

**OpenManage Integration for VMware vCenter
Quick Installation Guide for vSphere Web Client
Version 2.3.1**



Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2015 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

April 2015

Rev. A01

Contents

1 Quick Start Installation.....	4
Installation Introduction.....	4
Prerequisites.....	4
Product Hardware Requirements.....	4
Software Requirements.....	5
Installation and Configuration Overview.....	5
Deploying the OpenManage Integration for VMware vCenter OVF Using the vSphere Web Client.....	6
Registering OpenManage Integration for VMware vCenter and Importing The License File.....	7
Installation Verification.....	9
Upgrading OMI Plugin from 2.x to 2.3.1.....	10
Migration Path to migrate from 2.x to 2.3.1.....	10
How to recover if I have unregistered the older plug-in after the backup.....	11
How to recover if I have unregistered the older plug-in after the backup.....	11
2 Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter.....	12
Configuration Wizard Welcome Page.....	12
vCenter Selection.....	12
Creating A New Connection Profile using the Initial Configuration Wizard.....	13
Scheduling Inventory Jobs [Wizard].....	15
Running A Warranty Retrieval Job [Wizard].....	15
Configuring Events And Alarms [Wizard].....	16
3 Additional Configuration Settings.....	17
Warranty Expiration Notification.....	17
Viewing Warranty Expiration Notification Settings.....	17
Configuring Warranty Expiration Notification.....	17
Firmware Update Repository.....	18
Setting Up the Firmware Update Repository.....	18
OMSA Web Server URL.....	18

Quick Start Installation

Installation Introduction

This guide provides step-by-step instructions for the installation and configuration of OpenManage Integration for VMware vCenter on Dell servers. After the installation is complete, see *OpenManage Integration for VMware vCenter User's Guide* for information about all aspects of administration including: inventory management, monitoring and alerting, firmware updates, and warranty management.

Prerequisites

The following information must be met before you start the product installation

- TCP/IP address information to assign to the OpenManage Integration for VMware vCenter virtual appliance.
- A user name and password for the OpenManage Integration for VMware vCenter to access the vCenter server. This should be an administrator role that has all needed permissions. For additional information on the available OpenManage Integration for VMware vCenter roles within vCenter, see the OpenManage Integration for VMware vCenter Configuration chapter of the *User's Guide*.
- Root password for ESX/ESXi host systems, or the active directory credentials that has administrative rights on the host..
- User name and password associated with iDRAC Express or Enterprise (only for host systems that include an iDRAC).
- Make sure the vCenter server and vSphere Web Client are currently running.
- Know the location of the OpenManage Integration for VMware vCenter OVF file.
- Install the OpenManage Integration for VMware vCenter (virtual appliance) on any ESX/ESXi host managed by a vCenter instance that will be registered with the virtual appliance.
- Your VMware vSphere environment must meet virtual appliance, port access, and listening port requirements. In addition, install Adobe Flash player 11.5 or higher on the client system. For more information on the VMware documentation see, **VMware vCenter 5.5 User's guide and Release Notes**

 **NOTE:** The virtual appliance functions as a regular virtual machine; any interruptions or shut downs impacts overall functionality of the virtual appliance.

 **NOTE:**

The OpenManage Integration for VMware vCenter shows the VMware Tools as 'Running (Out-of-date)' when deployed on ESXi 5.5 and above. You can upgrade the VMware tools after a successful deployment of the appliance or anytime later, if desired

Product Hardware Requirements

The OpenManage Integration for VMware vCenter provides full support for several generation of Dell servers, with full feature support for servers with iDRAC Express or Enterprise available, and limited feature support for older generation

Dell servers. Extensive information on the platform requirements can be found in the OpenManage Integration for VMware vCenter Release Notes. To verify your host servers are eligible, please see these tables in the Release notes:

- Supported server and minimum BIOS
- iDRAC supported versions (both deployment and management)
- OMSA support for older servers and ESX / ESXi version support (both deployment and management)

Software Requirements

The vSphere environment must meet virtual appliance, port access, and listening port requirements.

VMware vSphere has both a desktop client and Web client.

Requirements for Web Client

- Supported for vCenter 5.5 or higher.

 **NOTE:** It is recommended that the OpenManage Integration for VMware vCenter and vCenter server are located on the same network.

For specific software requirements, refer to the *OpenManage Integration for VMware vCenter Release Notes*.

OpenManage Integration for VMware vCenter Port Requirements

- 443 (https) and 80 (http) - For Administration Console
- 4433 (https) - For auto discovery and handshake
- 162 and 11620 - For SNMP trap listener
- 2049, 4001, 4002, 4003, 4004 - For NFS share

Installation and Configuration Overview

The following high-level steps outline the overall installation procedure for the OpenManage Integration for VMware vCenter. These procedures assume that the required hardware is in place and running the required VMware vCenter software. With installations on PowerEdge 12th and higher Generation servers and above, OMSA agent installation is not required. For more information about OMSA, see the *OpenManage Integration for VMware vCenter User's Guide*.

The following information is an outline of the installation process. To begin the actual installation, see the section **Deploy OVF Using Web Client**.

Installation Overview

1. Install the OpenManage Integration for VMware vCenter .
 - a. Be sure systems are connected, vCenter server and vSphere client, and vSphere Web client are started.
 - b. Deploy the Open Virtualization Format (OVF) file that contains the OpenManage Integration for VMware vCenter by using the vSphere client or vSphere Web client.
 - c. Upload the license file.
 - d. Register the OpenManage Integration for VMware vCenter with vCenter server using the Administration Console.

 **NOTE:** Register using FQDN is highly recommended. For both IP / FQDN based registrations, the hostname of the vCenter should be properly resolvable by the DNS server.

2. Type or select information on the Initial Configuration Wizard.

Deploying the OpenManage Integration for VMware vCenter OVF Using the vSphere Web Client

This procedure assumes that you have downloaded and extracted the product zip file (**Dell_OpenManage_Integration_<version number>.<build number>.zip**) from the Dell website.

 **NOTE:** Thick Provision Eager Zeroed is the disk format recommended during this installation.

To deploy the OpenManage Integration for VMware vCenter OVF using the vSphere Web Client:

1. Locate the OpenManage Integration for VMware vCenter virtual disk that you downloaded and extracted and run **Dell_OpenManage_Integration.exe**.
2. Accept the EULA, extract the Quick Installation guide and save the OVF file.
3. Copy or move the OVF file to a location accessible to the VMware vSphere host to which you will upload the appliance.
4. Start the VMware vSphere Web Client.
5. From the VMware vSphere Web Client, select a host and in the main menu click **Actions** → **Deploy OVF Template**. You can also right-click **Host** and select **Deploy OVF Template**.
The **Deploy OVF Template** wizard is displayed.
6. In the **Select Source** window, do the following:
 - a. **URL:** If you want to download the OVF package from internet, select **URL**.
 - b. **Local file:** If you want to select the OVF package from your local system, select the **Local file** and click **Browse**.
 **NOTE:** The installation can take between 10 to 30 minutes, if the OVF package resides on a network share. For a quick installation, it is recommended that you host the OVF on a local drive.
7. Click **Next**. The **Review Details** window is displayed.
8. The following information is displayed in the **Review Details** window:
 - a. **Product:** The OVF template name is displayed.
 - b. **Version:** The version of the OVF template is displayed.
 - c. **Vendor:** The vendor name is displayed.
 - d. **Publisher:** The publisher details are displayed.
 - e. **Download Size:** The actual size of the OVF template in Gigabytes.
 - f. **Size on Disk:** Details of thick and thin provisioned details are displayed.
 - g. **Description:** You can view the comments.
9. Click **Next**. The **Select Name and Folder** window is displayed.
10. In the **Select Name and Folder** window, do the following:
 - a. In the **Name** box, enter the name of the template. This name can contain up to 80 characters.
 - b. In the **Select a folder or datacenter** list, select a location to deploy the template.
11. Click **Next**.
The **Select Storage** window is displayed.
12. In the **Select Storage** window, do the following:
 - a. From the **Select Virtual Disk Format** drop-down list, select either Thick Provision (lazy Zeroed), Thick Provision (Eager zeroed), or Thin Provision to store the virtual disk. It is recommended that you select Thick Provision (lazy Zeroed).
 - b. From the **VM Storage Policy** drop-down list, select one of the policies.
13. Click **Next**. The **Setup Networks** window is displayed.
14. The **Setup Networks** window is displayed which contains details about the source and destination networks. Click **Next**.

15. In the **Ready to Complete** window, review the selected options for the OVF deployment task and click **Finish**.
The deployment job runs and provides a completion status window where you can track job progress.

Registering OpenManage Integration for VMware vCenter and Importing The License File

This procedure assumes that you have received the licenses in the form of an e-mail attachment from **download_software@dell.com**. If you have more than one license, you can add the licenses one after another. The license file is available as an XML format file.

 **NOTE:** If you want to upload a custom certificate for your appliance, you must upload the new certificate prior to vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed in the Web client. To fix this issue, you must unregister and reregister the appliance with the vCenter.

1. From the vSphere Web Client, click **Home** → **Hosts and Clusters**, then in the left panel, locate the OpenManage Integration just deployed, and then click **Power on the virtual machine**. During Deployment, if you select the **Power on after Deployment** check box, the VM will be turned on automatically after deployment.
2. Click the **Console** tab in the main VMware vCenter window to initiate the Administration Console.
3. Allow the OpenManage Integration for VMware vCenter to finish booting up, and then enter the user name for the administrator (the default is Admin), and then set a password.
4. Configure the OpenManage Integration for VMware vCenter network and time zone information.

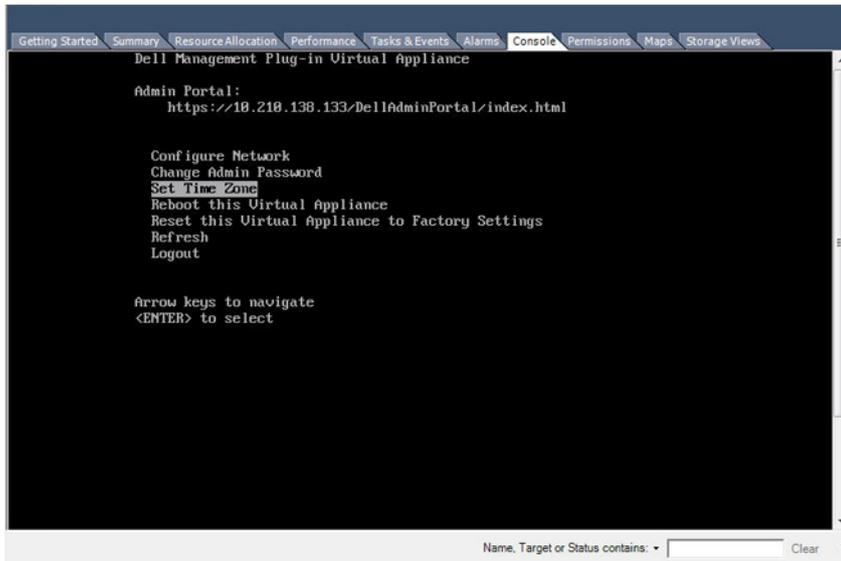


Figure 1. Console tab

5. To open the Administration Console for the product, open a Web browser and type the appliance's IP address or hostname. The IP address is the IP address of the appliance VM and not the ESXi host IP address. The Administration Console can be accessed by using the URL mentioned at the top of the console. For example: <https://10.210.126.120> or <https://myesxihost>

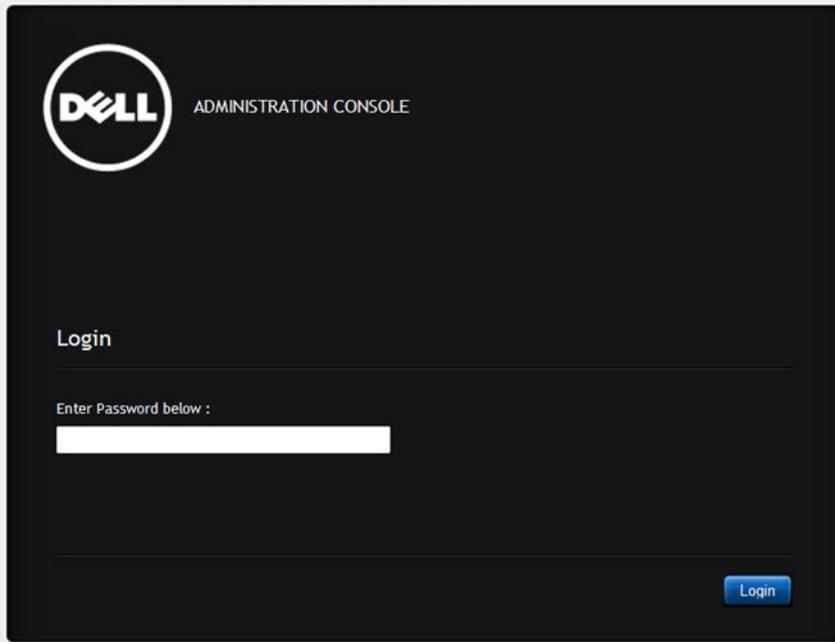


Figure 2. Administration Console

6. In the **Administration Console** login window, enter the password, and then click **Login**.

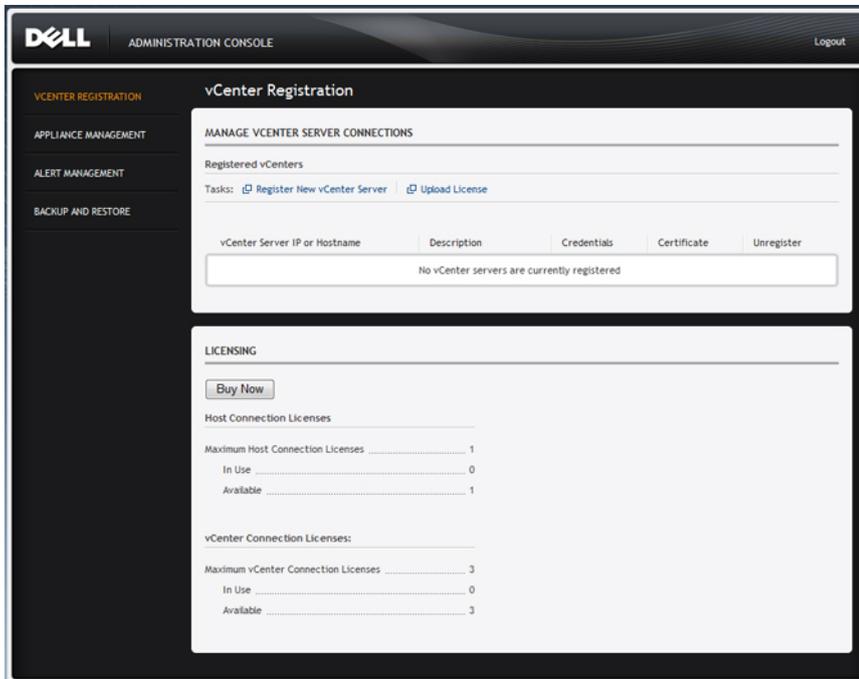


Figure 3. vCenter Registration Window from within the Administration Console

7. In the **vCenter Registration** window, click **Register New vCenter Server**.
8. In the **Register New vCenter Server** window, do the following:

- a. Under **vCenter Name**, in the **vCenter Server IP or Hostname** text box, enter the server IP or hostname and then in the **Description** text box, enter the optional description.
 - b. Under **Admin User Account**, in the **Admin User Name** text box, enter the Admin user name. Enter the username as domain/user or domain\user or user@domain. The Admin user account is used by the OpenManage Integration for vCenter administration.
 - c. In the **Password** text box, enter the password.
 - d. In the **Verify Password** text box, enter the password again.
9. Click **Register**.
 10. Do one of the following:
 - If you are using the OpenManage Integration for VMware vCenter trial version, go to step 12.
 - If you are using the full product version, the license file will be e-mailed to you, and you must import this license to your virtual appliance. To import the license file, click **Upload License**.
 11. In the **Upload License** window, click the **Browse** button to navigate to the license file. Click **Upload** to import the license file.
- NOTE:**
- If the license file is modified or edited in any way, the license file will not work and you must send an e-mail with the original order number to **download_software@dell.com**. For any license file support, e-mail to **download_software@dell.com** with your original order number. The license XML file is used in this procedure and it does not come with a hard coded file name.
 - You cannot use an individual license XML file to upload, instead use the license XML file included in a compressed file.
12. After the OpenManage Integration for VMware vCenter is registered, the OpenManage Integration icon displays under the Administration category of the Web Client home page.

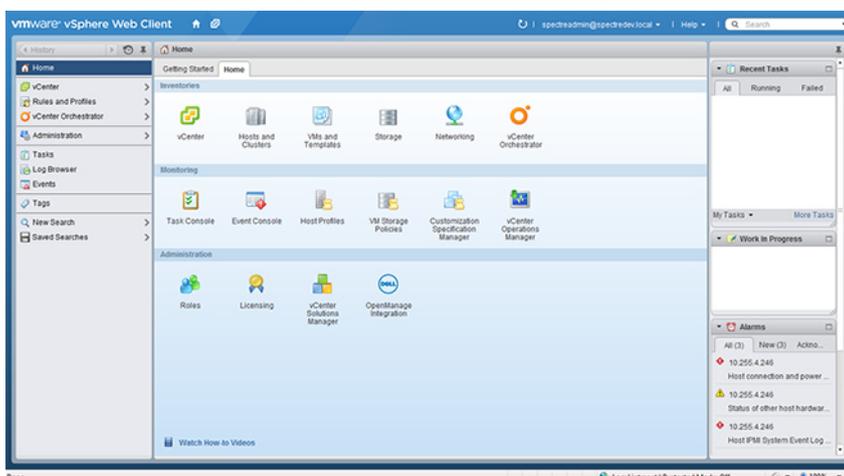


Figure 4. The OpenManage Integration for VMware vCenter Successfully Added to vCenter

Installation Verification

The following steps verify that the OpenManage Integration for VMware vCenter installation was successful:

1. Close any vSphere Client windows and start a new vSphere Web Client.
2. Confirm that the OpenManage Integration icon appears inside vSphere Web Client.

3. Make sure that vCenter can communicate with the OpenManage Integration for VMware vCenter by attempting a PING command from the vCenter server to the virtual appliance IP address or hostname.
4. In **vSphere Web Client**, click **Plug-ins** → **Managed Plug-ins**. In the **Plug-in Manager** window verify the OpenManage Integration for VMware vCenter is installed and enabled.

Upgrading OMI Plugin from 2.x to 2.3.1

There is no RPM update support available from older versions to 2.3.1.

Migration Path to migrate from 2.x to 2.3.1

You can migrate from older version (2.x) to the version 2.3.1 release using the Backup and Restore path. or start with a fresh deployment of the v2.3.1 OVF after uninstalling the old version..

Do the following to migrate from older version to the OpenManage Integration for VMware vCenter 2.3.1 version:

1. Take a Backup of the database for the older (v2.x) release. For more information, See, **OpenManage Integration for VMWare vCenter version 2.3.1 User's Guide**.
2. Power off the older appliance from the vCenter.

NOTE:

Do not unregister the Plug-in from the vCenter. Unregistering the plug-in from the vCenter will remove all the Alarms registered on the vCenter by the plug-in and remove all the customizing performed on the alarms like actions and so on, on the vCenter. For more information, see the section **How to recover if I have unregistered the older plugin after the backup** in this guide if you have already unregistered the Plug-ins after the backup.

3. Deploy the new OpenManage Integration version 2.3.1 OVF. For more information, see the section **Deploying the OpenManage Integration for VMware vCenter OVF Using the vSphere Web Client** in this guide to deploy the OVF.
4. Power on the OpenManage Integration version 2.3.1 appliance.
5. Setup the network, time zone and so on to the appliance. It is mandatory that the new OpenManage Integration version 2.3.1 appliance has the same IP address as the old appliance. To setup the network details, see the section, **Registering OpenManage Integration for VMware vCenter And Importing The License File** in this guide. **Note:** The plug in might not work properly if the IP address for the 2.3.1 appliance is different from the IP address of the older appliance. In such a scenario, you need to un-register and re-register all the vCenter instances.
6. Restore the database to the new appliance. For more information, see the section, **Restoring The Database From A Backup** in the **OpenManage Integration for VMWare vCenter Version 2.3.1 User Guide**.
7. Upload the new license file. For more information, see the section, **Registering OpenManage Integration for VMware vCenter And Importing The License File** in guide.
8. Verify the appliance. For more information, see the section **Installation Verification** in this guide to ensure the database migration is successful.
9. Run the Inventory on all the registered vCenters.

NOTE:

It is recommended that you run the inventory on all the hosts managed by the plug-in again after the upgrade. For more information, see the section **Running Inventory Jobs** for steps to run the inventory on demand.

If the IP address of the new OpenManage Integration version 2.3.1 appliance has changed from that of the old appliance, the trap destination for the SNMP traps must be configured to point to the new appliance. For 12G and 13G servers, this will be fixed by running the Inventory on these hosts. For all 11G or lower generation hosts that were earlier complaint, this IP change will show up as non-complaint and will require configuring OMSA. For more information, see the section, **Running the Fix Non-Compliant VSphere hosts Wizard** to fix the host compliance in the **OpenManage Integration for VMWare vCenter Version 2.3.1 User Guide**.

How to recover if I have unregistered the older plug-in after the backup

If you have unregistered the plug-ins after taking backup of the database of the older version, perform the following steps before proceeding with the migration.

 **NOTE:** Unregistering the plug-in has removed all the customizing that was done on the registered alarms by the plug-in. The following steps will not be able to restore the customizing, however, it will re-register the alarms in the default state.

1. Perform the steps 3-5 in the section **Migration Path to migrate from 2.x to 2.3.1**.
2. Register the plug-in to the same vCenter that you had registered earlier in the older plug-in.
3. Proceed with step 6 through step 9 in the section **Migration Path to migrate from 2.x to 2.3.1** to complete the migration.

How to recover if I have unregistered the older plug-in after the backup

If you have unregistered the plug-ins after taking backup of the database of the older version, perform the following steps before proceeding with the migration.

 **NOTE:** Unregistering the plug-in has removed all the customizing that was done on the registered alarms by the plug-in. The following steps will not be able to restore the customizing. However, it will re-register the alarms in the default state.

1. Perform the steps 3 –5 in the section **Migration Path to migrate from 2.x to 2.3.1**.
2. Register the plug-in to the same vCenter that you had registered earlier in the older plug-in.
3. Go to step 6 through step 9 in the section **Migration Path to migrate from 2.x to 2.3.1** to complete the migration.

Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter

After you complete the basic installation of the OpenManage Integration for VMware vCenter, the Initial Configuration Wizard is displayed when you click on the Dell OpenManage Integration icon. Use the Initial Configuration Wizard to configure the Settings on first launch. For subsequent instances use the **Settings** page. Also, from the Initial Configuration Wizard you can edit the settings of warranty, inventory, events and alarms. Although using the Initial Configuration Wizard is the most common method used, you can also accomplish this task through the appliance's **OpenManage Integration** → **Manage** → **Settings** page in the OpenManage Integration for VMware vCenter. For more information on the Initial Configuration Wizard, see, **OpenManage Integration for VMWare vCenter User Guide**.

Configuration Tasks Using the Configuration Wizard

The Initial Configuration Wizard can be used to configure the following for one vCenter or for all registered vCenters:

1. [vCenter Selection](#)
2. [Creating A New Connection Profile](#)
3. [Scheduling Inventory Jobs](#)
4. [Running A Warranty Retrieval Job](#)
5. [Configuring Events And Alarms](#)

 **NOTE:** You can also launch the Initial Configuration Wizard using the link **Start Initial Configuration Wizard** under **Basic Tasks** in the **Getting Started** page.

Configuration Wizard Welcome Page

After you install the OpenManage Integration for VMware vCenter, it must be configured.

1. In the **vSphere Web Client**, click on **Home**, and then **OpenManage Integration** Icon
2. The first time you click on the **OpenManage Integration** icon, it opens the **Configuration Wizard**. You can also access this wizard on the **OpenManage Integration** → **Getting Started** → **Start Initial Configuration Wizard** page.

vCenter Selection

The vCenter selection page allows you to select a specific vCenter to configure it, or allows you to select all vCenters to configure them.

1. In the **Initial Configuration Wizard**, click on **Next** in the **Welcome** screen.
2. Select one vCenter or all vCenters from the **vCenters** drop-down list. Select an individual vCenter for those not configured yet or if you have added a new vCenter to your environment. The vCenter selection page allows you to select one or more vCenters to configure settings
3. Click **Next** to proceed to the Connection Profile description page.

Creating A New Connection Profile using the Initial Configuration Wizard

A connection profile stores the iDRAC and host credentials that the virtual appliance uses to communicate with Dell servers. Each Dell server must be associated with a connection profile to be managed by the OpenManage Integration for VMware vCenter. You may assign multiple servers to a single connection profile. Creating the Connection Profile is similar between the Configuration Wizard and from the **OpenManage Integration for VMware vCenter** → **Settings** option.

You can log in to iDRAC and Host using Active directory credential. Prior using the Active Directory credentials with a connection profile, the Active Directory user's account must exist in Active Directory and the iDRAC and host must be configured for Active Directory based authentication.

 **NOTE:** The active directory credential can be same for both iDRAC and host or it can be set as separate active directory credential. The user credential must have administrative privilege.

 **NOTE:** You are not allowed to create a connection profile if the number of hosts added exceeds the license limit for creating a Connection Profile

To create a new connection profile using the wizard:

1. From the **Connection Profile Description** page, click **Next** to proceed.
2. In the **Name and Credentials** page, enter the **Connection Profile Name** and an optional **Connection Profile Description**.
3. In the **Name and Credentials** page, under **iDRAC Credentials**, do one of the following:

-  **NOTE:** The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.
- For iDRACs already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure the iDRAC credentials.
 - In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain/username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
 - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
 - In the **Verify Password** text box, type the password again.
 - Perform one of the following actions:
 - * To download and store the iDRAC certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
 - * To not store and perform the iDRAC certificate check during all future connections, clear the **Enable Certificate Check**.
- To configure iDRAC credentials without Active Directory, do the following:
 - In the **User Name** text box, type the user name. The user name is limited to 16 characters. Refer to the iDRAC documentation for information about user name restrictions for your version of iDRAC.
 - In the **Password** text box type the password. The password is limited to 20 characters.
 - In the **Verify Password** text box, type the password again.

- Perform one of the following actions:
 - * To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check** check box.
 - * To not store and perform the iDRAC certificate check during all future connections, clear **Enable Certificate Check** check box.
4. In the Host Root area, do one of the following:
- For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure your Host Credentials.
 - In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain/username or username@domain. The user name is limited to 256 characters.
For host user name and domain restrictions, refer the following:
Host Username Requirements:
 - a. Between 1 and 64 characters long
 - b. No non-printable characters
 - c. Invalid characters: "/\ [] ; | = , + * ? < > @
 Host Domain Requirements:
 - a. Between 1 and 64 characters long
 - b. First character must be alphabetical
 - c. Cannot contain a space
 - d. Invalid characters: "/\ : | , * ? < > ~ ! @ # \$ % ^ & ' () { } _
 - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
 - In the **Verify Password** text box, type the password again.
 - Perform one of the following actions:
 - * To download and store the Host certificate and validate it during all future connections, select the **Enable Certificate Check** check box .
 - * To not store and perform the Host certificate check during all future connections, clear the **Enable Certificate Check** check box.
 - To configure Host Credentials without Active Directory, do the following:
 - In the **User Name** text box, the user name is root. This is the default username and you cannot change the username. However, if the Active directory is set, you can choose any Active directory user not just root.
 - In the **Password** text box type the password. The password is limited to 127 characters.
 **NOTE:** The OMSA credentials are the same credentials used for ESX and ESXi hosts.
 - In the **Verify Password** text box, type the password again.
 - Perform one of the following actions:
 - * To download and store the Host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
 - * To not store and perform the Host certificate check during all future connections, clear the **Enable Certificate Check** check box

5. Click **Next**.
6. In the **Associated Hosts** page, select the hosts for the connection profile and click **OK**.
7. To test the connection profile, select one or more hosts and select the **Test Connection** button. This step is optional. This is used to check whether the Host and iDRAC credentials are correct or not.
8. To complete the profile, click **Next**. For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states Not Applicable for this system.

Scheduling Inventory Jobs [Wizard]

The inventory schedule configuration is similar between the Configuration Wizard and from the OpenManage Integration under Manage section, Settings option.

-  **NOTE:** To make sure that the OpenManage Integration for VMware vCenter continues to display updated information, it is recommended that you schedule a periodic inventory job. The inventory job consumes minimal resources and will not degrade host performance.
-  **NOTE:** Chassis gets discovered automatically once the inventory for all hosts is run. If the chassis is added to a chassis profile, then the chassis inventory automatically runs. In a SSO environment having multiple vCenters, the chassis inventory runs automatically with every vCenter when the inventory for any vCenter is run at a scheduled time.

To schedule an inventory job:

1. In the **Configuration Wizard**, in the **Inventory Schedule** window, do one of the following:
 - The **Enable Inventory Data Retrieval** check box is selected by default to enable you to schedule the inventory.
2. Under **Inventory Data Retrieval Schedule**, do the following:
 - a. Select the check box next to each day of the week that you want to run the inventory. By default, **all the days** are selected.
 - b. In the text box, enter the time in HH:MM format.
The time you enter is your local time. Therefore, if you want to run the inventory at the virtual appliance time zone, calculate the time difference between your local and virtual appliance time zone, and then enter the time appropriately.
3. To apply the changes and continue, click **Next** to proceed with the warranty schedule settings.

Running A Warranty Retrieval Job [Wizard]

The warranty retrieval job configuration is similar between the wizard and from the OpenManage Integration for VMware vCenter, Settings option. In addition, you can run the Warranty Retrieval Job now, from Job Queue. Scheduled jobs are listed in the Job queue. In a SSO environment having multiple vCenters, the chassis warranty runs automatically with every vCenter when the warranty for any vCenter is run. Warranty is not automatically run if it added to chassis profile.

To run a warranty retrieval job:

1. In the **Configuration Wizard**, in the **Warranty Schedule** window, do one of the following:
 - Select the **Enable Warranty Data Retrieval** check box to enable you to schedule the warranty.
2. Under **Warranty Data Retrieval Schedule**, do the following:
 - a. Select the check box next to each day of the week that you want to run the warranty.
 - b. In the text box, enter the time in HH:MM format.
The time you enter is your local time. Therefore, if you want to run the inventory at the virtual appliance time zone, calculate the time difference between your local and virtual appliance time zone, and then enter the time appropriately.

3. To apply the changes and continue, click **Next** to proceed with the warranty schedule settings.

Configuring Events And Alarms [Wizard]

Configure events and alarms using the Configuration Wizard or from the OpenManage Integration for VMware vCenter, Settings option for Events and Alarms.

 **NOTE:** On hosts prior to Dell PowerEdge 12th generation servers, use Host Compliance Fix Option to configure trap destination list in OMSA to display host events in vCenter.

To configure events and alarms:

1. In the **Initial Configuration Wizard**, under **Event Posting Levels**, select one of the following:
 - Do not post any events - Block hardware events.
 - Post All Events - Post all hardware events.
 - Post only Critical and Warning Events - Post only critical or warning level hardware events.
 - Post only Virtualization-Related Critical and Warning Events - Post only virtualization-related critical and warning events; this is the default event posting level.
2. To enable all hardware alarms and events, select the **Enable Alarms for Dell Hosts** check box.

 **NOTE:** Dell hosts that have alarms enabled respond to some specific critical events by entering maintenance mode.
3. A dialog box **Enabling Dell Alarm Warning** is displayed, click **Continue** to accept the change, or click **Cancel**.

 **NOTE:** This step is only seen if **Enable Alarms For Dell Hosts** is selected.
4. To continue the wizard, click **Apply**.

Additional Configuration Settings

The following configuration settings are optional. However, it can be used for monitoring the hosts in your VMware vCenter using the plug-in.

- [Warranty Expiration Notification](#)
- [Firmware Update Repository](#)
- [OMSA Web Server URL](#)

Warranty Expiration Notification

Viewing Warranty Expiration Notification Settings

1. In the OpenManage Integration for VMware vCenter, click **Manage** → **Settings** tab.
2. Under **Appliance Settings**, click **Warranty Expiration Notification**.
The **Warranty Expiration Notification** page displays the following:
 - Indicates whether the setting is enabled or disabled
 - The number of days set for the first warning setting.
 - The number of days set for the critical warning setting
3. To configure the Warranty Expiration Notification, see [Configuring Warranty Expiration Notifications](#).

Configuring Warranty Expiration Notification

You can configure warranty expiration thresholds to alert about warranty expiration.

1. In the OpenManage Integration for VMware vCenter, click **Manage** → **Settings** tab.
2. Under **Appliance Settings**, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.
3. In the **Warranty Expiration Notification** dialog box, perform the following:
 - a. If you want to enable this setting, select the **Enable warranty expiration notification for hosts** check box. Selecting the check box enables warranty expiration notification.
 - b. Under **Minimum Days Threshold Alert**, perform the following:
 1. In the **Warning** drop-down list, select the number of days before you want receive the alert for the warranty expiration.
 2. In the **Critical** drop-down list, select the number of days before you want to receive the alert for the warranty expiration.
4. Click **Apply**.

Firmware Update Repository

In the OpenManage Integration for VMware vCenter, in the **Settings** tab, you can set the location from which the servers can receive firmware updates. It is a global setting.

Firmware repository settings contain the firmware catalog location used to update deployed servers. Following are the location types:

- **Dell (ftp.dell.com)** — Uses the firmware update repository of Dell (ftp.dell.com). The OpenManage Integration for VMware vCenter downloads selected firmware updates from Dell repository.
- **Shared Network Folder** — Created with Dell Repository Manager™. These local repositories are located on CIFS or NFS file share.

Setting Up the Firmware Update Repository

You can configure the firmware update repository on the OpenManage Integration for VMware vCenter in the **Settings** tab.

1. In OpenManage Integration for VMware vCenter, click **Manage** → **Settings**.
2. Under **Appliance Settings**, to the right side of **Firmware Update Repository**, click the Edit icon.
3. In the **Firmware Update Repository** dialog box, select one of the following:
 - **Dell Online** — Default firmware repository (ftp.dell.com) with a staging folder. The OpenManage Integration for VMware vCenter downloads selected firmware updates and stores them in the staging folder, and then you need to run the firmware wizard to update the firmware
 - **Shared Network Folder** — These are created with the Dell Repository Manager application. Locate these local repositories on Windows-based file shares. Use the live link to go to Dell Repository Manager.
4. If you selected the **Shared Network Folder** option, perform the following
 - a. Enter the catalog file location using the following format
 - NFS share for **xml file**: **host/share/filename.xml**
 - NFS share for **gz file**: **host/share/filename.gz**
 - CIFS share for **xml file**: **\\host\share\filename.xml**
 - CIFS share for **gz file**: **\\host\share\filename.gz**
 - b. In the Select Update Source page, if the downloading of the files that is displayed selected repository path is in progress, a message is displayed to notify that the download is in progress
5. When the file download is complete, click **Apply**.

OMSA Web Server URL

OMSA Link is the URL to launch the OMSA GUI for hosts that have OMSA installed.

 **NOTE:** OMSA is only required on Dell PowerEdge 11th generation servers or earlier.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** → **Settings**.
2. Under **vCenter Settings**, to the right side of the OMSA Web Server URL, click **Edit**.
3. In the **OMSA Web Server URL** dialog box, type the URL.
You must include the full URL including the HTTPS.

4. Select the **Apply these settings to all vCenters** check box to apply the OMSA URL to all vCenters.
If you do not select this check box, the OMSA URL is applied only to one vCenter.
5. From the corresponding host **Summary** tab, verify whether the link works or not.
6. Verify whether or not the OMSA Console link is functional within the Dell Host Information.