivers, and firmware as that of the imported catalog.
- **Non-Compliant Systems** – Servers in this category require BIOS, firmware or driver updates. This report also displays the level of importance of each applicable package. For example, critical, recommended, and optional packages.
- **Non-Inventoried Systems** – Servers in this category have not been inventoried yet. You can run the server inventory task from the **Non-Inventoried Systems** tab if necessary.

Note: For the servers that are classified as compliant or non-compliant, you can find the installed package version in the **Software Inventory Information** table on the **Device details** page. The **Software Inventory Information** table is populated when the server is inventoried.



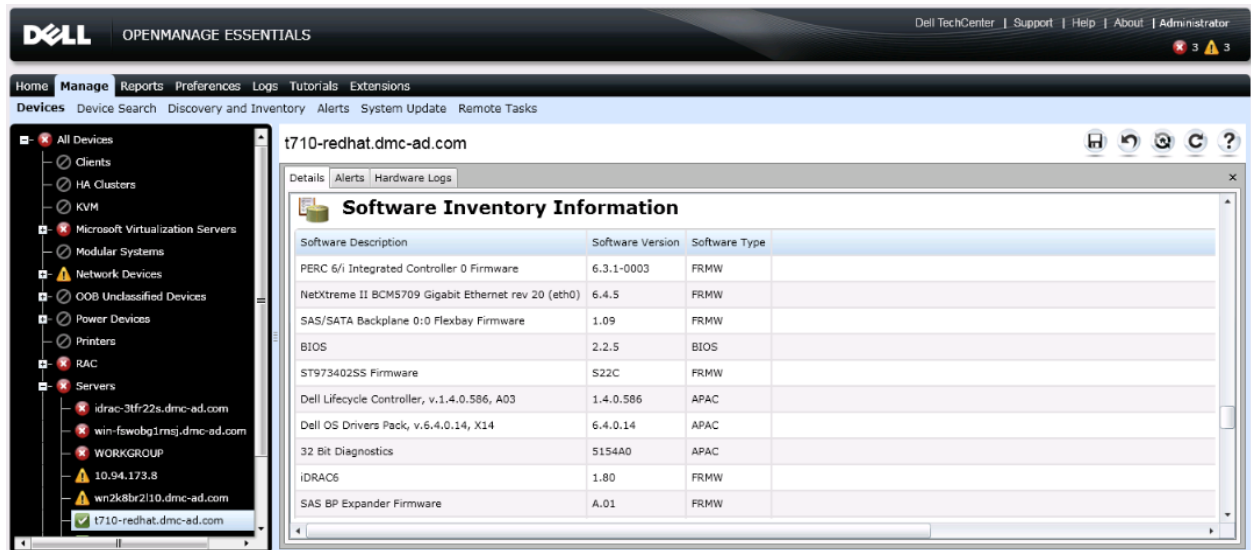


Figure 3 Software Inventory Information table

3.1 Updating the hardware at your convenience

You must create a system update task and set a schedule to apply applicable updates to the non-compliant servers. To view an illustration of the system update task creation page, see Figure 5.

You can select various combinations to update servers:

- *Single update on a single server:* You can select one package to be applied on a single server.
- *Multiple updates on a single server:* You can select all packages (BIOS, drivers and firmware) to be applied on a single server using a single task.
- *Single update on multiple servers:* You can select a single package applicable to multiple servers and apply the package on multiple servers. For example, if there are 10 Dell PowerEdge R515 servers that require a BIOS update, then the update can be applied on all the 10 servers using a single task. Each of the 10 servers must have the same credentials for the task to run successfully.
- *Multiple updates on multiple servers:* You can select all applicable packages on multiple servers to be applied using a single task. All servers being updated using the task must have the same credentials for the task to run successfully.

Note: You cannot update servers running Windows and Linux operating systems in a single task unless both operating systems share the same credentials.

Reboot device option:

Packages such as BIOS, network firmware, storage controller firmware and drivers, PERC, and SAS require a system reboot for the update to be successful. By default, the Reboot option is disabled in the update task, so that you can manually reboot the servers later during non-working hours. In this case, the updates are applied to the servers, but the update does not come into effect until the server is rebooted. If you

want to reboot at the time of update, you can select the **After update, if required, reboot the server** option in the system update task wizard.

The reboot option's default selection is controlled by the **System Update→Advanced Settings→After update, if required, reboot the server** check box. If the **After update, if required, reboot the server** check box is selected,

Based on the selection of the **After update, if required, reboot the server** check box, the system update task wizard's reboot server option will either be selected or not selected.

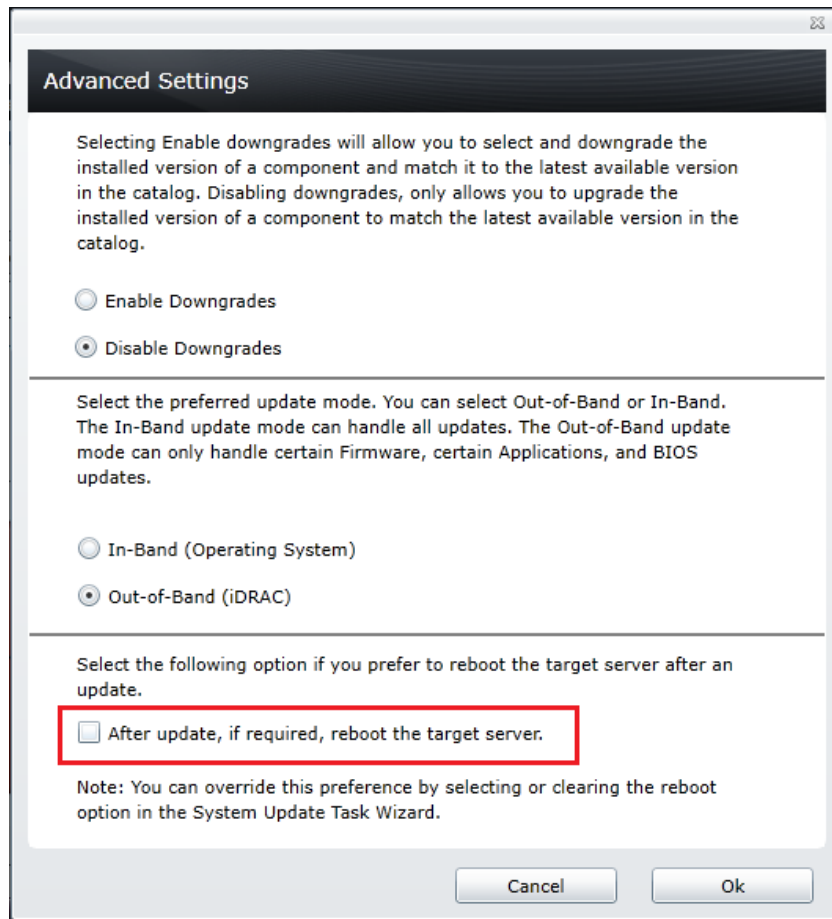


Figure 4 Default reboot target server setting

Skip Signature Hash Check:

Select the **Skip Signature Hash Check** option to skip the signature and hash check on the system update package.

System Update Task

Task Name: System Update Task - 10/23/2012 1:37:39 PM

System Name	Importance	Deliver	Component	Type	Installer	Upgrade	Availability	Package Name
10.94.173.8	Critical	OMSA	BIOS	BIOS	1.1.13	1.2.0	PER900_BIOS	
10.94.173.8	Recommended	OMSA	Broadcom Net	Firmware	5.0.12	7.2.14	Network_Firm	
10.94.173.8	Recommended	OMSA	Broadcom Net	Firmware	5.0.12	7.2.14	Network_Firm	
10.94.173.8	Recommended	OMSA	PERC 6/E Adap	Firmware	6.2.0-0013	6.3.1-0003	SAS-RAID_Fin	
10.94.173.8	Recommended	OMSA	PERC 6/i Integ	Firmware	6.2.0-0013	6.3.1-0003	SAS-RAID_Fin	
idrac-3tfr22s.dmc-i	Recommended	OMSA	BIOS	BIOS	1.4.7	1.10.2	BIOS_C97CP	
idrac-3tfr22s.dmc-i	Recommended	OMSA	Broadcom Net	Firmware	4.6.8	7.2.14	Network_Firm	
idrac-3tfr22s.dmc-i	Optional	OMSA	Dell 32 Bit Dia	Application	5142A0	5154A0	Diagnostics_A	

Set the Task Schedule:

☒ Run now ☐ Set schedule 10/23/2012 1:47 PM (UTC-08:00)

☒ After update, if required, reboot the device. ☒ Skip Signature and Hash Check

Enter Credentials for the task execution:

SSH Port number: 22

Server User Name:

Server Password:

Help Cancel Finish

Figure 5 Create (in-band) system update task

After the update task is completed, OpenManage Essentials inventories the updated servers (after 20 minutes). Comparison between the installed packages version and baseline catalog are automatically completed and the servers are classified as either compliant or non-compliant systems. The system update functionality of OpenManage Essentials ensures that as an IT administrator, you can always be aware of the status of servers in your datacenter environment.

When BIOS, drivers, firmware and application packages are selected for updates on a server, the packages are applied in the following order:

1. Drivers
2. Firmware
3. ESM firmware
4. BIOS
5. Application

During the system update process, packages are downloaded from the selected source and saved in the **Packages** folder under the **Essentials\SystemUpdate** folder.

(C:\Program Files\Dell\SysMgt\Essentials\SystemUpdate\Packages)

3.2 Supported models for system update

For information about the list of device models that support system update, see the OpenManage Essentials User's Guide at dell.com/OpenManageManuals.

3.3 Dell OpenManage Server Administrator (OMSA)

For information about deploying OMSA, see the [Deploying OpenManage Server Administrator Using OpenManage Essentials](#) technical white paper.

3.4 Updating systems

1. Enable In-band (Operating System) update mode from advanced settings: Click **System Update**→ **Summary**→ **Advanced Settings**, and select **In-Band (Operating System)**.

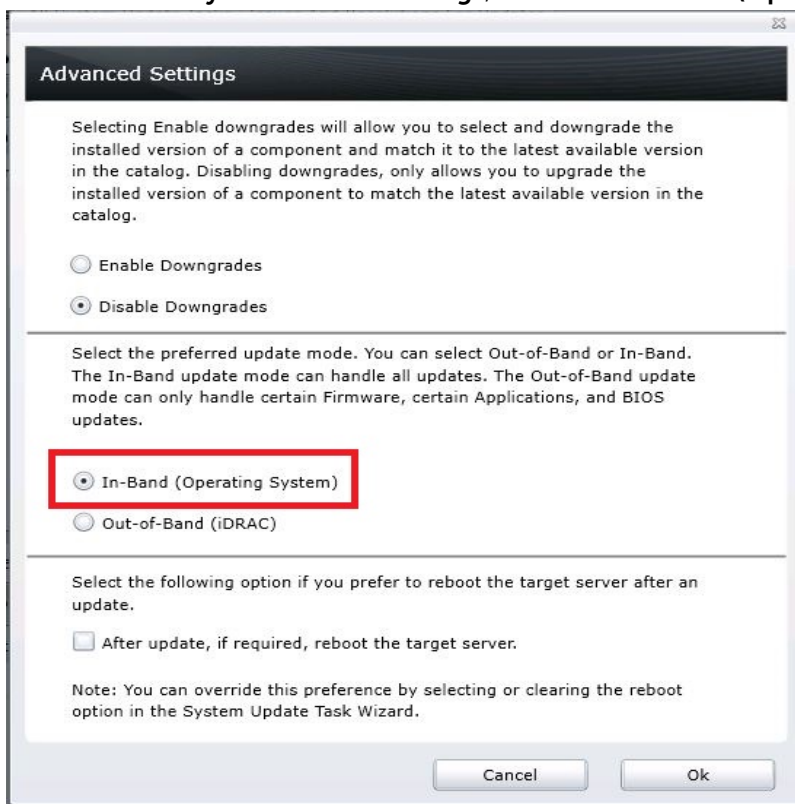


Figure 6 Advanced settings preferred update in-band mode

2. Select the non-compliant systems you want to update: Click **System Update**→ **Non-Compliant Systems** and select systems listed under **Select Any of the Non-Compliant Systems to Update**.

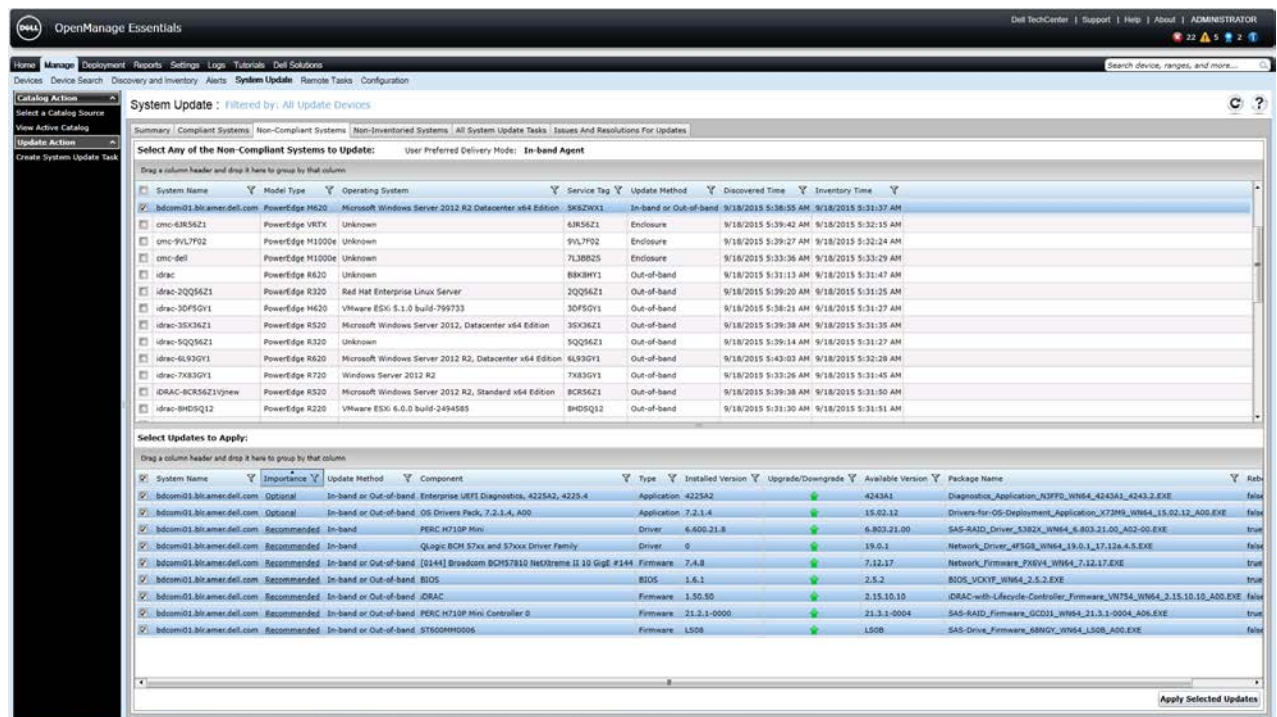


Figure 7 Non-Compliant Systems

Note:

- User Preferred Delivery Mode – In-band agent.
- Update Method for Selected Systems – In-band or Out-of-Band.
- Update Method for Selected Components – In-band or In-band & Out-of-Band.

3. Create an In-band update mode System update task.
4. Select available components to update from the **Select Updates to Apply** (BIOS, Firmware, Drivers and Applications) and click **Apply Selected Updates**.
5. Enter the task name and set the task schedule – select the **Run now** or **Set Schedule** option.
6. Select **After update, if required, reboot the device** and **Skip Signature and Hash Check**.
7. Enter the user name and password of the target server.
8. Click **Finish**.

The in-band system update task is be created and completed.

Task Name: System Update Task - 9/18/2015 3:07:35 PM

<input checked="" type="checkbox"/>	System Name	Importance	Delivery Mode	Component	Type
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Optional	In-band	Enterprise UEFI Diagnostics, 4225A2, 4225.4	Application
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Optional	In-band	OS Drivers Pack, 7.2.1.4, A00	Application
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Recommended	In-band	PERC H710P Mini	Driver
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Recommended	In-band	QLogic BCM 57xx and 57xxx Driver Family	Driver
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Recommended	In-band	[0144] Broadcom BCM57810 NetXtreme II 10 GigE #144	Firmware
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Recommended	In-band	BIOS	BIOS
<input checked="" type="checkbox"/>	bdcomi01.blr.amer.dell.com	Recommended	In-band	iDRAC	Firmware

Set the Task Schedule:

☐ Run now
 ☐ After update, if required, reboot the target server.

☒ Set schedule: 9/18/2015 3:17 PM (UTC+05:30)
 ☐ Skip Signature and Hash Check

Enter Credentials for the task execution:

Server User Name:
 Server Password:

Figure 8 Create In-band delivery mode system update task

Note:

- Delivery Mode – In-band.
- Updatable components – BIOS, Firmware, Drivers & Applications.
- Server credentials are required.
- All above packages can be updated using In-band update mode.

You can view the status of the system update task in the **Task Execution History** in the **System Update** portal. To view the **Task Execution History**, click the **Summary** or **All System Update Tasks** tab.

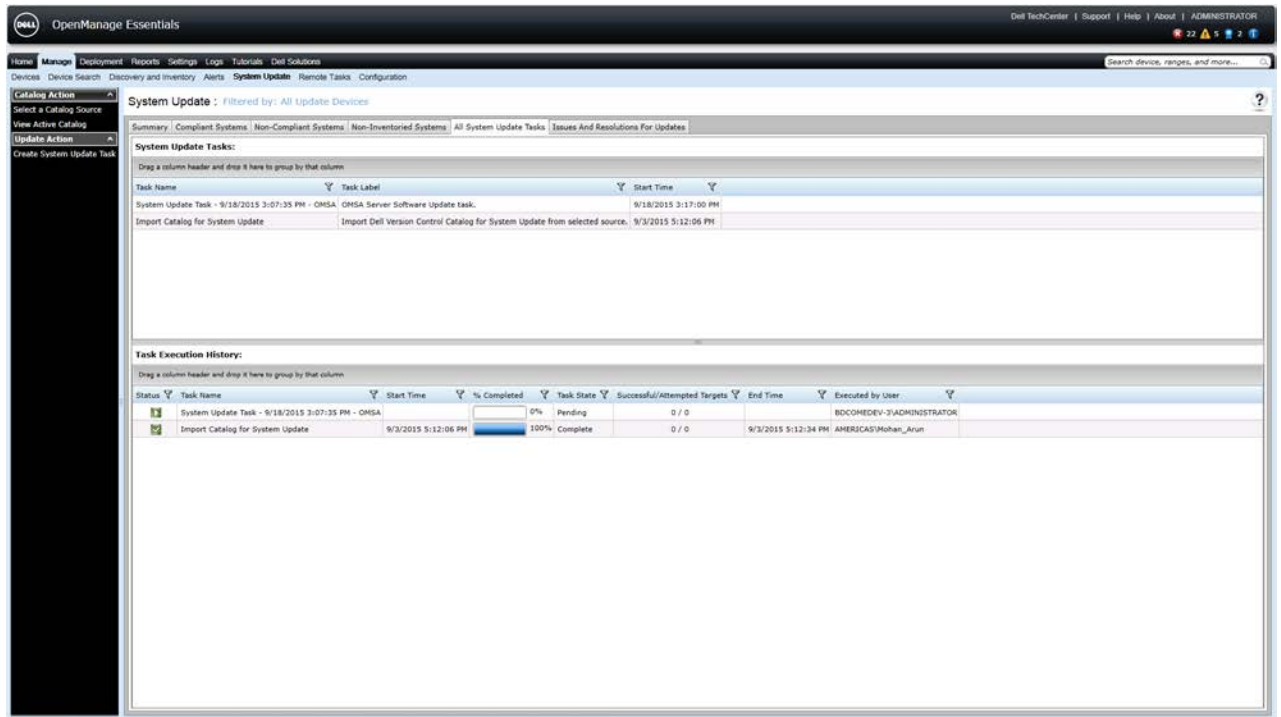


Figure 9 System Update Task (OMSA) Execution Status

On completion of the system update task, the **Task State** displays a **Completed** status. About 20 minutes after the task is completed, an auto inventory task is initiated to gather the updated inventory information.

3.5 Agent Free In-Band System Update

You can also update servers on which agents such as OMSA are not installed. For information about updating systems (in-band) that do not have an agent installed, see the [Agentless In-band System Update with Dell OpenManage Essentials](#) technical white paper.

4 Out-Of-Band System Updates (iDRAC)

Out-of-band system updates rely on the iDRAC with Lifecycle controller mechanism to update Dell PowerEdge servers. Out-of-band system update is useful for an IT administrator when there is managed PowerEdge server that either has or does not have an operating system installed and does not have OMSA installed.

Agent-free system update in OpenManage Essentials does not require the operating system and OMSA on the managed system to gather inventory and deploy firmware and BIOS updates. Agent free updates are applied through the Integrated Dell Remote Controller (iDRAC6/iDRAC7/iDRAC8) on Dell's 11th, 12th and 13th generation of PowerEdge servers.

The following updates can be applied through the iDRAC:

- BIOS
 - Firmware
 - Applications (Dell Diagnostics and Dell Lifecycle Controller)
1. Perform discover and inventory of iDRAC6/iDRAC7/iDRAC8 using WS-Man protocol:
 - a. Click **Manage**→ **Discovery and Inventory**→ **Add discovery range**.
 - b. Type the iDRAC addresses.
 - c. Click **Next** and clear the SNMP protocol.
 - d. Click **Next**.
 - e. Select **Enable WS-Man Discovery**, type the user name and password.
 - f. Select **Secure Mode**, **Skip common name check**, and **Trusted site** options.
 - g. Click **Next**.
 - h. In the **Discovery Range Action** page select **Perform both discovery and Inventory**.
 - i. Click **Finish**.
 2. Click **Manage**→ **Devices**.
Verify that the device is discovered and classified under RAC device group.

Note: The discovered iDRAC will be present either under the compliant or non-compliant systems section in the compliance pie-chart.

3. Click **System Update**→ **Advanced Settings**.
4. Set preferred update mode to **Out-of-Band (iDRAC)**.
5. Click **Ok** to save the settings and close the **Advanced Settings** window.



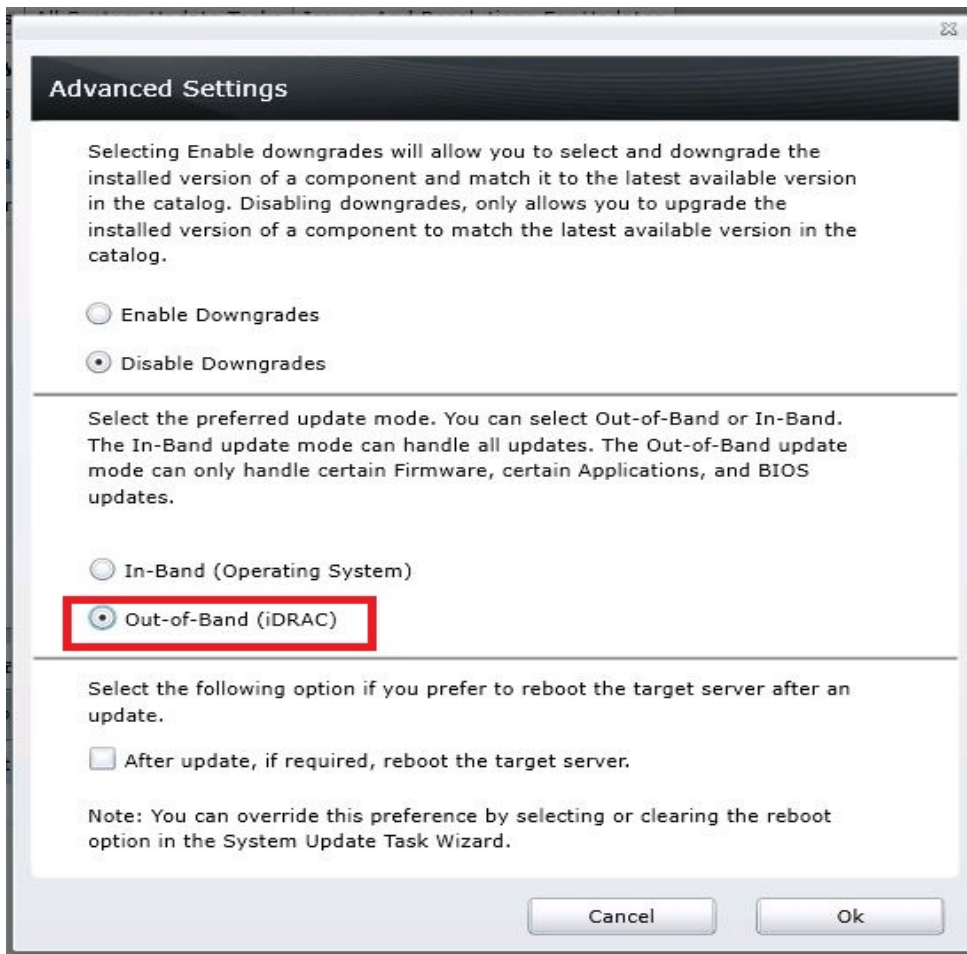


Figure 10 Advanced Settings preferred update mode iDRAC

6. Download latest catalog. See [Obtaining the latest version of update packages](#).
7. If the discovered iDRAC is non-compliant, click the **Non-Compliant** tab.
8. Ensure that the **User Preferred Delivery Mode** is set to **Out-of-Band**.
9. Select the iDRAC that is non-compliant and the package to be updated on the system and click **Apply Selected Updates**.
10. When the **User Preferred Delivery Mode** is set to iDRAC, the **Update Method** will display **Out-of-Band** for all the available components (DUPs).

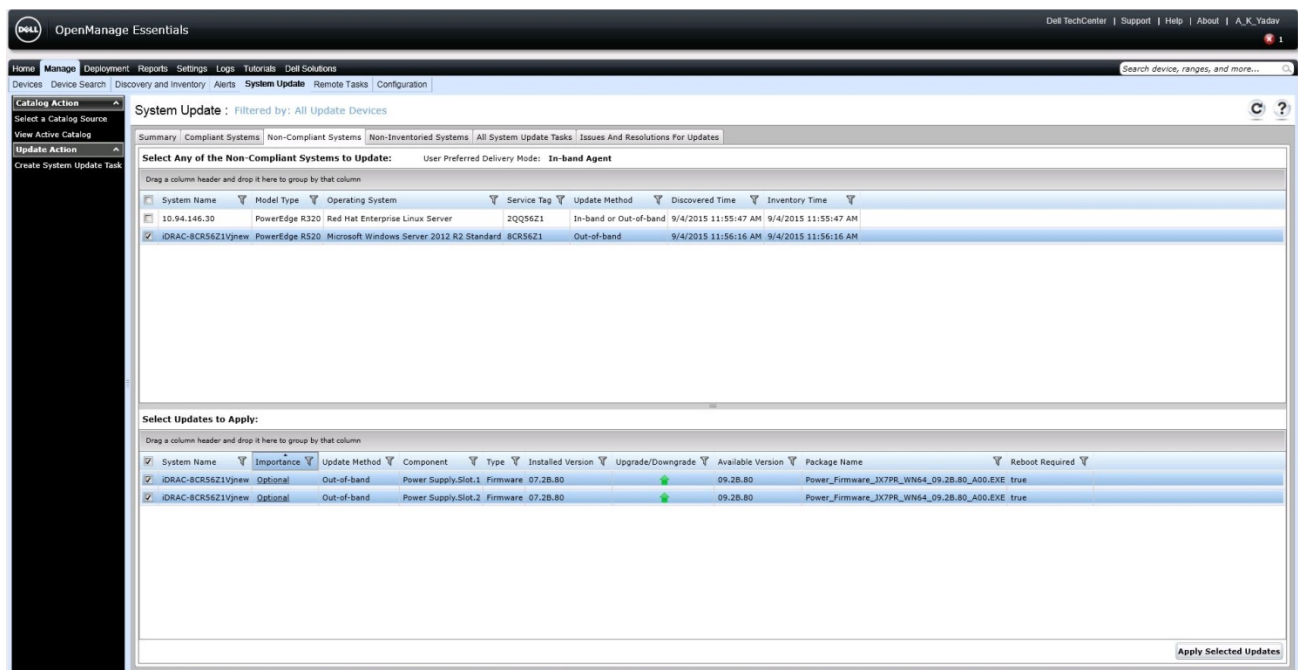


Figure 11 iDRAC Non-Compliant Report

The **System Update Task** window is displayed.

11. Type the task name.
12. Enter the task name and set the task schedule – select the **Run now** or **Set Schedule** option.
13. Enter the user name and password of the iDRAC.
14. Click **Finish** to create system update task.

System Update Task

Task Name: System Update Task - 9/18/2015 3:32:48 PM

<input checked="" type="checkbox"/> System Name	Importance	Delivery Mode	Component	Type	
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Optional	Out-of-band	Enterprise UEFI Diagnostics, 4225A2, 4225.4	Application	4
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Optional	Out-of-band	OS Drivers Pack, 7.2.1.4, A00	Application	7
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Recommended	Out-of-band	[0144] Broadcom BCM57810 NetXtreme II 10 GigE #144	Firmware	7
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Recommended	Out-of-band	BIOS	BIOS	1
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Recommended	Out-of-band	iDRAC	Firmware	1
<input checked="" type="checkbox"/> bdcomi01.blr.amer.dell.com	Recommended	Out-of-band	PERC H710P Mini Controller 0	Firmware	2

Set the Task Schedule:

☐ Run now
 ☐ After update, if required, reboot the target server.

☒ Set schedule 9/18/2015 3:42 PM (UTC+05:30)
 ☐ Skip Signature and Hash Check

☐ Before update, cancel all scheduled iDRAC jobs

Enter Credentials for the task execution:

iDRAC User Name:

iDRAC Password:

Figure 12 Create out-of-band system update task

Note: Select **Skip Signature and hash check** to skip the signature and hash check.

The system update task is created with the name provided and "- iDRAC" appended to the task name. This indicates that the preferred mode of delivery is Out-of-Band. The task remains in a pending state when the packages are being downloaded to the local system running OpenManage Essentials. After the packages are downloaded, the task status changes to **Running**. After all the selected components (DUPs) are successfully applied on the selected managed system, the task status is set to **Complete**. About 20 minutes after the task is completed, an auto inventory task is initiated to gather the updated inventory information.

To view the execution details of the task, double-click the task or right-click the task and select **Details**.

To copy the execution details result, click **Copy Results**.

The screenshot displays the Dell OpenManage Essentials interface. The top navigation bar includes the Dell logo, 'OPENMANAGE ESSENTIALS', and links for Dell TechCenter, Support, Help, About, and Administrator. Below this, a secondary navigation bar shows 'Home', 'Manage', 'Reports', 'Preferences', 'Logs', 'Tutorials', and 'Extensions'. The main content area is titled 'System Update' and is filtered by 'All Update Devices'. It features a sidebar on the left with 'Catalog Section' and 'View Active Catalog'. The main panel has tabs for 'Summary', 'Compliant Systems', 'Non-Compliant Systems', 'Non-Inventoried Systems', 'All System Update Tasks', and 'Issues And Resolutions For Updates'. The 'All System Update Tasks' tab is active, showing a table of tasks. Below this, a 'Task Execution History' section shows a table of task execution details.

Task Name	Task Label	Start Time
System Update Task - 10/22/2012 2:32:12 PM - iDRAC	iDRAC Server Software Update task.	10/22/2012 2:42:00 PM
Import Catalog for System Update	Import Dell Version Control Catalog for System Update from selected source.	10/22/2012 2:23:41 PM

Status	Task Name	Start Time	% Completed	Task State	Successful	End Time	Executed by User
	System Update Task - 10/22/2012 2:32:12 PM - iDRAC		0%	Pending	0 / 0		WIN-ROM4HPF6MJR\Administrator
	Import Catalog for System Update	10/22/2012 2:23:41 PM	100%	Complete	0 / 0	10/22/2012 2:23:	WIN-ROM4HPF6MJR\Administrator

Figure 13 Out-of-band (iDRAC) system update task execution status

Note: If update package requires a reboot and **After update, if required, reboot the Target server** is selected, then the server will be rebooted after the system update task is complete. An inventory task runs automatically 20 minutes after system update task is completed and inventory of the server will be updated.

In OpenManage Essentials version 2.1, a new option is available to clear the iDRAC jobs before starting system update operation.

System Update Task

Task Name: Out of band system update task

<input checked="" type="checkbox"/>	System Name	Importance	Delivery Mode	Component
<input checked="" type="checkbox"/>	172.16.2.171	Optional	Out-of-band	Dell 32 Bit Diagnostics, v.5118A0, 5118.3
<input checked="" type="checkbox"/>	172.16.2.171	Recommended	Out-of-band	BIOS
<input checked="" type="checkbox"/>	172.16.2.171	Recommended	Out-of-band	Broadcom NetXtreme II Gigabit Ethernet (BCM5709)
<input checked="" type="checkbox"/>	172.16.2.171	Recommended	Out-of-band	Dell Unified Server Configurator - Lifecycle Controller Enabled, v.1.1.0.188, A00
<input checked="" type="checkbox"/>	172.16.2.171	Recommended	Out-of-band	Drvr
<input checked="" type="checkbox"/>	172.16.2.171	Recommended	Out-of-band	iDRAC6

Set the Task Schedule:

☐ Run now
 ☒ Set schedule
 9/18/2015 8:00 AM (UTC+05:30)

☐ After update, if required, reboot the target server.
☐ Skip Signature and Hash Check
☒ Before update, cancel all scheduled iDRAC jobs

Enter Credentials for the task execution:

iDRAC User Name:
 iDRAC Password:

Figure 14 Out-of-band (iDRAC) - cancel iDRAC jobs

When the **Before update, cancel all scheduled iDRAC jobs** option is selected, OpenManage Essentials sends a Clear_All request to the iDRAC. This will clear the job queue in the target iDRAC.

Use this feature if you have any pending jobs in iDRAC job queue which is impacting system update.

Direct versus Staged Updates

The updates supported on Dell PowerEdge servers can be classified into Direct and Staged updates:

- Direct updates are those that do not require a server restart for the update to take effect.
- Staged updates are updates where the updates are staged and are applied only when the server is restarted. Lifecycle Controller is invoked during the server startup.

Direct updates	Staged updates
Lifecycle Controller	BIOS
iDRAC firmware	NIC firmware
Diagnostics	RAID firmware
OS driver pack	Backplane firmware
Identity module	PSU firmware
	CPLD

Note: iDRAC and driver pack updates on 11th generation and prior PowerEdge servers are staged updates. For 12th and later generations of PowerEdge servers, the iDRAC and OS driver pack updates are direct updates.



5 System updates on correlated devices – servers and iDRACs

Correlation is the process of relating resources to each other. OpenManage Essentials manages and identifies the relationship between resources (server and iDRAC) that are discovered using different protocols.

Dell PowerEdge servers can be updated using both the OMSA and iDRAC method. IT administrator can use the OMSA and iDRAC update method when there is a specific requirement to update system components, BIOS, firmware, applications and drivers, or only BIOS, firmware and applications respectively.

Correlation of servers is supported as follows:

- Perform discovery and inventory of Dell PowerEdge server SNMP [server IP address] and WS-Man [iDRAC IP address] – Windows and Linux operating systems.
- Perform discovery and inventory of Dell PowerEdge server WMI [server IP address] and WS-Man [iDRAC IP address] – Only Windows operating systems.

To update correlated devices after performing discovery and inventory described earlier:

1. Click **System Update** and import a latest catalog (perferred online). See [Obtaining the latest version of update packages](#).
2. Perform system updates using one of the following methods:
 - a. In-band as the preferred update mode. See [In-Band System Updates](#).
 - b. Out-of-Band as the preferred update mode. See [Out-Of-Band System Updates \(iDRAC\)](#).



6 In-band system update task (Linux) using sudo users

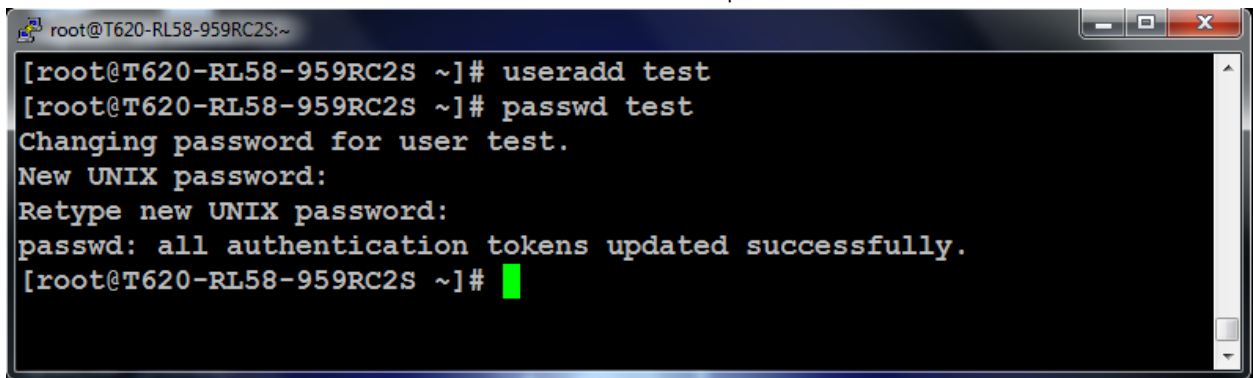
In a Linux environment, an IT administrator may manage Dell PowerEdge servers running various Linux distributions (for example, Red Hat Enterprise Linux and SUSE Linux Enterprise Server) using the OpenManage Server Administrator (OMSA) agent installed on it.

Using OpenManage Essentials an IT administrator can perform system updates on servers running Linux, using sudo (non-root) user authentication. This feature is helpful when the IT administrator has created a security policy on the root user.

Note: Applying system updates using sudo is not supported for target servers running SUSE Linux Enterprise.

6.1 Configuring a sudo user in Linux

1. Login to the Linux server through SHH (putty) as a root user.
2. Create a new user and authenticate the user with a password.

A terminal window titled 'root@T620-RL58-959RC2S:~' showing the execution of commands to create a new user. The commands are 'useradd test' and 'passwd test'. The output shows the password being set for the user 'test' and a confirmation message: 'passwd: all authentication tokens updated successfully.'

```
root@T620-RL58-959RC2S:~  
[root@T620-RL58-959RC2S ~]# useradd test  
[root@T620-RL58-959RC2S ~]# passwd test  
Changing password for user test.  
New UNIX password:  
Retype new UNIX password:  
passwd: all authentication tokens updated successfully.  
[root@T620-RL58-959RC2S ~]#
```

Figure 15 Creating a Linux user.

3. Edit the sudoers file using the 'visudo' command and add the following:
Cmnd_Alias OMEUPDATE = /bin/tar,
/opt/dell/srvadmin/bin/omexec,/tmp/LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackag
e/omexec <sudo_user_name> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE

```
root@T620-RL58-959RC2S:~  
## Sudoers allows particular users to run various commands as  
## the root user, without needing the root password.  
##  
## Examples are provided at the bottom of the file for collections  
## of related commands, which can then be delegated out to particular  
## users or groups.  
##  
## This file must be edited with the 'visudo' command.  
  
## Host Aliases  
## Groups of machines. You may prefer to use hostnames (perhaps using  
## wildcards for entire domains) or IP addresses instead.  
# Host_Alias      FILESERVERS = fs1, fs2  
# Host_Alias      MAILSERVERS = smtp, smtp2  
  
## User Aliases  
## These aren't often necessary, as you can use regular groups  
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname  
## rather than USERALIAS  
# User_Alias      ADMINS = jsmith, mikem  
  
## Command Aliases  
## These are groups of related commands...  
  
## Networking  
# Cmnd_Alias      NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool  
  
Cmnd_Alias OMEUPDATE = /bin/tar, /opt/dell/srvadmin/bin/omexec, /tmp/LinuxPreInstallPackage/runbada, /tmp/LinuxPreInstallPackage/omexec test ALL=OMEUPDATE, NOPASSWD:OMEUPDATE  
  
## Installation and management of software  
-- INSERT --
```

Figure 16 Editing the sudoers file

4. Ensure that you are able to log in to the server running Linux through SSH (putty) as a sudo user.

```
test@T620-RL58-959RC2S:~  
login as: test  
test@10.94.173.179's password:  
[test@T620-RL58-959RC2S ~]$ cd /home/test  
[test@T620-RL58-959RC2S ~]$ ls  
[test@T620-RL58-959RC2S ~]$ pwd  
/home/test  
[test@T620-RL58-959RC2S ~]$
```

Figure 17 Logging in as a sudo user

5. After the sudo user configuration is successful, perform discovery and inventory of the Linux server in OpenManage Essentials using the SNMP protocol.
6. Create an in-band system update task for the server running Linux, select the **Enable Sudo** option, and provide the sudo user credentials required for the running the task.
7. Click **Finish** to run the task.

23

System Update Task

Task Name:

System Update Task - 7/25/2013 3:05:37 PM

<input checked="" type="checkbox"/>	System Name	Importance	Delivery Mode	Component	Type	Installed Version
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Critical	OMSA	12G iDRAC7 BASE V1.00	Firmware	1.30.30
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Critical	OMSA	ST9146853SS	Firmware	YS08
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Optional	OMSA	Enterprise UEFI Diagnostics, 4217A5, 4217.8	Application	4217A5
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Optional	OMSA	Lifecycle Controller, 1.1.0.1108, A00	Application	1.1.0.1108
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Optional	OMSA	OS Drivers Pack, 7.2.1.4, A00	Application	7.2.1.4
<input checked="" type="checkbox"/>	win-m089cl4rbu3.dmc-ad.com	Recommended	OMSA	PERC H710 Adapter Controller 0	Firmware	21.1.0-00

Set the Task Schedule:

☐ Run now
 ☒ Set schedule

7/25/2013 3:15 PM (UTC-08:00)

☒ After update, if required, reboot the device.
 ☒ Skip Signature and Hash Check

Enter Credentials for the task execution:

☒ Enable Sudo

SSH Port number: 22

Server User Name: test

Server Password:

Help

Cancel

Finish

Figure 18 System update task – Enable Sudo

7 System update using the guided wizard

From OpenManage Essentials version 2.1 onwards, you can apply updates on servers using a **Guided Wizard** accessible from the **System Update** portal.

To access the wizard, click **System Update**→ **Update Action**→ **Create System Update Task**.

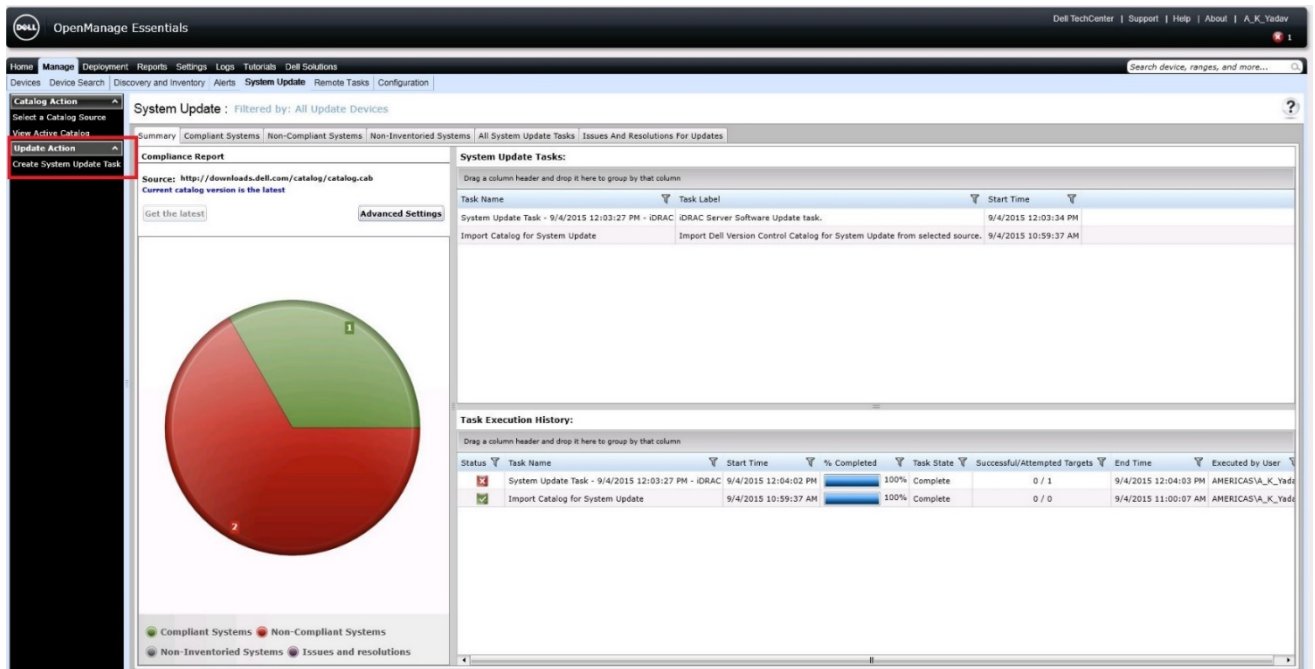


Figure 19 System update wizard

When you click **Create System Update Task**, a wizard that guides you through the selection of Non-Compliant Systems and Applicable Packages is displayed.

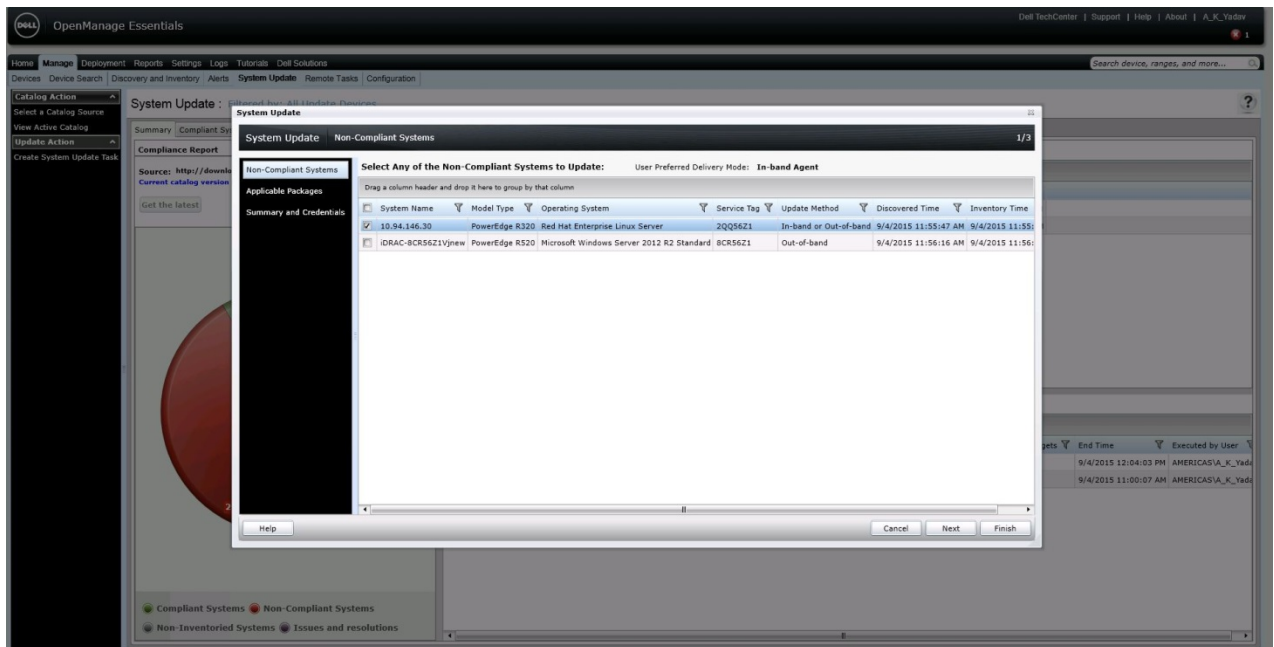


Figure 20 System update wizard – Non-Compliant Systems

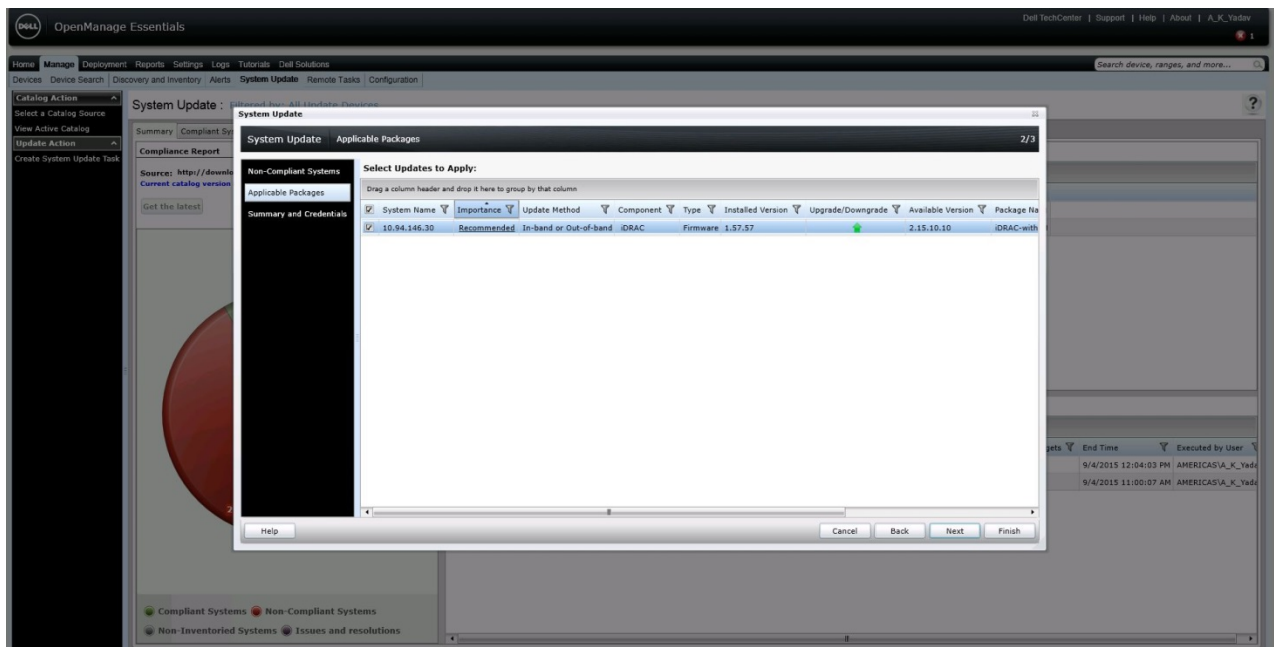


Figure 21 System update wizard – Applicable Packages

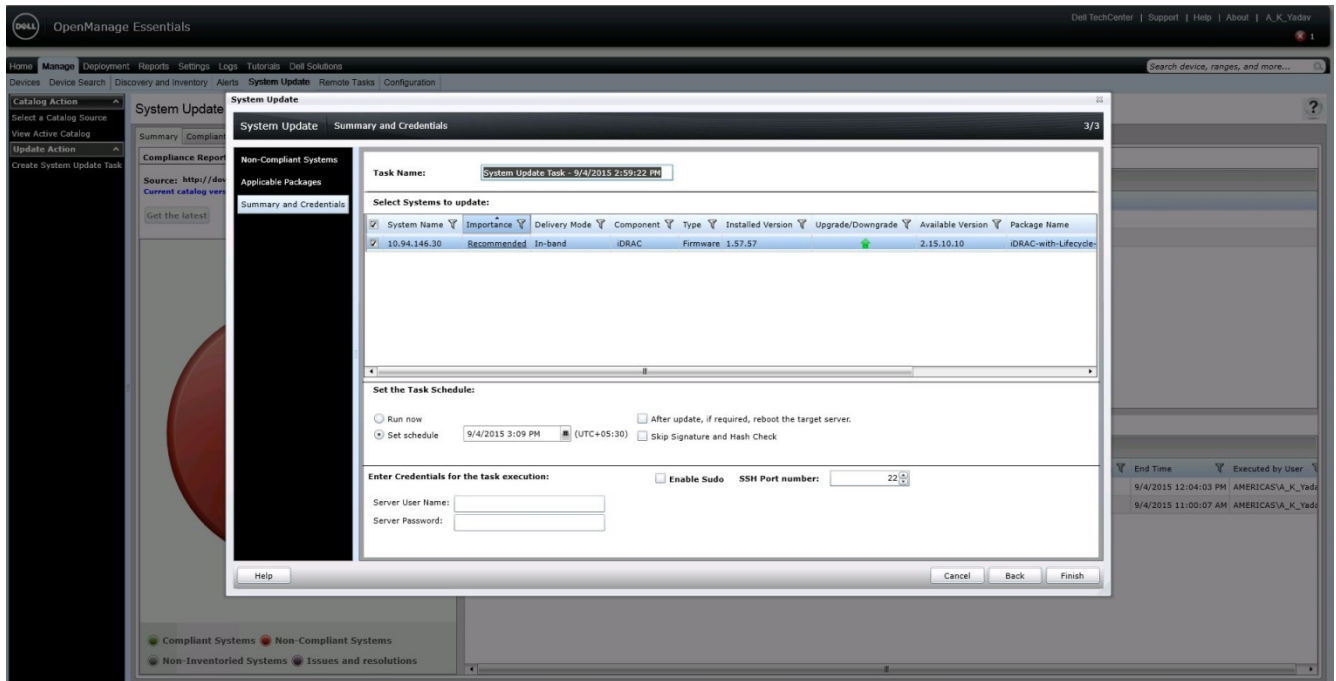


Figure 22 Credentials page of the system update wizard

After you click **Finish**, a task is created in the system update portal. The result of the task is displayed in the in execution details.

8 System Update – Run Option

The **Run** option in **System Update Tasks** enables you to re-run completed system update tasks. For example, you can re-run the **Import Catalog for System Update** task and other in-band and out-of-band system update tasks that you have created.

After a system update task is complete, if some components fail to update on a target, you can use the **Run** option to re-run the system update task. Instead of creating a new system update task to apply the components that failed, you can use the Run option to re-run the system update task and apply the components that failed. For example, if a system update task has five components to update, but only three components are applied successfully and the other two components have failed, you can use the **Run** option to re-run the system update task and apply the components that failed.

To re-run a system update task, right-click on the system updated task and then click **Run**.

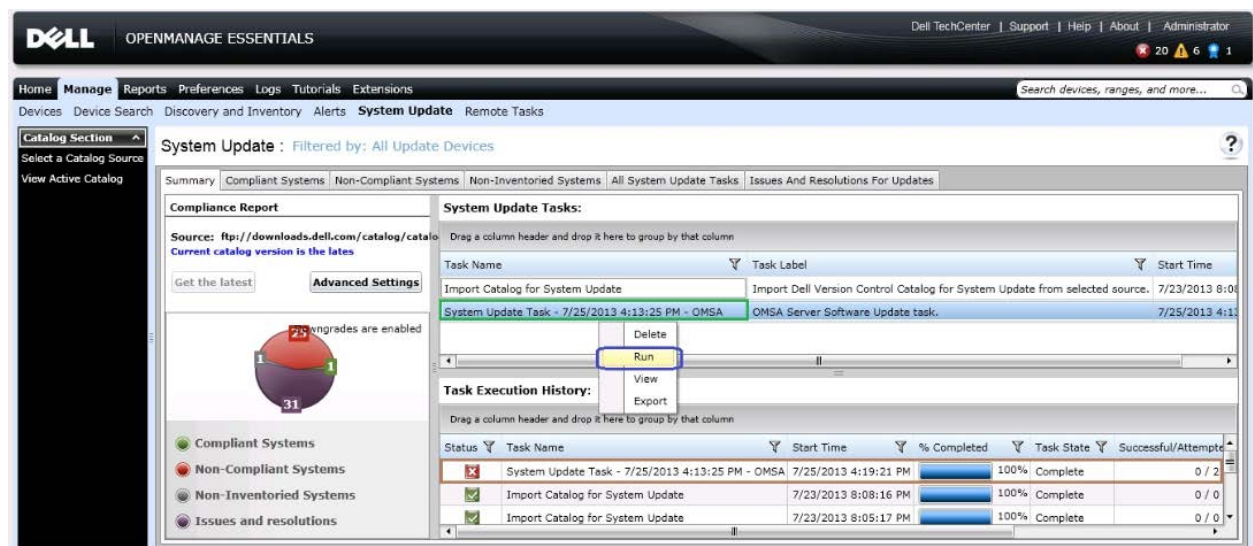


Figure 23 Running a system update task

Note: The **Run** option is not supported for a system update task that is already running. For more information, see the [FAQs](#).

You can also re-run the Import Catalog for System Update task. See Figure 24.

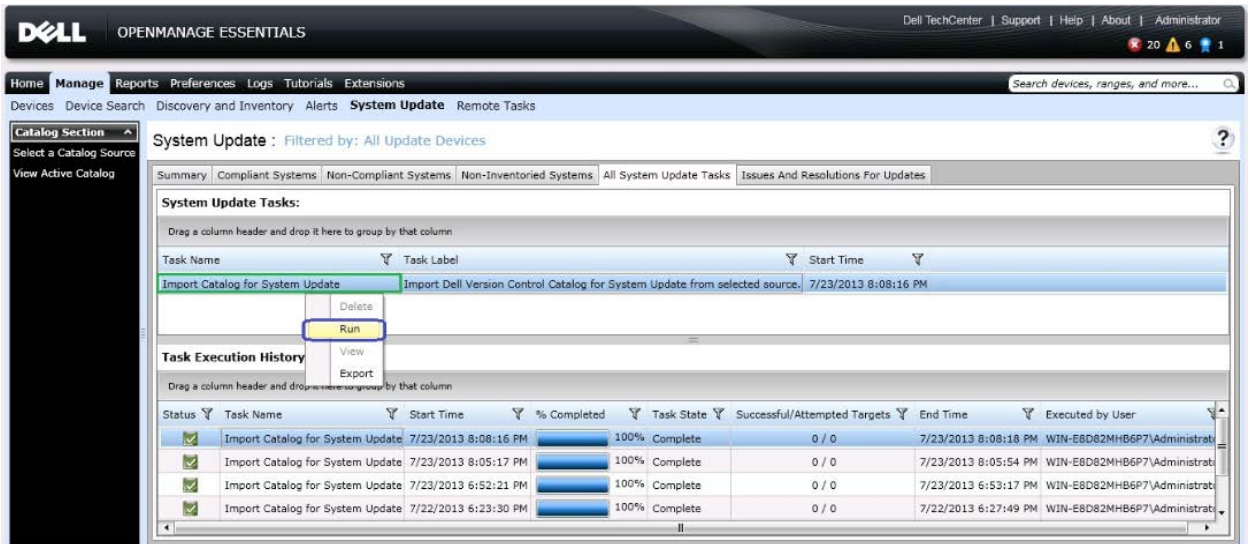


Figure 24 Running the Import Catalog for System Update task

9 Initiating firmware and driver inventory

Firmware and driver inventory has been designed as a remote task considering following scenarios:

1. Should be independent of discovery/inventory cycle since it might increase the time to discover/inventory the system
2. Should be able to run whenever needed
3. Should be able to schedule for a later time
4. Should be able to have a recurrent schedule
5. Should be able to use different credentials than discovery/inventory

The firmware and driver inventory task can be created in following ways:

- From the Remote Tasks portal
- From the System Update portal

9.1 Creating the firmware and driver inventory task from the Remote Tasks portal

1. Click **Manage**→ **Remote Tasks**→ **Create F/W & Driver Inventory Task**.

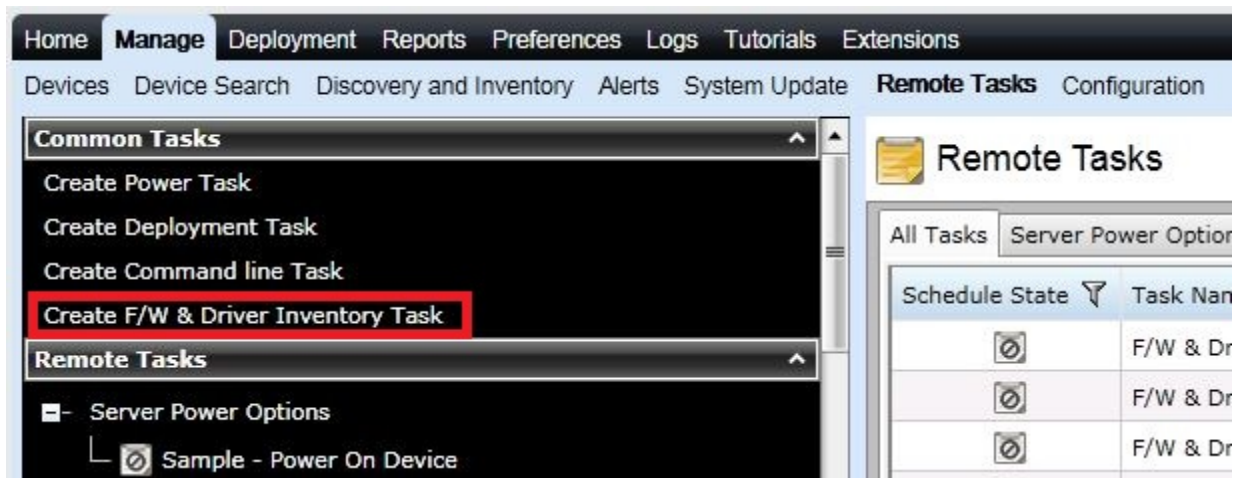


Figure 25 Remote Task – Firmware & Driver Inventory Task - launch point

2. The **Create Firmware & Driver Inventory Task** wizard will open with a default name for the task. If required you can modify the name.

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Task Name F/W & Driver Inventory Task - 9/14/2015 11:11:38 AM

Note: This task will deploy a inventory collection component on the target devices. The component will be removed after the task is completed.

☒ Filter devices based on Operating system

Select the Operating System

☒ Windows
☐ Linux
☐ 64-bit System

☐ Show OMSA based targets

Future Software Inventory Data Controlled by:

☒ OMSA based inventory
☐ F/W and Driver task based inventory*

Help Cancel Next Finish

Figure 26 Firmware & Driver Inventory Task – Task Name

3. The wizard provides an option to filter the servers based on the operating system type. The highlighted check box shown in Figure 5 can be used to enable/disable the filtering.

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Task Name F/W & Driver Inventory Task - 9/14/2015 11:11:38 AM

Note: This task will deploy a inventory collection component on the target devices. The component will be removed after the task is completed.

☒ Filter devices based on Operating system

Select the Operating System

☒ Windows
☐ Linux
☐ 64-bit System

☐ Show OMSA based targets

Future Software Inventory Data Controlled by:

☒ OMSA based inventory
☐ F/W and Driver task based inventory*

Help Cancel Next Finish

Figure 27 Firmware & Driver Inventory Task – Filter devices based on the operating system

4. You can also group/filter the servers based on the following operating system types:

- Windows – 32 bit
- Windows – 64 bit
- Linux – 32 bit
- Linux – 64 bit

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Task Name F/W & Driver Inventory Task - 9/14/2015 11:11:38 AM

Note: This task will deploy a inventory collection component on the target devices. The component will be removed after the task is completed.

☒ Filter devices based on Operating system

Select the Operating System

☒ Windows

☐ Linux

☐ 64-bit System

☐ Show OMSA based targets

Future Software Inventory Data Controlled by:

☒ OMSA based inventory

☐ F/W and Driver task based inventory*

Help Cancel Next Finish

Figure 28 Firmware & Driver Inventory Task – Select the Operating System

You can also configure the task wizard to display OMSA-based targets which will not be shown by default. This is a new addition in OpenManage Essentials version 2.1 which was necessary because of problems faced by users in the past, where OMSA was unable to provide the latest inventory details after performing a system update from OpenManage Essentials. In some cases, users had to restart OMSA services (or) the managed node itself to get the correct inventory details. The show OMSA based targets option is useful in these scenarios.

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Task Name F/W & Driver Inventory Task - 9/14/2015 11:57:23 AM

Note: This task will deploy a inventory collection component on the target devices. The component will be removed after the task is completed.

☒ Filter devices based on Operating system

Select the Operating System

☐ Windows
☐ Linux
☐ 64-bit System

☒ Show OMSA based targets

Future Software Inventory Data Controlled by:

☐ OMSA based inventory
☒ F/W and Driver task based inventory*

*Select this option only if you want to always use the F/W Driver inventory task to collect software inventory, even though OMSA is present on the device.

[Note] If you want to revert to the OMSA inventory, you must either select "OMSA based inventory" option and then run the F/W Driver inventory task or delete the device and rediscover it again.

Help Cancel Next Finish

Figure 29 Firmware and Inventory task – Show OMSA based targets

The future software inventory option controls the decision of following:

1. After performing a system update, which inventory should be triggered to collect software inventory?
2. On any inventory cycle (scheduled/user initiated), should the data from OMSA be considered for software inventory?

Based on the selection & execution of the task, software inventory will be controlled by either OMSA or the Firmware & Driver inventory collection task.

Future software inventory - selection	Inventory after system update task		Scheduled/user created inventory	
	Inventory type	Software inventory data updated by	Inventory type	Software inventory data updated by
OMSA based	OMSA – full inventory	OMSA	OMSA – full inventory	OMSA
F/W and driver inventory task based	OMSA – full inventory + F/W and driver inventory	F/W and driver inventory	OMSA full inventory	No update with regular inventory cycle User has to schedule the F/W inventory task

Important points:

- i. This selection is applicable only for target servers that have OMSA installed. For target servers that do not have OMSA installed, by default, the F/W and Driver inventory collection task runs after the system update.
- ii. If both the server and iDRAC of the server are discovered using the preferred protocols, the iDRAC software inventory takes precedence for the components found in both the in-band and out-of-band inventory. Driver components which are not included in the out-of-band inventory are taken from the in-band inventory.

Note: The selection is preserved only **after the successful completion** of the F/W inventory collection task. Therefore, if you make modifications, you must ensure that the F/W inventory task runs once again to preserve the preference.



5. On **Task Target**, you can select the servers from the list as shown in Figure 8.

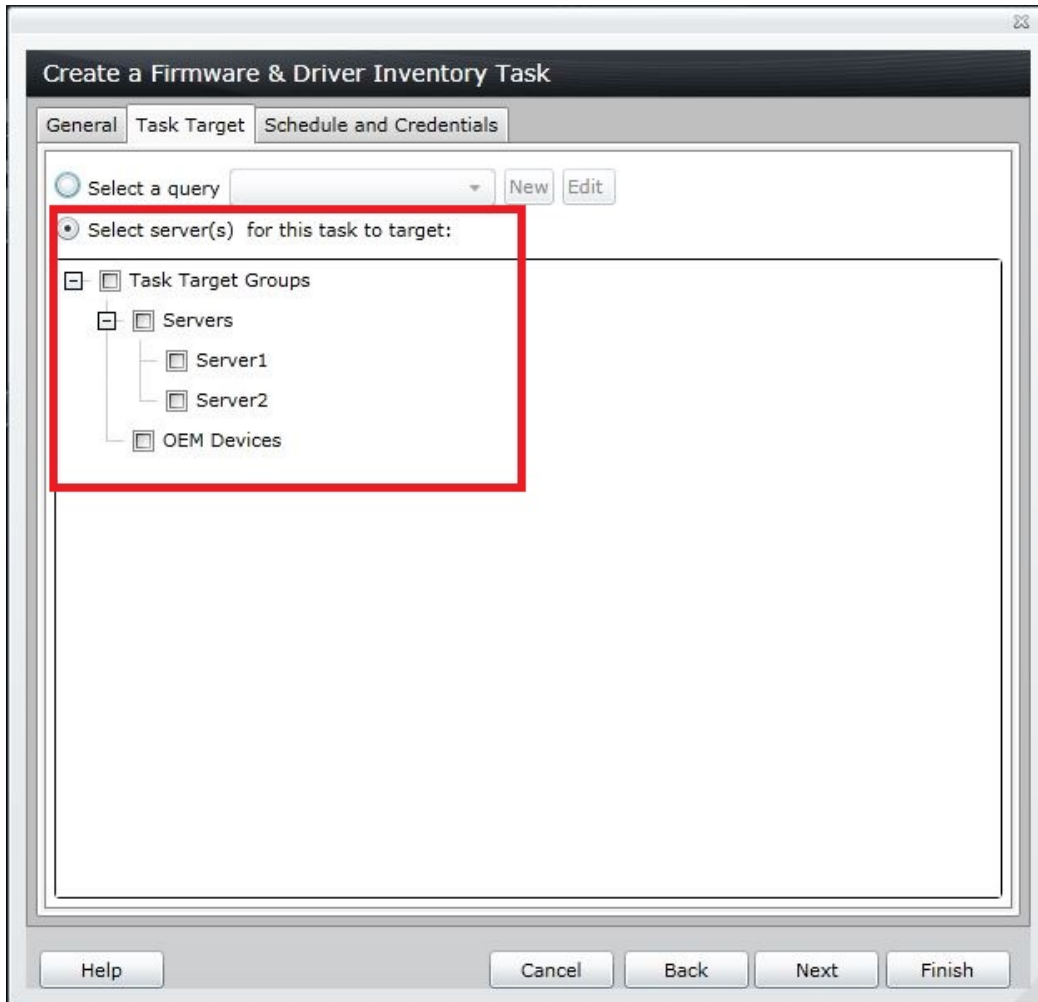


Figure 30 Firmware & Driver Inventory Task – Select Target

6. If required, you can also select the devices from a query.

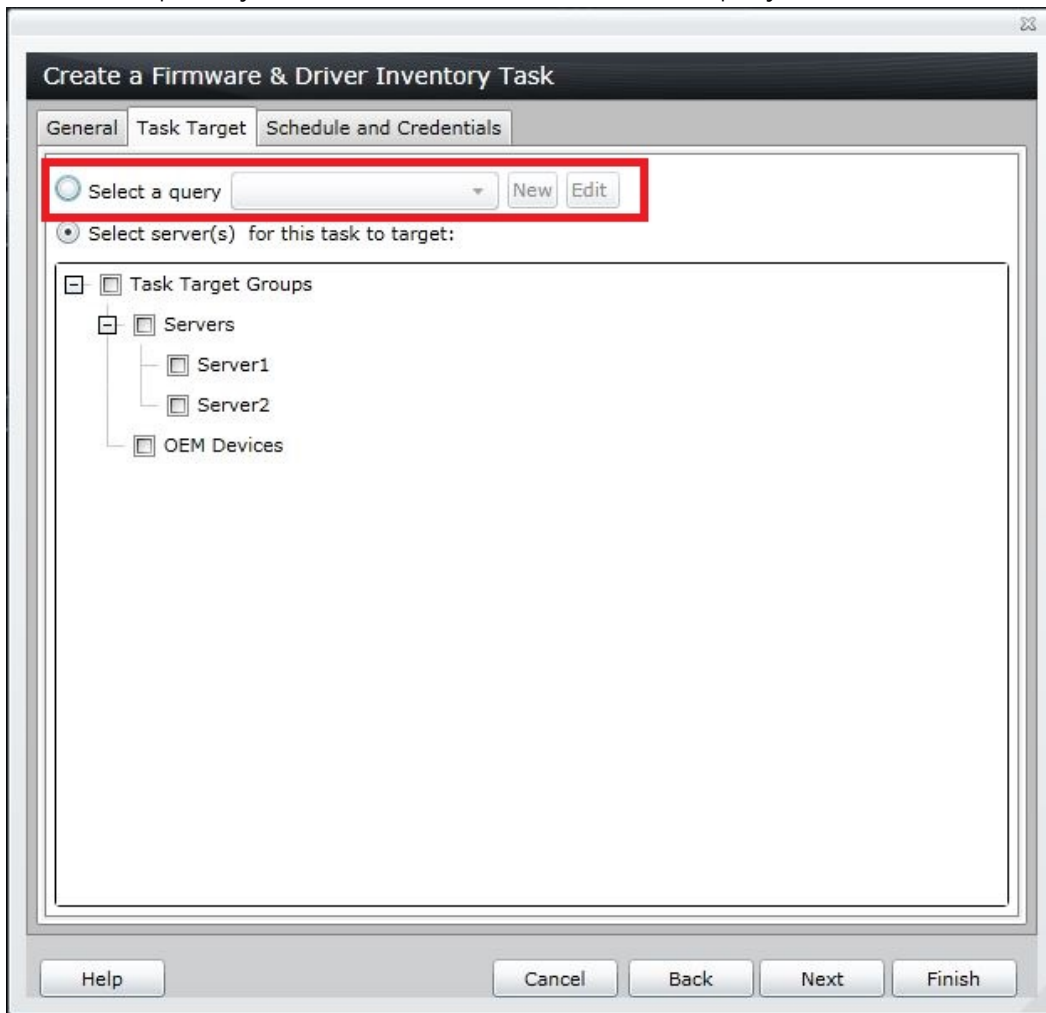


Figure 31 Firmware & Driver Inventory task – Select a query

7. If OMSA based targets are chosen for the task, by default, those targets will be disabled. To be able to select those targets, you must select the **Enable All** option.

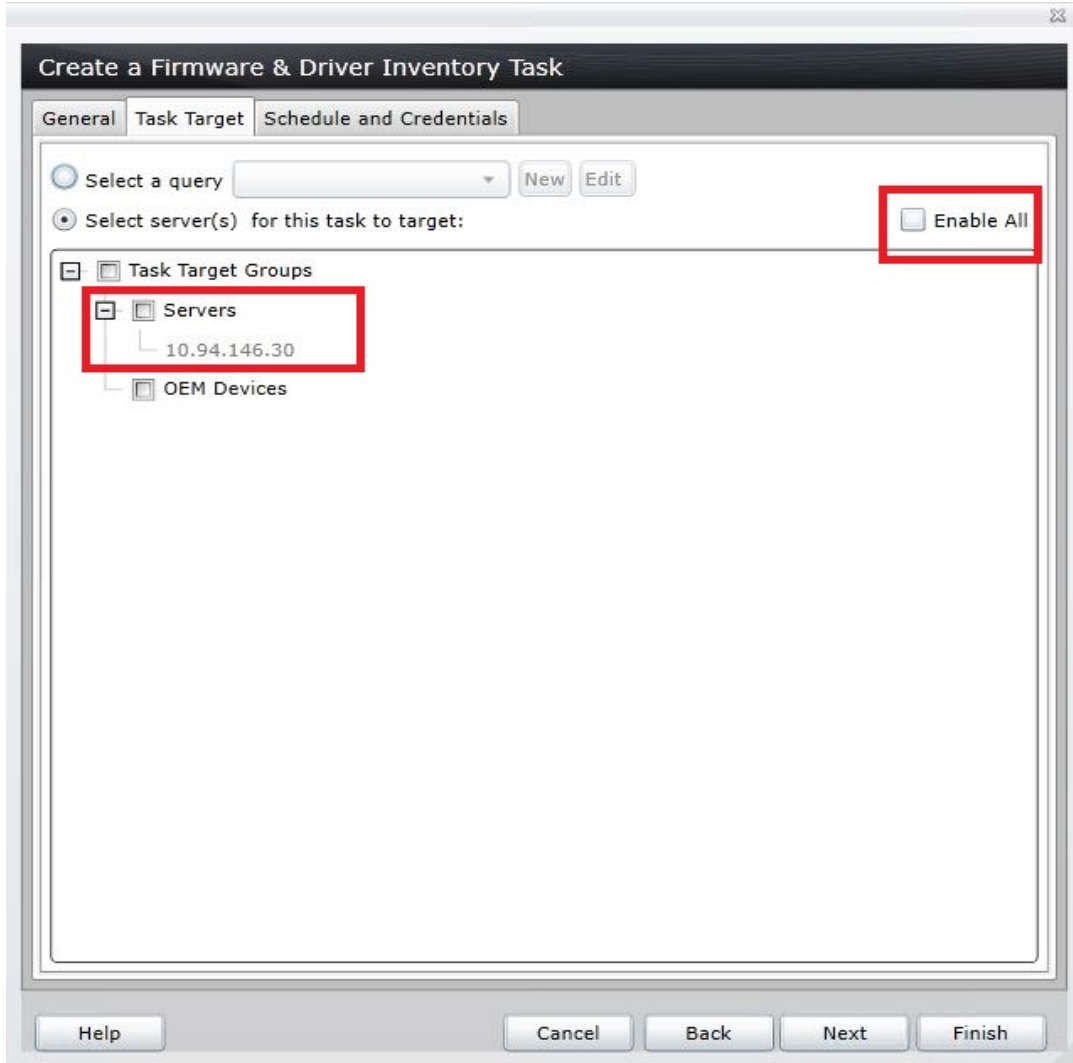


Figure 32 Firmware & Driver Inventory task – Enable All option for OMSA based targets

8. In **Schedule and Credentials**, by default, a schedule is selected as shown in Figure 11.

The screenshot shows a Windows-style dialog box titled "Create a Firmware & Driver Inventory Task". It has three tabs: "General", "Task Target", and "Schedule and Credentials", with the last one being active. The "Set schedule:" section has a checked "Activate Schedule" checkbox and four radio button options: "Run now", "Set schedule", "Run Once", and "Periodic". The "Set schedule" option is selected and highlighted with a red rectangle. Next to it is a date and time field showing "8/26/2014 11:26 AM" and a time zone field showing "(UTC+05:30)". Below this is the "Enter credentials of the remote target(s)" section, which includes a placeholder text "<domain>\<user name> or localhost\<user name>" and two input fields labeled "User Name:" and "Password:". At the bottom of the dialog are four buttons: "Help", "Cancel", "Back", and "Finish".

Figure 33 Firmware & Driver Inventory Task –Set schedule

9. You can also choose the **Run now** button to initiate the task immediately as shown in Figure 12.

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Set schedule:

☒ Run now

☐ Set schedule 8/26/2014 11:26 AM (UTC+05:30)

☐ Run Once

☐ Periodic

☒ Activate Schedule

Enter credentials of the remote target(s)

<domain>\<user name> or localhost\<user name>

User Name:

Password:

Help Cancel Back Finish

Figure 34 Firmware & Driver Inventory Task – Run now

10. Type the credentials in the highlighted section shown in Figure 13.

Create a Firmware & Driver Inventory Task

General Task Target Schedule and Credentials

Set schedule: ☒ Activate Schedule

☐ Run now

☒ Set schedule 8/26/2014 11:26 AM (UTC+05:30)

☐ Run Once

☐ Periodic

Enter credentials of the remote target(s)

<domain>\<user name> or localhost\<user name>

User Name:

Password:

Help Cancel Back Finish

Figure 35 Firmware & Driver Inventory Task – Credentials

11. Click **Finish** to create the task.

9.2 Creating the firmware and driver inventory from the System Update portal

12. Click **Manage** → **System Update** → **Non-Inventoried Systems** tab.

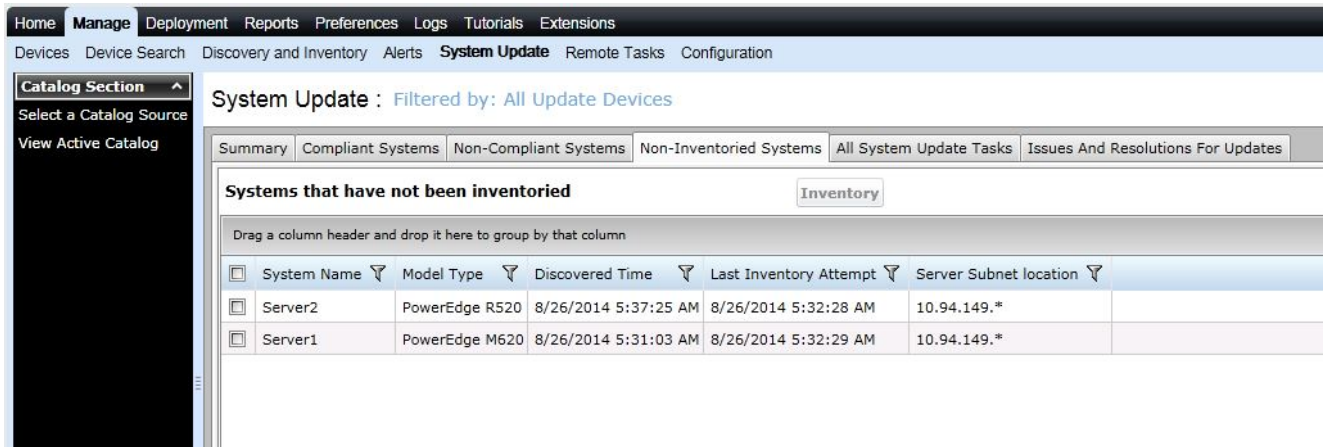


Figure 36 System Update Portal – Non inventoried Systems

13. From the list of servers that are displayed, select the server(s) and click **Inventory**.

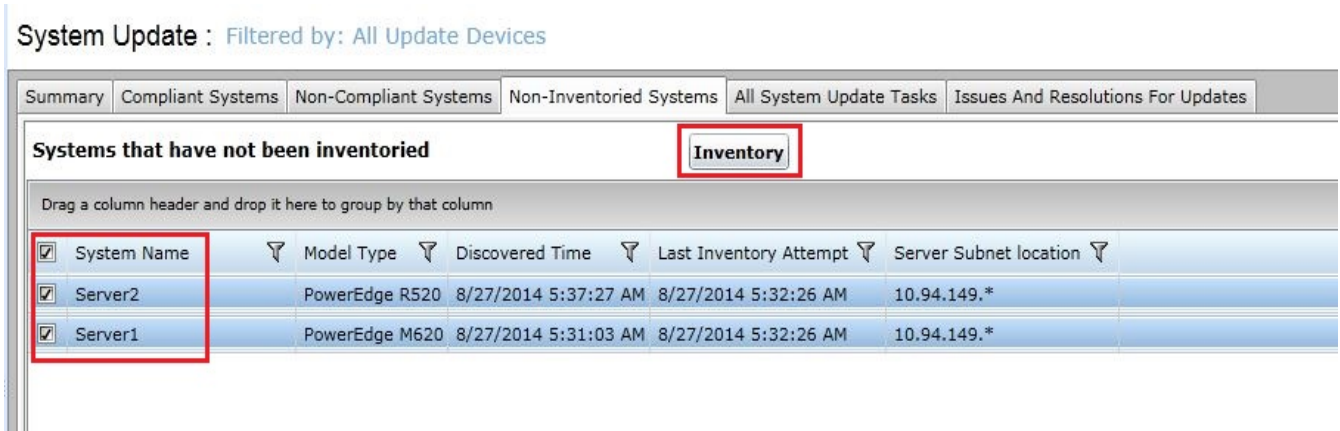


Figure 37 System update portal – Select the servers

14. If the device you have selected does not have OMSA installed, and is discovered using WMI/SSH, the Firmware and software inventory wizard will be displayed.

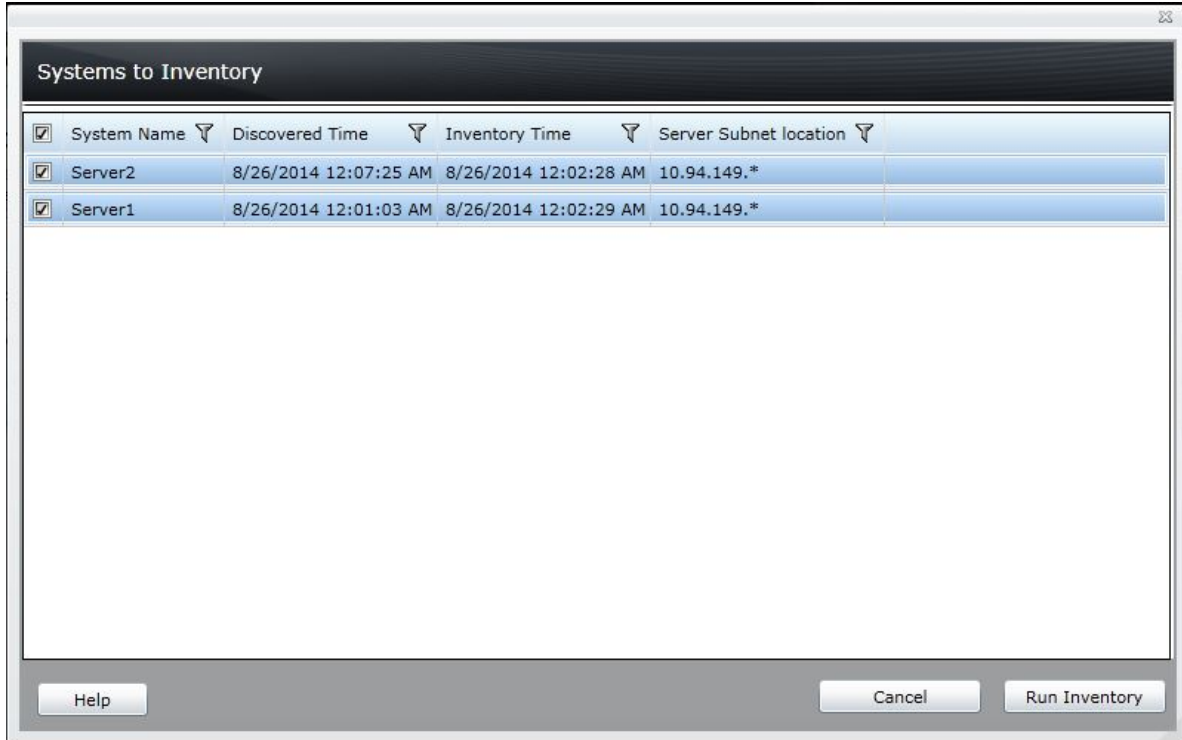


Figure 38 System update portal – Run inventory

15. Once you click **Run Inventory**, the **Create Firmware & Driver Inventory Task** wizard will be displayed. The servers which you selected in the previous step are pre-selected in the wizard. The **Run now** option is selected as well. To run the task, type the credentials, and click **Finish**.

The screenshot shows a wizard window titled "Create a Firmware & Driver Inventory Task". It has three tabs: "General", "Task Target", and "Schedule and Credentials", with the third tab being active. The "Set schedule:" section has a checkbox "Activate Schedule" which is unchecked. Below it are four radio button options: "Run now" (selected), "Set schedule" (with a date/time field showing "8/26/2014 11:30 AM" and a time zone "(UTC+05:30)"), "Run Once", and "Periodic". The "Enter credentials of the remote target(s)" section contains a placeholder text "<domain>\<user name> or localhost\<user name>" and two input fields labeled "User Name:" and "Password:". At the bottom are buttons for "Help", "Cancel", "Back", and "Finish".

Figure 39 System update portal – Firmware & Driver inventory wizard

If you want to change the name of the task, you can go to the **General** tab and make the modifications.

If you want to make modifications to the target servers, you can do so in the **Task Target** tab.

Note: If you select/clear the **Filter device based on Operating System** option, all the targets which are pre-selected will be cleared. To complete creating the task, you have to select the devices again.

10 Performing system update

After the firmware and driver inventory is collected from the target, it will be moved from the **Non-Inventoried Systems** tab to either the **Complaint Systems** or **Non Complaint Systems** tab based on whether the system is at par with the hardware baseline or not.

When the system is not at par with the hardware baseline, it will be listed under **Non Complaint Systems**. From there on, you can select in-band system update and proceed further for system update.

The screenshot shows the Dell OpenManage Essentials System Update portal. The top navigation bar includes Home, Manage, Deployment, Reports, Preferences, Logs, Tutorials, and Extensions. The left sidebar has a 'Catalog Section' dropdown and a 'View Active Catalog' link. The main content area is titled 'System Update : Filtered by: All Update Devices'. Below this, there are tabs for Summary, Compliant Systems, Non-Compliant Systems, Non-Inventoried Systems, All System Update Tasks, and Issues And Resolutions For Updates. The 'Non-Compliant Systems' tab is active. It shows a table of systems with columns: System Name, Model Type, Operating System, Service Tag, Update Method, Discovered Time, and Inventory Time. Two systems are listed: Server1 (PowerEdge M620, Microsoft Windows Server 2008 R2 Enterprise x64 Edition, 5K6ZWX1, In-band) and Server2 (PowerEdge R520, Microsoft Windows Server 2012 R2 Datacenter x64 Edition, 8CR56Z1, In-band). Below this table, there is a section 'Select Updates to Apply:' with a table of updates. The updates table has columns: System Name, Importance, Update Method, Component, Type, Installed Version, Upgrade/Downgrade, and Available Version. Four updates are listed for Server1: [0156] Broadcom BCM57810 NetXtreme II 10 GigE #156 (Firmware, 7.6.15, Upgrade), BIOS (BIOS, 1.6.1, Upgrade), iDRAC (Firmware, 1.50.50.00, Upgrade), and PERC H710P Mini Controller 0 (Firmware, 21.2.1-0000, Upgrade). An 'Apply Selected Updates' button is at the bottom right.

System Name	Model Type	Operating System	Service Tag	Update Method	Discovered Time	Inventory Time
Server1	PowerEdge M620	Microsoft Windows Server 2008 R2 Enterprise x64 Edition	5K6ZWX1	In-band	8/28/2014 5:31:04 AM	8/28/2014 5:32:35 AM
Server2	PowerEdge R520	Microsoft Windows Server 2012 R2 Datacenter x64 Edition	8CR56Z1	In-band	8/28/2014 5:37:24 AM	8/28/2014 5:32:34 AM

System Name	Importance	Update Method	Component	Type	Installed Version	Upgrade/Downgrade	Available Version
Server1	Recommended	In-band	[0156] Broadcom BCM57810 NetXtreme II 10 GigE #156	Firmware	7.6.15	Upgrade	7.8.53
Server1	Recommended	In-band	BIOS	BIOS	1.6.1	Upgrade	2.2.10
Server1	Recommended	In-band	iDRAC	Firmware	1.50.50.00	Upgrade	1.57.57
Server1	Recommended	In-band	PERC H710P Mini Controller 0	Firmware	21.2.1-0000	Upgrade	21.3.0-0009

Figure 40 System update portal – Non-Complaint Systems tab

10.1 Linux system update as a “sudo” user

For the Linux servers displayed in the **System Update** portal, OpenManage Essentials provides the option of using “sudo” credentials for updating the firmware/drivers.

The screenshot shows the 'System Update' portal with the 'Filtered by: All Update Devices' filter. The 'Select Any of the Non-Compliant Systems to Update' section shows a table with one system selected: 'Linux-Server' (PowerEdge M710, Red Hat Enterprise Linux Server release 6.4 (Santiago), 4CP362S, In-band, 8/28/2014 12:34:46 PM). The 'Select Updates to Apply' section shows a table with three updates selected:

System Name	Importance	Update Method	Component	Type	Installed Version	Upgrade/Downgrade	Available Version	Package Name
Linux-Server	Critical	In-band	PERC H200M Controller 0	Firmware	07.01.33.00	↑	07.02.42.00	RAID_FRMW_LX_R294622.BIN
Linux-Server	Optional	In-band	ST9500430SS	Firmware	DS62	↑	DS64	FRMW_LX_R277996.BIN
Linux-Server	Recommended	In-band	ST9500620SS	Firmware	AS02	↑	AS05	SAS-Drive_Firmware_DPVD9_LN32

The 'Apply Selected Updates' button is visible at the bottom right.

Figure 41 System update portal – Linux server select packages

The screenshot shows the 'System Update Task' dialog box. The 'Task Name' is 'System Update Task - 8/28/2014 12:47:29 PM'. The table shows the same three updates as in Figure 41. The 'Set the Task Schedule' section has 'Run now' selected. The 'Enter Credentials for the task execution' section has 'Enable Sudo' checked and 'SSH Port number' set to 22.

Task Name: System Update Task - 8/28/2014 12:47:29 PM

System Name	Importance	Delivery Mode	Component	Type	Installed Version	Upgrade/Downgrade
Linux-Server	Critical	In-band	PERC H200M Controller 0	Firmware	07.01.33.00	↑
Linux-Server	Optional	In-band	ST9500430SS	Firmware	DS62	↑
Linux-Server	Recommended	In-band	ST9500620SS	Firmware	AS02	↑

Set the Task Schedule:

☐ Run now ☒ Set schedule 8/28/2014 12:57 PM (UTC+05:30) ☒ After update, if required, reboot the device. ☐ Skip Signature and Hash Check

Enter Credentials for the task execution:

☒ Enable Sudo SSH Port number: 22

Server User Name:
Server Password:

Buttons: Help, Cancel, Finish

Figure 42 System update portal – Linux sudo

Even though the firmware and driver inventory collection task does not provide any option for “sudo” users, you can still use sudo option to update the server.

Note: When you update a target server that does not have a Dell agent, it is recommended not to use sudo credentials because you have to give NOPASSWD, EXECUTE permissions for the binaries which are copied and executed under the /tmp directory. If you still have to use sudo users, ensure that you have other security measures/mitigations in place if you have to update the server that does not have OMSA installed as a sudo user, edit the sudoers file using the visudo command, and add the following:

For target servers running a 32-bit operating system:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,  
/tmp/LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec,  
/tmp/invcol.bin  
<sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

For target servers running a 64-bit operating system:

```
Cmnd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec,  
/tmp/LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec,  
/tmp/invcol64.bin  
<sudo_username> ALL=OMEUPDATE,NOPASSWD:OMEUPDATE.
```

10.2 Scheduled Firmware & Driver Inventory collection task after update

When OMSA is installed on the target server, OpenManage Essentials refreshes the inventory details of the target 20 minutes after all the updates are applied,

Similarly, when the system update is applied on a target server that does not have OMSA installed, OpenManage Essentials runs the “firmware and driver inventory collection” task on the target server using the credentials provided for the task. This system task is scheduled to run 20 minutes after the update task is completed.

These system tasks will not have any entry as a “Task” in the task portal; instead they will be represented in the **Task Execution History**.

Task Status						
Task Name	Task State	% Completed	Start Time	End Time		
Scheduled F/W & Driver Inventory-10.94.102.77	Complete	<div><div></div></div> 100%	8/4/2014 11:13:46 AM	8/4/2014 11:17:03 AM		
System Update Task - 8/4/2014 10:50:53 AM - OMSA	Complete	<div><div></div></div> 100%	8/4/2014 10:51:16 AM	8/4/2014 10:53:45 AM		

Figure 43 Scheduled F/W& Driver inventory Task

11 Difference between managing a server with or without OMSA

The following table provides information about the differences between managing a server with/without OMSA using OpenManage Essentials.

Feature	Server with OMSA	Server without OMSA
Discovery protocol	SNMP / WMI / SSH	WMI / SSH
Overall health	Defined	Unknown
Eventing	Supported	Not supported
Software inventory	Supported	Supported from OpenManage Essentials version 2.0 onwards Need to run the "F/W & Driver inventory task"
System update	Supported	Supported from OpenManage Essentials version 2.0 onwards



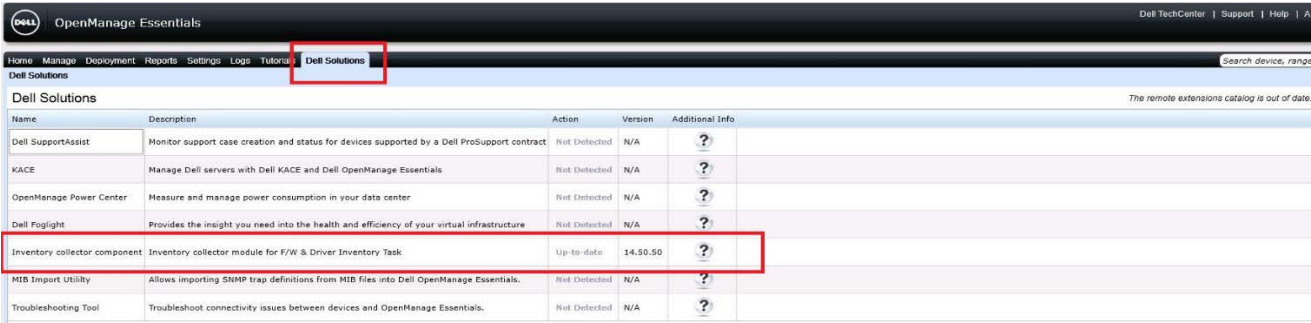
12 Updating the inventory collector component in OpenManage Essentials

OpenManage Essentials integrates the latest version of inventory collector component that is available within the timeline of the OpenManage Essentials release. At times the inventory collector component needs to be updated either to support new devices or to resolve issues. OpenManage Essentials version 2.1 addresses this issue by introducing update capability in the **Dell Solutions** tab.

The **Dell Solutions** tab lists the “Inventory collector component” and indicates whether the current version of the component is of the latest version or not. Similar to any other OpenManage Essentials versions, these components version are checked when you open OpenManage Essentials or the **Dell Solutions** tab.

Note: Functionality of **Dell Solutions** tab dependent on the availability of the OpenManage Essentials catalog from the Dell site. Therefore, you must ensure that you have proper proxy settings/connectivity to the OpenManage Essentials catalog from the Dell site.

If the OpenManage Essentials catalog is not reachable, the following error message is displayed within the top-right of the Dell Solutions tab: “The remove extensions catalog is not accessible.”



Name	Description	Action	Version	Additional Info
Dell SupportAssist	Monitor support case creation and status for devices supported by a Dell ProSupport contract	Not Detected	N/A	?
KACE	Manage Dell servers with Dell KACE and Dell OpenManage Essentials	Not Detected	N/A	?
OpenManage Power Center	Measure and manage power consumption in your data center	Not Detected	N/A	?
Dell Foglight	Provides the insight you need into the health and efficiency of your virtual infrastructure	Not Detected	N/A	?
Inventory collector component	Inventory collector module for F/W & Driver Inventory Task	Up-to-date	14.50.50	?
MIB Import Utility	Allows importing SNMP trap definitions from MIB files into Dell OpenManage Essentials.	Not Detected	N/A	?
Troubleshooting Tool	Troubleshoot connectivity issues between devices and OpenManage Essentials.	Not Detected	N/A	?

Figure 44 Dell Solutions tab showing Inventory Collector Component

When a newer version of the inventory collector component is available, OpenManage Essentials, the Action column displays an **Update** link. When you click the **Update** link, OpenManage Essentials downloads all components of the inventory collector that are available online and replaces the components in the local repository.












 OpenManage Essentials					
Home Manage Deployment Reports Settings Logs Tutorials Dell Solutions					
Dell Solutions					
Dell Solutions					
Name	Description	Action	Version	Additional Info	
Dell SupportAssist	Monitor support case creation and status for devices supported by a Dell ProSupport contract	Not Detected	N/A		
KACE	Manage Dell servers with Dell KACE and Dell OpenManage Essentials	Not Detected	N/A		
OpenManage Power Center	Measure and manage power consumption in your data center	Not Detected	N/A		
Dell Foglight	Provides the insight you need into the health and efficiency of your virtual infrastructure	Not Detected	N/A		
Inventory collector component	Inventory collector module for F/w & driver inventory task	Update	14.50.50 		
MIB Import Utility	Allows importing SNMP trap definitions from MIB files into Dell OpenManage Essentials.	Not Detected	N/A		
Troubleshooting Tool	Troubleshoot connectivity issues between devices and OpenManage Essentials.	Not Detected	N/A		

Figure 45 Update link for inventory collector component

Note: The update inventory collector operation is not reversible. If you want to revert to the version of the inventory collector component that was originally integrated with OpenManage Essentials, you must either repair or reinstall OpenManage Essentials.

Note: Updating the inventory collector component is optional. It is recommended to update the collector component only if you face problems with current version of inventory collector or you want to add new support.

A Additional resources (optional)

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

For more information on Dell OpenManage Essentials:

- Dell OpenManage Essentials Wiki:
<http://en.community.dell.com/techcenter/systems-management/w/wiki/1989.openmanage-essentials.aspx>

