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.
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2013</td>
<td>Initial release</td>
</tr>
<tr>
<td>September 2015</td>
<td>Updates with the OpenManage Essentials version 2.1 release</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Select a catalog source</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Importing the latest Dell FTP catalog</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Software Inventory Information table</td>
<td>12</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Default reboot target server setting</td>
<td>13</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Create (in-band) system update task</td>
<td>14</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Advanced settings preferred update in-band mode</td>
<td>15</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Non-Compliant Systems</td>
<td>16</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Create In-band delivery mode system update task</td>
<td>17</td>
</tr>
<tr>
<td>Figure 9</td>
<td>System Update Task (OMSA) Execution Status</td>
<td>18</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Advanced Settings preferred update mode iDRAC</td>
<td>20</td>
</tr>
<tr>
<td>Figure 11</td>
<td>iDRAC Non-Compliant Report</td>
<td>21</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Create out-of-band system update task</td>
<td>22</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Out-of-band (iDRAC) system update task execution status</td>
<td>23</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Out-of-band (iDRAC) - cancel iDRAC jobs</td>
<td>24</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Creating a Linux user</td>
<td>27</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Editing the sudoers file</td>
<td>28</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Logging in as a sudo user</td>
<td>28</td>
</tr>
<tr>
<td>Figure 18</td>
<td>System update task – Enable Sudo</td>
<td>29</td>
</tr>
<tr>
<td>Figure 19</td>
<td>System update wizard</td>
<td>30</td>
</tr>
<tr>
<td>Figure 20</td>
<td>System update wizard – Non-Compliant Systems</td>
<td>31</td>
</tr>
<tr>
<td>Figure 21</td>
<td>System update wizard – Applicable Packages</td>
<td>31</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Credentials page of the system update wizard</td>
<td>32</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Running a system update task</td>
<td>33</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Running the Import Catalog for System Update task</td>
<td>34</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Remote Task – Firmware &amp; Driver Inventory Task - launch point</td>
<td>35</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Firmware &amp; Driver Inventory Task – Task Name</td>
<td>36</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Firmware &amp; Driver Inventory Task – Filter devices based on the operating system</td>
<td>37</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Firmware &amp; Driver Inventory Task – Select the Operating System</td>
<td>38</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Firmware and Inventory task – Show OMSA based targets</td>
<td>39</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Firmware &amp; Driver Inventory Task – Select Target</td>
<td>41</td>
</tr>
<tr>
<td>Figure 31</td>
<td>Firmware &amp; Driver Inventory task – Select a query</td>
<td>42</td>
</tr>
<tr>
<td>Figure 32</td>
<td>Firmware &amp; Driver Inventory task – Enable All option for OMSA based targets</td>
<td>43</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>33</td>
<td>Firmware &amp; Driver Inventory Task - Set schedule</td>
<td>44</td>
</tr>
<tr>
<td>34</td>
<td>Firmware &amp; Driver Inventory Task - Run now</td>
<td>45</td>
</tr>
<tr>
<td>35</td>
<td>Firmware &amp; Driver Inventory Task - Credentials</td>
<td>46</td>
</tr>
<tr>
<td>36</td>
<td>System Update Portal - Non inventoried Systems</td>
<td>47</td>
</tr>
<tr>
<td>37</td>
<td>System update portal - Select the servers</td>
<td>47</td>
</tr>
<tr>
<td>38</td>
<td>System update portal - Run inventory</td>
<td>48</td>
</tr>
<tr>
<td>39</td>
<td>System update portal - Firmware &amp; Driver inventory wizard</td>
<td>49</td>
</tr>
<tr>
<td>40</td>
<td>System update portal - Non-Complaint Systems tab</td>
<td>50</td>
</tr>
<tr>
<td>41</td>
<td>System update portal - Linux server select packages</td>
<td>51</td>
</tr>
<tr>
<td>42</td>
<td>System update portal - Linux sudo</td>
<td>51</td>
</tr>
<tr>
<td>43</td>
<td>Scheduled F/W&amp; Driver inventory Task</td>
<td>52</td>
</tr>
<tr>
<td>44</td>
<td>Dell Solutions tab showing Inventory Collector Component</td>
<td>54</td>
</tr>
<tr>
<td>45</td>
<td>Update link for inventory collector component</td>
<td>55</td>
</tr>
</tbody>
</table>
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)

![Select a Catalog Source](image)

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](image)
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.
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.
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.

![Advanced Settings](image)

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.
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).

![Advanced Settings](image)

**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.
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.

![Task Execution History](image)

**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.
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.
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).
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.
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**.
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.
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.
<table>
<thead>
<tr>
<th>Direct updates</th>
<th>Staged updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle Controller</td>
<td>BIOS</td>
</tr>
<tr>
<td>iDRAC firmware</td>
<td>NIC firmware</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>RAID firmware</td>
</tr>
<tr>
<td>OS driver pack</td>
<td>Backplane firmware</td>
</tr>
<tr>
<td>Identity module</td>
<td>PSU firmware</td>
</tr>
<tr>
<td></td>
<td>CPLD</td>
</tr>
</tbody>
</table>

**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.
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 (preferred 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 SSH (putty) as a root user.
2. Create a new user and authenticate the user with a password.

![Creating a Linux user](image.png)

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/LinuxPreInstallPackage/omexec <sudo_user_name> ALL=OMEUPDATE, NOPASSWD:OMEUPDATE
   ```
4. Ensure that you are able to log in to the server running Linux through SSH (putty) 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.
Figure 18  System update task – Enable Sudo
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
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**.
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](image)
2. The **Create Firmware & Driver Inventory Task** wizard will open with a default name for the task. If required you can modify the name.

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](image)

**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

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](image)

**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.

<table>
<thead>
<tr>
<th>Future software inventory - selection</th>
<th>Inventory after system update task</th>
<th>Scheduled/user created inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inventory type</td>
<td>Software inventory data updated by</td>
</tr>
<tr>
<td>OMSA based</td>
<td>OMSA – full inventory</td>
<td>OMSA</td>
</tr>
<tr>
<td>F/W and driver inventory task based</td>
<td>OMSA – full inventory + F/W and driver inventory</td>
<td>F/W and driver inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

![Image of Task Target screen]

*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.

![Image of Firmware & Driver Inventory task - Enable All option for OMSA based targets]

**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.

![Figure 33 Firmware & Driver Inventory Task –Set schedule]

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.

**Figure 34** Firmware & Driver Inventory Task – Run now
10. Type the credentials in the highlighted section shown in Figure 13.

![Firmware & Driver Inventory Task - Credentials](image)

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.

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

![Figure 36 System Update Portal – Non inventoried Systems](image)

![Figure 37 System update portal – Select the servers](image)
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**.

![Create a Firmware & Driver Inventory Task](image)

**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.
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.

![System update portal – Non-Complaint Systems tab](image-url)
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.

![System update portal – Linux server select packages](image1)

Figure 41  System update portal – Linux server select packages

![System update portal – Linux sudo](image2)

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:

```
Cmd_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:

```
Cmd_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**.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Status</th>
<th>% Completed</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled F/W &amp; Driver Inventory-10.94.102.77</td>
<td>Complete</td>
<td>100%</td>
<td>8/4/2014 11:13:46 AM</td>
<td>8/4/2014 11:17:03 AM</td>
</tr>
</tbody>
</table>

*Figure 43  Scheduled F/W& Driver inventory Task*
### 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Server with OMSA</th>
<th>Server without OMSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery protocol</td>
<td>SNMP / WMI / SSH</td>
<td>WMI / SSH</td>
</tr>
<tr>
<td>Overall health</td>
<td>Defined</td>
<td>Unknown</td>
</tr>
<tr>
<td>Eventing</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Software inventory</td>
<td>Supported</td>
<td>Supported from OpenManage Essentials version 2.0 onwards Need to run the “F/W &amp; Driver inventory task”</td>
</tr>
<tr>
<td>System update</td>
<td>Supported</td>
<td>Supported from OpenManage Essentials version 2.0 onwards</td>
</tr>
</tbody>
</table>
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.”

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.
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.
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: