

# OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2



# Notes, cautions, and warnings

-  **NOTE:** A NOTE indicates important information that helps you make better use of your product.
-  **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.

# Contents

<b>1 Quick Start Installation.....</b>	<b>5</b>
Installation Introduction.....	5
Prerequisites.....	5
Hardware Requirements.....	5
Software Requirements.....	6
Installation and Configuration Overview.....	6
Deploying the OMIVV OVF Using the vSphere Web Client.....	6
Registering a vCenter server by using a user with necessary privileges.....	7
Registering OpenManage Integration for VMware vCenter and importing license file.....	9
Installation Verification.....	13
Upgrading OMIVV from existing version to current version.....	13
Migrating from 2.x to 3.2.....	14
Recovering OMIVV after unregistering earlier version of OMIVV.....	15
<b>2 Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter.....</b>	<b>16</b>
Configuration Wizard Welcome Page.....	16
vCenter Selection.....	16
Creating A New Connection Profile using the Initial Configuration Wizard.....	17
Scheduling Inventory Jobs [Wizard].....	19
Running A Warranty Retrieval Job [Wizard].....	19
Configuring Events And Alarms [Wizard].....	19
Creating A Chassis Profile.....	20
<b>3 Additional Configuration Settings.....</b>	<b>22</b>
Warranty Expiration Notification.....	22
Viewing Warranty Expiration Notification Settings.....	22
Configuring Warranty Expiration Notification.....	22
Firmware Update Repository.....	22
Setting Up the Firmware Update Repository.....	23
OMSA Web Server URL.....	23
<b>4 OpenManage Integration for VMware vCenter licensing.....</b>	<b>24</b>
Buying and uploading software license.....	24
Options after uploading Licenses.....	25
License file for new purchases.....	25
Stacking licenses.....	25
Expired licenses.....	25
Replacement of licenses .....	25
Enforcement.....	25
Appliance updates.....	25
Evaluation License.....	25



Adding hosts to connection profiles.....	25
<b>5 For More Configuration Information.....</b>	<b>26</b>
<b>6 Related documentation and resources.....</b>	<b>27</b>
Accessing documents from Dell support site.....	27



# Quick Start Installation

## Installation Introduction


This guide provides step-by-step instructions for the installation and configuration of OpenManage Integration for VMware vCenter (OMIVV) on Dell servers. After the installation is complete, for information about all aspects of administration including: inventory management, monitoring and alerting, firmware updates, and warranty management, see the *OpenManage Integration for VMware vCenter User's Guide* available at [dell.com/support/manuals](http://dell.com/support/manuals).

## Prerequisites

The following prerequisites must be fulfilled before you start the product installation:

- TCP/IP address information to be assigned to the OMIVV virtual appliance.
- A user name and password for OMIVV to access the vCenter server. This should be an administrator role that has all necessary permissions. For more information about the available OMIVV roles within vCenter, see *OpenManage Integration for VMware vCenter User's Guide* available at [dell.com/support/manuals](http://dell.com/support/manuals).
- Root password for 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.
- Make sure the vCenter server is currently running.
- Know the location of the OMIVV OVF file.
- Install the OMIVV (virtual appliance) on any ESXi host.
- Your VMware vSphere environment must meet virtual appliance, port access, and listening port requirements. In addition, install Adobe Flash Player on the client system. For more information on the supported Flash Player version, see the *OpenManage Integration for VMware vCenter Compatibility Matrix*.

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

 **NOTE: The OMIVV shows the VMware Tools as Running (Out-of-date) when deployed on ESXi 5.5 and later. You can upgrade the VMware tools after a successful deployment of the appliance or anytime later, if necessary.**

 **NOTE: It is recommended that the OMIVV and vCenter server are located on the same network.**

## Hardware Requirements

OMIVV provides full support for several generation of Dell servers, with full feature support for servers with iDRAC Express or Enterprise. Extensive information on the platform requirements can be found in the *OpenManage Integration for VMware vCenter Release Notes* available at [Dell.com/support/manuals](http://Dell.com/support/manuals). To verify that your host servers are eligible, refer to the tables in the *OpenManage Integration for VMware vCenter Compatibility Matrix* available at [Dell.com/support/manuals](http://Dell.com/support/manuals).

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



## Software Requirements

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

 **NOTE: VMware vSphere has both a desktop client and Web client.**

### Requirements for Web Client

Supported for vCenter version 5.5 upto vCenter version 6.0 U3.

 **NOTE: You will be able to register vCenters under one Platform Services Controller to a single OMIVV appliance only.**

For specific software requirements, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at [dell.com/support/manuals](http://dell.com/support/manuals).

### OpenManage Integration for VMware vCenter Port Requirements

Port number	Description
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 OMIVV. These procedures assume that the required hardware is in place and running the required VMware vCenter software.

The following information is an outline of the installation process. To begin the actual installation, see the [Deploy OVF Using Web Client](#) section.

### Installation Overview

1. Install OMIVV.
  - a. Be sure that systems are connected and the vCenter server is up and running.
  - b. Deploy the Open Virtualization Format (OVF) file that contains the OMIVV appliance using the vSphere client or vSphere Web client.
  - c. Upload the license file.
  - d. Register the OMIVV with vCenter server using the **Administration Console**.
2. Complete the **Initial Configuration Wizard**.

## Deploying the OMIVV 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.

To deploy the OMIVV OVF using the vSphere Web Client:

1. Locate the OMIVV virtual disk that you downloaded and extracted and run **Dell\_OpenManage\_Integration.exe**.
2. Accept the **EULA** 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 **Name**, 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 (Eager 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**.

 **NOTE: It is recommended that the OMIVV and the vCenter server are located in the same network.**

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 a vCenter server by using a user with necessary privileges

You can register vCenter servers for the OMIVV appliance with vCenter administrator credentials of the vCenter server or a user with necessary privileges.

Perform the following steps to enable a user with the required privileges to register a vCenter server:

1. Add a role and select relevant privileges for the role, or modify an existing role to change the privileges selected for that role. See VMware vSphere documentation for the steps required to create or modify a role and select privileges in vSphere Web client. See [Defining privileges](#) to select all the relevant privileges for the role.

 **NOTE: The vCenter administrator should add or modify a role.**

2. After you define a role and select privileges for the role, assign a user and their role to the relevant inventory object. See VMware vSphere documentation for more information on assigning permissions in the vSphere Web client. A vCenter server user with the required privileges can now register and/or unregister vCenter.



 **NOTE: The vCenter administrator should assign permissions in the vSphere Web client.**

3. Register a vCenter server in the administration console by using a user with necessary privileges. See [Registering vCenter server by non-administrator user with required privileges](#).
4. Associate the Dell privileges to the role created or modified in step 1 for performing the OMIVV operations. See [Assigning Dell privileges to the role in vSphere Web client](#).

Now, a user with the required privileges can experience the OMIVV features with Dell hosts.

## Defining privileges

To enable a user with the required privileges to register a vCenter server, select the following privileges:

- Alarms
  - Create alarm
  - Modify alarm
  - Remove alarm
- Extension
  - Register extension
  - Unregister extension
  - Update extension
- Global
  - Cancel task
  - Log event
  - Settings
- Host
  - CIM
    - \* CIM Interaction
  - Configuration
    - \* Advanced settings
    - \* Connection
    - \* Maintenance
    - \* Query patch
    - \* Security profile and firewall
  - Inventory
    - \* Add host to cluster
    - \* Add standalone host
- Host profile
  - Edit
  - View
- Permissions
  - Modify permission
  - Modify role
- Sessions
  - Validate session
- Task

- Create task
- Update task

 **NOTE: If the mentioned privileges are not assigned, an error message is displayed while registering a vCenter server by using a user with the available privileges.**

### Registering vCenter server by non-administrator user with required privileges

You can register a vCenter server for the OMIVV appliance by using a non-administrator user with the required privileges. See step 5 to step 9 of [Registering OpenManage Integration for VMware vCenter and importing license file](#) for information on registering a vCenter server through a non-administrator user or as an administrator.

### Assigning Dell privileges to the role in vSphere Web client

You can edit an existing role to assign Dell privileges. When completed, these privileges are applied to the user or group that is assigned the edited role.

 **NOTE: Ensure that you are logged in as a user with Administrator privileges.**

To assign the Dell privileges to an existing role, perform the following:

1. Log in to the vSphere Web client with administrative rights.
2. Browse to **Administration → Role Manager** in vSphere Web client.
3. Select a vCenter server system from the drop-down menu.
4. Select a role and click **Edit role action**.
5. Select the following privileges for Dell Infrastructure Deployment Role, Dell Operational Role, and click **OK**.
  - Dell
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting


See *OpenManage Integration for VMware vCenter User's Guide* for more information on the available OMIVV roles within vCenter.

The changes to permissions and roles take effect immediately. The user with necessary privileges can now perform the OpenManage Integration for VMware vCenter operations.

 **NOTE: For all vCenter operations, OMIVV uses the privileges of the registered user and not the privileges of the logged-in user.**

### Registering OpenManage Integration for VMware vCenter and importing license file

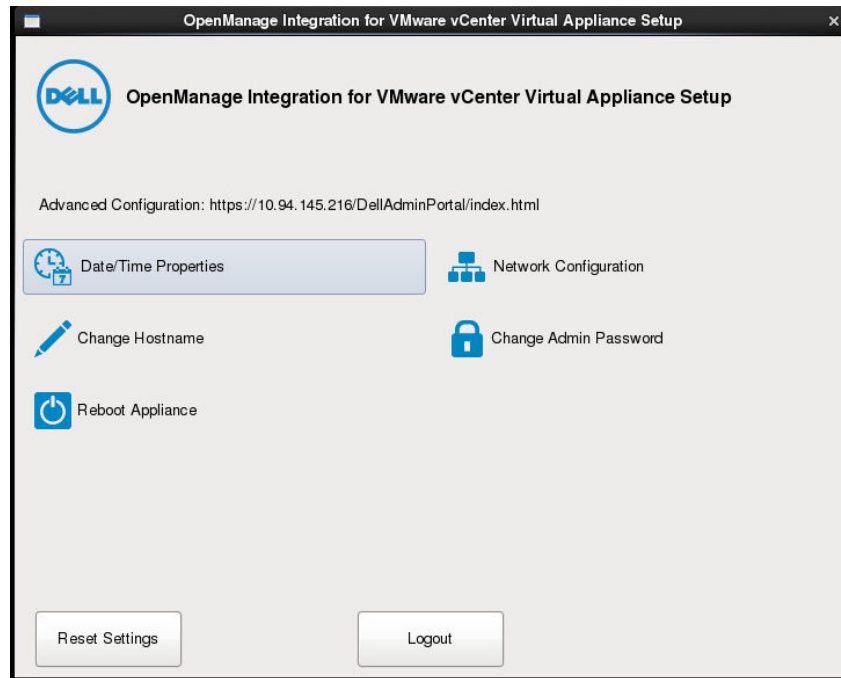
When you purchase a license, the .XML file (license key) is available for download through the Dell Digital store that is available at <http://www.dell.com/support/licensing>. If you are unable to download your license key(s), contact Dell Support by going to [www.dell.com/support/softwarecontacts](http://www.dell.com/support/softwarecontacts) to locate the regional Dell Support phone number for your product.

 **NOTE: If you want to upload a custom certificate for your appliance, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed in the web client. To fix this issue, unregister, and re-register the appliance with vCenter.**

1. From the vSphere web client, click **Home → Hosts and Clusters**, then in the left panel, locate OMIVV that you had deployed, and click **Power on the virtual machine**.  
During deployment, if you select **Power on after Deployment**, the VM is powered on automatically after deployment is complete.
2. To run the **Administration Console**, click the **Console** tab in the main **VMware vCenter** window.
3. Allow OMIVV to complete booting up, and then enter the user name as, **Admin** (the default is Admin), and press **Enter**.



4. Enter a new admin password, and set the password as per the password complexity rules displayed in the interface. Press **Enter**.
5. Reenter the password that was provided earlier and press **Enter**.  
To configure the network and time zone information in the OMIVV appliance, press **Enter**.
6. To configure the OMIVV time zone information, click **Date/Time Properties**.



**Figure 1. Console tab**

7. In the **Date and Time** tab, select the **Synchronize date and time over the network**.  
The **NTP Servers** box is displayed.
8. Add valid NTP server details to which your vCenter is synchronized with.
9. Click **Time Zone** and select the applicable time zone, and click **OK**.
10. To configure static IP to the OMIVV appliance, click **Network Configuration**, or skip to step 17.
11. Select **Auto eth0**, and then click **Edit**.
12. Select the **IPv4 Settings** tab, and select **Manual** in the **Method** drop-down.
13. Click **Add**, and add a valid IP Address Netmask and gateway information.
14. In the **DNS Servers** field, provide the DNS server detail.
15. Click **Apply**.
16. To change the host name of the OMIVV appliance, click **Change Hostname**.
17. Enter a valid host name, and click the **Update hostname**.

 **NOTE: After host name and NTP are changed, ensure that the system is rebooted.**

 **NOTE: If any vCenter servers are registered with the OMIVV appliance, unregister and re-register all the vCenter instances.**

Before opening the administration console, ensure that you manually update all references to the appliance such as, provisioning server in iDRAC, DRM.

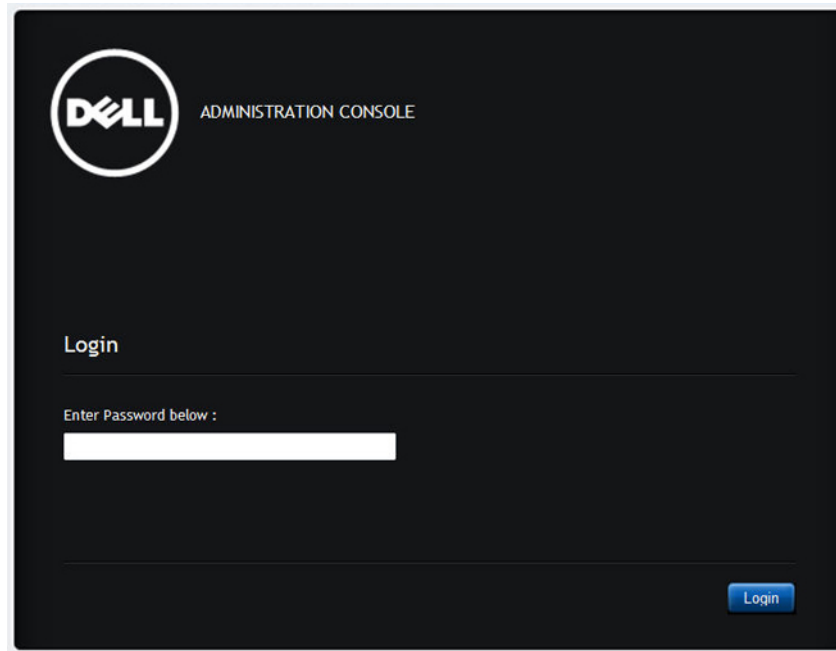
18. Open **Administration Console** from a supported browser.

To open **Administration Console**, in the **Help and Support** tab of OpenManage Integration for VMware vCenter, click the link under **Administration Console** or start a web browser and provide the `https://<ApplianceIP/hostname>\DellAdminPortal` url.

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](https://10.210.126.120) or [Https://myesxihost](https://myesxihost)

The URL is not case-sensitive.



**Figure 2. Administration Console**

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

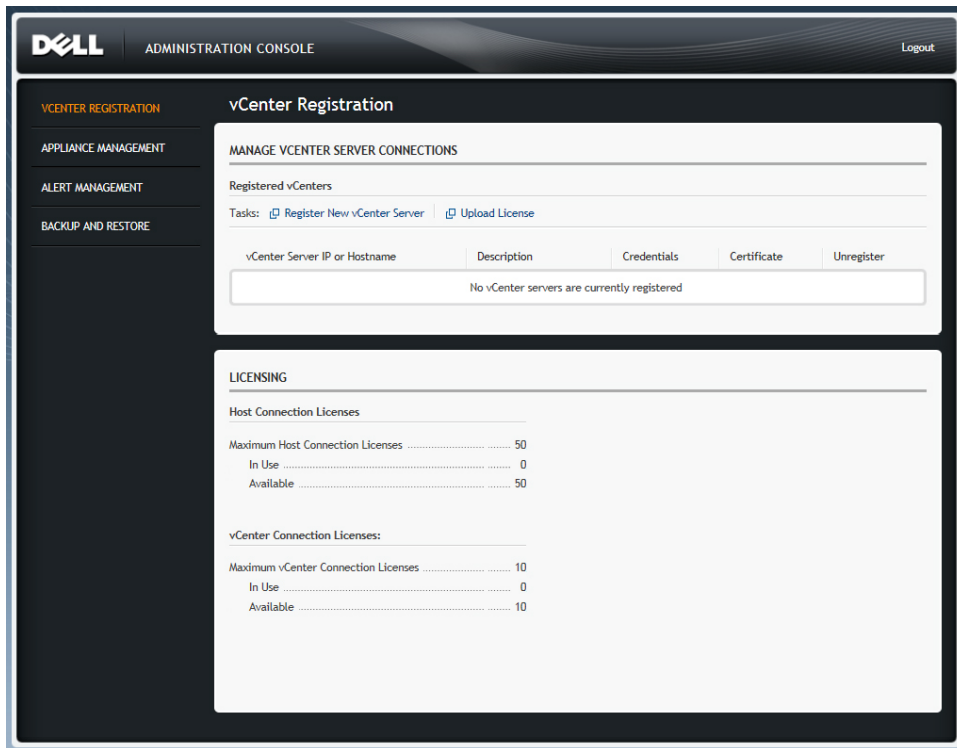


Figure 3. vCenter registration window from Administration Console

20. In the **vCenter Registration** window, click **Register a New vCenter Server**.
21. In the **Register a New vCenter Server** window, perform the following substeps:
  - a. Under **vCenter Name**, in the **vCenter Server IP or Hostname** text box, enter the server IP or host name, and then in the **Description** text box, enter a description.  
The description is optional.
 

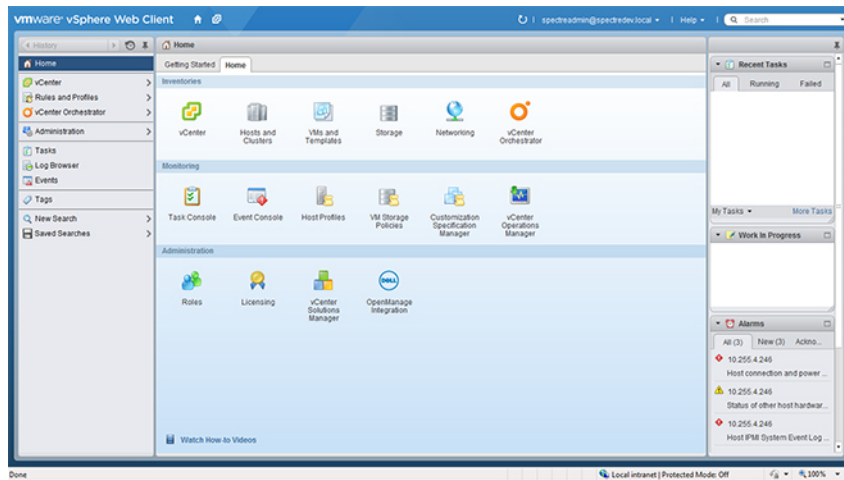
**NOTE:** Dell recommends registering OpenManage Integration for VMware vCenter with the VMware vCenter by using Fully Qualified Domain Name (FQDN). Ensure that the host name of the vCenter is properly resolvable by the DNS server for FQDN-based registrations.
  - b. Under **vCenter User Account**, in **vCenter User Name**, enter the Admin user name or the user name with necessary privileges.  
Enter the **username** as **domain\user** or **domain/user** or **user@domain**. OMIVV uses the Admin user account or the user with necessary privileges for vCenter administration.
  - c. In **Password**, enter the password.
  - d. In **Verify Password**, enter the password again.
22. Click **Register**.
 

**NOTE:** OpenManage Integration for VMware vCenter currently supports up to 1000 hosts for large deployment mode with a single vCenter instance or multiple vCenter servers by using the linked mode.
23. Perform one of the following actions:
  - If you are using the OMIVV trial version, you can view the OMIVV icon.
  - If you are using the full product version, the license file is emailed to you, and you can import this license to your virtual appliance. To import the license file, click **Upload License**.
24. In the **Upload License** window, click **Browse** to navigate to the license file, and then click **Upload** to import the license file.
 

**NOTE:** If you modify or edit the license file, the license file does not work and you can contact Dell Support by going to [www.dell.com/support/softwarecontacts](http://www.dell.com/support/softwarecontacts) to locate the regional Dell Support phone number for your product. The license file used in this procedure does not come with a hard-coded file name.

Once OMIVV is registered, the OMIVV icon is displayed under the **Administration** category of the web client home page.





**Figure 4. OpenManage Integration for VMware vCenter successfully added to vCenter**

For all vCenter operations, OMIVV uses the privileges of a registered user and not the privileges of a logged-in user.

For example: User X with the necessary privileges registers OMIVV with vCenter, and user Y has only Dell privileges. User Y can now log in to the vCenter and can trigger a firmware update task from OMIVV. While performing the firmware update task, OMIVV uses the privileges of user X to put the machine into maintenance mode or reboot the host.

## Installation Verification

The following steps verify that the OMIVV installation was successful:

1. Close any vSphere Client windows and start a new vSphere Web Client.
2. Confirm that the OMIVV icon appears inside vSphere Web Client.
3. Make sure that vCenter can communicate with the OMIVV 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**.
5. In the **Plug-in Manager** window verify the OMIVV is installed and enabled.


## Upgrading OMIVV from existing version to current version

1. To open Administration Console, in the **Help and Support** tab of OpenManage Integration for VMware vCenter, click the link under **Administration Console** or start a web browser and provide the `https://<ApplianceIP>hostname>` url.
2. In the **Login** dialog box, type the password.
3. In Administration Console, in the left pane, click **APPLIANCE MANAGEMENT**.
4. In the **APPLIANCE MANAGEMENT** page, depending on your network settings, enable proxy and provide proxy settings if your network needs proxy.
5. To upgrade the OpenManage Integration plug in from an existing version to the current version, perform one of the following steps:
  - To upgrade using RPM that is available in **Update Repository Path**, ensure that **Update Repository Path** is set to the path: <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>. If the path is different, in the **Appliance Management** window, in the **APPLIANCE UPDATE** area, click **Edit** to update the path to `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest` in the **Update Repository Path** text box. To save, click **Apply**.
  - To upgrade using the latest downloaded RPM folders or files if there is no internet connectivity, download all the files and folders from the `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/` path and copy them to an HTTP share. In the **Appliance Management** window, in the **APPLIANCE UPDATE** section, click **Edit**, and then in the **Update Repository Path** text box, include the path to the offline HTTP share, and click **Apply**.
6. Compare the available virtual appliance version and current virtual appliance version and ensure that the available virtual appliance version is greater than the current virtual appliance version.
7. To apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
8. In the **UPDATE APPLIANCE** dialog box, click **Update**.



After you click **Update**, you are logged off from the **ADMINISTRATION CONSOLE** window.

9. Close the web browser.

 **NOTE:** While upgrading OMIVV from 3.1 to the current version, the custom certificate is not migrated. Therefore, ensure that you reapply the settings that you had applied for the certificate. If you have enabled Proactive HA on clusters, OMIVV unregisters the Dell Inc provider for those clusters and re-registers the Dell Inc provider after upgrade. Hence, health updates for the Dell hosts are not available until upgrade is complete.


 **NOTE:** The future available release information will be displayed in the Administration Console. See the *OpenManage Integration Version 3.2 for VMware vCenter User's Guide* available at [Dell.com/support/manuals](http://Dell.com/support/manuals) for RPM and OVF information.

## Migrating from 2.x to 3.2


You can start with a fresh deployment of the v3.2 OVF after uninstalling the old version and then migrate the data from older version (2.x) to 3.2 version by using backup and restore path.

To migrate from an older version to the OMIVV 3.2 version, perform the following steps:


1. Take a backup of the database for the older (v2.x) release.  
For more information, see *OpenManage Integration for VMware vCenter User's Guide* available at [Dell.com/support/manuals](http://Dell.com/support/manuals).
2. Power off the older appliance from vCenter.

 **NOTE:** Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes all the alarms registered on vCenter by the OMIVV plug-in and all the customization that is performed on the alarms such as, actions and so on. For more information, see [Recovering OMIVV after unregistering the earlier plug-in version if you have unregistered the plug-in after the backup.](#)

3. Deploy the new OpenManage Integration version 3.2 OVF.  
For more information on deploying the OVF, see [Deploying the OMIVV OVF by using the vSphere web client.](#)
4. Power on the OpenManage Integration version 3.2 appliance.
5. Set up the network and time zone on the appliance.  
Ensure that the new OpenManage Integration version 3.2 appliance has the same IP address as the old appliance. To set up the network details, see [Registering OMIVV and importing the license file.](#)

 **NOTE:** The OMIVV plug-in might not work properly if the IP address for the OMIVV 3.2 appliance is different from the IP address of the older appliance. In such a scenario, unregister and re-register all the vCenter instances.

6. Restore the database to the new OMIVV appliance.

 **NOTE:** If you have enabled Proactive HA on clusters, OMIVV unregisters the Dell Inc provider for those clusters and re-registers the Dell Inc provider after restore. Hence, health updates for the Dell hosts are not available until restore is complete.

For more information, see **Restoring the OMIVV database from a backup** in the *OpenManage Integration for VMware vCenter User's Guide* available at [Dell.com/support/manuals](http://Dell.com/support/manuals).

7. Upload the new license file.  
For more information, see [Registering OMIVV and importing the license file.](#)
8. Verify the appliance.  
For more information, see the [Verifying installation](#) to ensure that the database migration is successful.
9. Run the **Inventory** on all the hosts.

 **NOTE:**

It is recommended that after the upgrade, you run the inventory again on all the hosts that the OMIVV manages. For more information, see the **Running inventory jobs** in *OpenManage Integration for VMware vCenter User's Guide*.

If the IP address of the new OMIVV version 3.2 appliance is changed from the old appliance, configure the trap destination for the SNMP traps to point to the new appliance. For 12th generation and higher generation servers, the IP change is fixed by running inventory on these hosts. For hosts earlier than 12th generation that were compliant with earlier versions, the IP change is displayed as noncompliant and requires you to configure Dell EMC OpenManage Server Administrator (OMSA). For more information on fixing the host compliance, see **Reporting and fixing compliance for vSphere hosts** in *OpenManage Integration for VMware vCenter User's Guide* available at [Dell.com/support/manuals](http://Dell.com/support/manuals).

## Recovering OMIVV after unregistering earlier version of OMIVV

If you have unregistered the OMIVV plug-in after taking backup of the database of the earlier version, perform the following steps before proceeding with the migration:

 **NOTE: Unregistering the plug-in removes all the customization that was implemented on the registered alarms by the plug-in. The following steps do not restore the customization. However, it re-registers the alarms in their default state.**

1. Perform step 3 through step 5 in [Migrating from 2.x to 3.2](#).
2. Register the plug-in to the same vCenter that you had registered in the earlier plug-in.
3. To complete the migration, perform step 6 through step 8 in [Migrating from 2.x to 3.2](#).

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

After you complete the basic installation of the OMIVV, the **Initial Configuration Wizard** is displayed when you click the OMIVV icon. Use the **Initial Configuration Wizard** to configure the **Settings** on first launch. For subsequent instances use the **Settings** page. From the **Initial Configuration Wizard** you can create a connection profile, 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 OMIVV. For more information on the Initial Configuration Wizard, see, *OpenManage Integration for VMware vCenter User Guide* available at [dell.com/support/manuals](http://dell.com/support/manuals).

## 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:

 **NOTE: If you view a web communication error in the vCenter Web client while performing OMIVV related tasks after changing the DNS settings, perform the following:**

- Clear the browser cache.
- Logout and login from the Web client.

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 OMIVV, it must be configured.

1. In the **vSphere Web Client**, click **Home**, and then click **OpenManage Integration** icon.
2. The first time you click 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

Using the **vCenter Selection** page you can configure:

- a specific vCenter
  - all available vCenters
1. In the **Initial Configuration Wizard**, click **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.


 **NOTE: If you have multiple vCenter servers as a part of the same SSO and if you chose to configure a single vCenter server, the following steps must be repeated until you configure each vCenter.**


## 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 OMIVV. You may assign multiple servers to a single connection profile. You can create the Connection Profile using the Configuration Wizard or from **OpenManage Integration for VMware vCenter** → **Settings**.

You can log in to iDRAC and the host using Active directory credentials.

 **NOTE: Before 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 the host or it can be set as separate active directory credentials. The user credential must have administrative privileges.**

 **NOTE: You cannot 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 Configuration Wizard:

1. In the **Connection Profile Description** page, click **Next**.
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 **Use Active Directory**; otherwise skip down to configure the iDRAC credentials.
  - In **Active Directory User Name**, 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. See Microsoft Active Directory documentation for user name restrictions.
  - In **Active Directory Password**, type the password. The password is limited to 127 characters.
  - In **Verify Password**, 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**.
    - \* To not store and perform the iDRAC certificate checking during all future connections, clear **Enable Certificate Check**.
- To configure iDRAC credentials without Active Directory, do the following:
  - In **User Name**, type the user name. The user name is limited to 16 characters. See the iDRAC documentation for information about user name restrictions for your version of iDRAC.
  - In **Password**, type the password. The password is limited to 20 characters.



- In **Verify Password**, 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**.
  - \* To not store and perform the iDRAC certificate check during all future connections, clear **Enable Certificate Check**.

**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 **Use Active Directory** ; otherwise configure your **Host Credentials**.
  - In **Active Directory User Name**, 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 to 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 **Active Directory Password**, type the password. The password is limited to 127 characters.
  - In **Verify Password**, 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 **Enable Certificate Check**.
    - \* To not store and perform the Host certificate check during all future connections, clear **Enable Certificate Check**.
  - To configure Host Credentials without Active Directory, do the following:
    - In **User Name**, 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 and not just root.
    - In **Password**, type the password. The password is limited to 127 characters.

 **NOTE: The OMSA credentials are the same credentials used for ESXi hosts.**

- In **Verify Password**, 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 **Enable Certificate Check**.
  - \* To not store and perform the Host certificate check during all future connections, clear **Enable Certificate Check**.

**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 click **Test Connection**.

 **NOTE: 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**.

 **NOTE: 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]

You can configure inventory schedule using the Configuration Wizard or OpenManage Integration under **OpenManage Integration** → **Manage** → **Settings**.

 **NOTE: To make sure that the OMIVV 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 after 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, select **Enable Inventory Data Retrieval** if it is not enabled. By default, **Enable Inventory Data Retrieval** is enabled.
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 from setting option in the OMIVV. In addition, you can also run or schedule warranty retrieval job from **Job Queue** → **Warranty**. Scheduled jobs are listed in the Job queue. In an 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 is added to chassis profile.


To run a warranty retrieval job:

1. In the **Configuration Wizard**, in the **Warranty Schedule** window, select **Enable Warranty Data Retrieval** 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 **Event and Alarm** settings.




## Configuring Events And Alarms [Wizard]

You can configure events and alarms using the **Configuration Wizard** or from the **Settings** option for **Events and Alarms**. To receive the events from the servers, OMIVV is configured as the trap destination. For 12th generation hosts and later, the SNMP trap destination must be set in iDRAC. For hosts prior to 12th generation, trap generation must be set in OMSA.

 **NOTE: OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later. For hosts earlier than 12th generation, OMIVV supports only SNMP v1 alerts.**




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: You must complete this step only if Enable Alarms For Dell Hosts is selected.**  
 **NOTE: After restoring the appliance the Events and Alarms settings are not enabled even if the Graphic User Interface shows it as enabled. You must enable the Events and Alarms settings again from the Settings page.**
4. Click **Apply**.

## Creating A Chassis Profile

OMIVV can monitor all Dell Chassis associated with the Dell servers that are managed by OMIVV. Chassis profile is required to monitor the chassis. A chassis credential profile can be created to associate with a single or multiple chassis. The chassis profile is created using the following steps:

1. In the **OpenManage Integration for VMware vCenter**, select **Manage** → **Profiles** → **Credential Profiles** → **Chassis Profile**.
2. In the **Chassis Profiles** page, click the **Plus (+)** icon to create a **New Chassis Profile**.
3. In the **Chassis Profile Wizard** page, do the following:
  - a. In the **Profile Name** text box, enter the profile name.
  - b. In the **Description** text box, enter an optional description.
4. Under **Credentials** do the following:
  - a. In the **User Name** text box, type the user name with administrative rights, which is typically used to log on to the Chassis Management Controller.
  - b. In the **Password** text box, type the password for the corresponding user name.
  - c. In the **Verify Password** text box, enter the same password you have entered in the **Password** text box. The passwords must match.

 **NOTE: The credentials can be a local or active directory credentials. Before using the Active Directory credentials with a Chassis Profile, the Active Directory user's account must exist in Active Directory and the Chassis Management Controller must be configured for Active Directory based authentication.**

5. Click **Next**.

The **Select Chassis** page is displayed, which shows all the available chassis.

 **NOTE: Chassis are discovered and available to be associated with the Chassis Profile only after the successful inventory run of any modular host present under that chassis.**

6. To select either an individual chassis or multiple chassis, select the corresponding check boxes next to the **IP/Host Name** column.

If the selected chassis is already a part of another profile, a warning message is displayed, stating that the selected chassis is associated with a profile.

For example, you have a profile **Test** associated with Chassis A. If you create another profile **Test 1** and try to associate Chassis A to **Test 1**, a warning message is displayed.

7. Click **OK**.

The **Associated Chassis** page is displayed.

8. Select the chassis and click the **Test Connection** icon to test the chassis connectivity, which verifies the credentials and the result is displayed in the **Test Result** column as **Pass** or **Fail**.

9. Click **Finish** to complete the profile.



**NOTE:** You can also add or remove a chassis by clicking the Plus Icon displayed on the top left corner of the Associated Chassis page.

# 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 OMIVV, 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 OMIVV, click **Manage** → **Settings**.
2. Under **Appliance Settings**, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.
3. In the **Warranty Expiration Notification** dialog box, to enable warranty expiration notification, select **Enable warranty expiration notification for hosts**.
4. In **Minimum Days Threshold Alert**, from the **Warning** list, select the number of days before warranty expiration, that you want to be notified.
5. From the **Critical** list, select the number of days before warranty expiration, that you want to be notified.
6. Click **Apply**.

## Firmware Update Repository

In OMIVV, in the **Settings** tab, you can set the location from which the servers can receive firmware updates. This is a global setting.

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

- **Dell (ftp.dell.com)** — Uses the firmware update repository of Dell (ftp.dell.com). The OMIVV downloads selected firmware updates from Dell repository.

 **NOTE: OMIVV connects to the Internet to get the catalog and firmware packages applicable for your hosts. Depending on your network settings, configure proxy for the firmware update task to run successfully from Dell online.**

- **Shared Network Folder** — Created with Dell Repository Manager. These local repositories should be located on CIFS or NFS file share.

## Setting Up the Firmware Update Repository

You can configure the firmware update repository on the OMIVV in the **Settings** tab.

1. In OMIVV, 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 OMIVV 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 or Linux based file shares. Use the live link to go to Dell Repository Manager.
4. If you selected the **Shared Network Folder** option, 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**

 **NOTE: You can view the progress of the download in the Select Update Source page.**

5. When the download is complete, click **Apply**.

## OMSA Web Server URL

OMSA link is the URL to launch the OMSA GUI for host servers that have OMSA installed.

 **NOTE: OMSA is only required on Dell PowerEdge 11<sup>th</sup> generation servers.**

1. In OMIVV, click **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 HTTPS and the port number. For example, **https://10.0.0.1:1311** or **https://omsaur:1311**
4. Select **Apply these settings to all vCenters** 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, check if the link works.
6. Check if the OMSA Console link is functional within the Dell Host Information.

# OpenManage Integration for VMware vCenter licensing

The OpenManage Integration for VMware vCenter has two types of licenses:

- Evaluation license—when the OMIVV version 3.2 appliance is powered on for the first time, an evaluation license is automatically installed. The trial version contains an evaluation license for five hosts (servers) managed by the OpenManage Integration for VMware vCenter. This is applicable only for 11th and later generations of the Dell servers and is a default license, which is for a 90 days trial period.
- Standard license—the full product version contains a standard license for up to 10 vCenter servers and you can purchase any number of host connections managed by OMIVV.

When you upgrade from an evaluation license to a full standard license, you will receive an email about the order confirmation, and you can download the license file from the Dell Digital store that is available at <http://www.dell.com/support/licensing>. Save the license .XML file to your local system, and upload the new license file by using the **Administration Console**.

Licensing presents the following information:

- Maximum vCenter Connection Licenses—up to 10 registered and in-use vCenter connections are allowed.
- Maximum Host Connection Licenses—the number of host connections that were purchased.
- In Use—the number of vCenter connection or host connection licenses in use. For host connection, this number represents the number of hosts (or servers) that have been discovered and inventoried.
- Available—the number of vCenter connections or host connection licenses available for future use.

 **NOTE: The standard license period is for three or five years only, and the additional licenses are appended to the existing license and not over written.**

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital store that is available at <http://www.dell.com/support/licensing>. If you are unable to download your license key(s), contact Dell Support by going to [www.dell.com/support/softwarecontacts](http://www.dell.com/support/softwarecontacts) to locate the regional Dell Support phone number for your product.

## Buying and uploading software license

You are running a trial license until you upgrade to a full product version. Use the **Buy License** link from the product to navigate to the Dell website and buy a license. After you buy it, upload it using the **Administration Console**.

 **NOTE: The Buy License option is displayed only if you are using a trial license.**

1. In the OpenManage Integration for VMware vCenter, perform one of the following tasks:
  - In the **Licensing** tab, next to **Software License**, click **Buy License**.
  - In the **Getting Started** tab, under **Basic Tasks**, click **Buy License**.
2. Save the license file to a known location that you had downloaded from the Dell Digital store that is available at <http://www.dell.com/support/licensing>.
3. In a web browser, type the Administration Console URL.  
Use the format: `https://<ApplianceIPAddress>`
4. In the **Administration Console** login window, type the password and click **Login**.
5. Click **Upload license**.
6. In the **Upload License** window, to navigate to the license file, click **Browse**.

7. Select the license file, and then click **Upload**.

 **NOTE: The license file might be packaged inside a .zip file. Ensure that you unzip the .zip file and upload only the license .xml file. The license file is likely to be named based on your order number, such as 123456789.xml.**

## Options after uploading Licenses

### License file for new purchases

When you place an order for purchasing a new license, an email is sent from Dell about the order confirmation, and you can download the new license file from the Dell Digital store that is available at <http://www.dell.com/support/licensing>. The license is in an .xml format. If the license is in a .zip format, extract the license .xml file from the .zip file before uploading.

### Stacking licenses

Starting from the OMIVV version 2.1, OMIVV can stack multiple standard licenses to increase the number of supported hosts to the sum of the hosts in the uploaded licenses. An evaluation license cannot be stacked. The number of supported vCenter servers cannot be increased by stacking, and requires the use of multiple appliances.

There are some restrictions around the functionality of stacking licenses. If a new standard license is uploaded before the existing standard license expires, the licenses stack. Otherwise, if the license expires and a new license is uploaded, only the number of hosts from the new license is supported. If there are already multiple licenses uploaded, the number of supported hosts are the sum of the hosts in the non-expired licenses at the time the last license was uploaded.

### Expired licenses

Licenses that are past their support duration, typically three or five years from the date of purchase are blocked from being uploaded. If licenses have expired after being uploaded, functionality for existing hosts continues; however upgrades to new versions of the OMIVV are blocked.

### Replacement of licenses

If there is a problem with your order and you receive a replacement license from Dell, the replacement license contains the same entitlement ID of the previous license. When you upload a replacement license, the license is replaced if a license was already uploaded with the same entitlement ID.

## Enforcement

### Appliance updates

The appliance does not allow updates to newer versions when all licenses are expired. Obtain and upload a new license before attempting to upgrade the appliance.

### Evaluation License

When an evaluation license expires, several key areas cease to work, and an error message is displayed.

### Adding hosts to connection profiles

When you attempt to add a host to a connection profile, if the number of licensed 11th Generation or newer hosts exceeds beyond the number of licenses, adding extra hosts is prevented.



## For More Configuration Information

For a complete guide on Dell Management Plug-in configuration, management, and deployment options, see the *Dell Management Plug-in for VMware vCenter User's Guide*.

## Related documentation and resources

In addition to this guide, you can access the other guides available at [dell.com/support/manuals](http://dell.com/support/manuals). On the Manuals page, click **View products** under the **Choose from all products** category. In the **All products** section, click **Software & Security** → **Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 3.2** to access the following documents:

- *OpenManage Integration for VMware vCenter Quick Install Guide for vSphere Client Version 3.2*
- *OpenManage Integration for VMware vCenter for Desktop Client User's Guide Version 3.2*
- *OpenManage Integration for VMware vCenter for Web Client User's Guide Version 3.2*
- *OpenManage Integration for VMware vCenter Release Notes Version 3.2*
- *OpenManage Integration for VMware vCenter Compatibility Matrix Version 3.2*

You can find the technical artifacts including white papers at [delltechcenter.com](http://delltechcenter.com). On the Dell TechCenter Wiki home page, click **Systems Management** → **OpenManage Integration for VMware vCenter** to access the articles.

## Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:
  - For all Enterprise Systems Management documents — [Dell.com/SoftwareSecurityManuals](http://Dell.com/SoftwareSecurityManuals)
  - For OpenManage documents — [Dell.com/OpenManageManuals](http://Dell.com/OpenManageManuals)
  - For Remote Enterprise Systems Management documents — [Dell.com/esmanuals](http://Dell.com/esmanuals)
  - For OpenManage Connections Enterprise Systems Management documents — [Dell.com/OMConnectionsEnterpriseSystemsManagement](http://Dell.com/OMConnectionsEnterpriseSystemsManagement)
  - For Serviceability Tools documents — [Dell.com/ServiceabilityTools](http://Dell.com/ServiceabilityTools)
  - For OpenManage Connections Client Systems Management documents — [Dell.com/DellClientCommandSuiteManuals](http://Dell.com/DellClientCommandSuiteManuals)
  - For OpenManage Virtualization Solution documents — [Dell.com/VirtualizationSolutions](http://Dell.com/VirtualizationSolutions)
- From the Dell Support site:
  - a. Go to [Dell.com/Support/Home](http://Dell.com/Support/Home).
  - b. Under **Select a product** section, click **Software & Security**.
  - c. In the **Software & Security** group box, click the required link from the following:
    - **Enterprise Systems Management**
    - **Remote Enterprise Systems Management**
    - **Serviceability Tools**
    - **Dell Client Command Suite**
    - **Connections Client Systems Management**
    - **Virtualization Solutions**
  - d. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

