

# **OpenManage Integration for VMware vCenter Quick Install Guide for vSphere Client Version 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 © 2016 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.

January 2016

Rev. A00

# Contents

|                                                                                             |           |
|---------------------------------------------------------------------------------------------|-----------|
| <b>1 Installing OpenManage Integration for VMware vCenter.....</b>                          | <b>5</b>  |
| Installation introduction.....                                                              | 5         |
| Prerequisites.....                                                                          | 5         |
| Upgrading OpenManage Integration Plugin from 3.0 version to the current version.....        | 14        |
| Migration Path to migrate from 2.x to 3.1.....                                              | 15        |
| Recover OpenManage Integration for VMware vCenter if the older plug-in is unregistered..... | 15        |
| <b>2 Configuring OpenManage Integration for VMware vCenter .....</b>                        | <b>16</b> |
| Configuration Wizard welcome page.....                                                      | 16        |
| Creating a new Connection Profile [Wizard].....                                             | 16        |
| Configuring Events And Alarms [Wizard].....                                                 | 17        |
| Setting Up A Proxy Server [Wizard].....                                                     | 18        |
| Scheduling Inventory Jobs [Wizard].....                                                     | 18        |
| Running A Warranty Retrieval Job [Wizard].....                                              | 19        |
| Configuring the Deployment Credentials [Wizard].....                                        | 19        |
| Setting The Default Firmware Update Repository [Wizard].....                                | 20        |
| Enabling The OMSA Link [Wizard].....                                                        | 20        |
| Configuring Dell iDRAC Auto-Discovery .....                                                 | 21        |
| Configuring NFS Shares.....                                                                 | 21        |
| <b>3 Licensing in OpenManage Integration for VMware vCenter.....</b>                        | <b>23</b> |
| License Types.....                                                                          | 23        |
| Evaluation License Standard License.....                                                    | 23        |
| Viewing Information about Uploaded Licenses.....                                            | 23        |
| Uploading License.....                                                                      | 24        |
| Options After Uploading Licenses.....                                                       | 24        |
| License file for new purchases.....                                                         | 24        |
| Stacking licenses.....                                                                      | 25        |
| Expired Licenses.....                                                                       | 25        |
| Replacement of Licenses .....                                                               | 25        |
| Enforcement.....                                                                            | 25        |
| Appliance Updates.....                                                                      | 25        |
| Evaluation Licenses.....                                                                    | 25        |
| Adding Hosts to Connection Profiles.....                                                    | 25        |
| <b>4 More Configuration Information.....</b>                                                | <b>26</b> |
| <b>5 Related documentation and resources.....</b>                                           | <b>27</b> |

|                                                 |    |
|-------------------------------------------------|----|
| Accessing documents from Dell support site..... | 27 |
|-------------------------------------------------|----|

# Installing OpenManage Integration for VMware vCenter

## Installation introduction

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

### Prerequisites

The following information is needed before you start installing OMIVV:

- TCP/IP address information to be assigned to the OMIVV virtual appliance.
- A user name and password for the OMIVV to access the vCenter server. This user should be an administrator role that has all needed permissions. For information on 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, which has admin rights on the host.
- User name and password associated with iDRAC Express or Enterprise.
- Make sure that vCenter server and vSphere client are available.
- Location of the OMIVV OVF file.
- Your VMware vSphere environment must meet the virtual appliance, port access, and listening port requirements. In addition, OMIVV URL must be in the trusted sites of Internet Explorer browser.



#### NOTE:

Install Adobe Flash Player on the vSphere client system. For accessing from Windows Server 2012 and later, you must enable the **Desktop Experience Feature** to enable the flash player for Internet Explorer browser. Install the OMIVV (virtual appliance) on any ESXi host. 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 impacts 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 desired.

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

## Hardware Requirements

Following are the hardware requirements for OMIVV:

- Supported servers and minimum BIOS requirements
- Supported iDRAC versions (both deployment and management)
- OMSA support for older servers and ESXi version support (both deployment and management). For more information, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at [dell.com/support/manuals](http://dell.com/support/manuals).

## 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.

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                         | Console                      |
|------------------------------|------------------------------|
| 443 (https) and 80 (http)    | Administration console       |
| 4433 (https)                 | Auto discovery and handshake |
| 162 and 11620                | SNMP trap listener           |
| 2049, 4001, 4002, 4003, 4004 | NFS Share                    |

## Installation and Configuration Overview

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

### Installation Overview

1. Install OMIVV.
  - a. Make sure vCenter server is up and running.
  - b. Deploy an Open Virtualization Format (OVF) file that contains the OMIVV using the vSphere client.
  - c. Upload the license file.
  - d. Register the OMIVV with vCenter server using the Administration Console.
2. Complete the steps in the Configuration Wizard.
3. Enable Dell events to set up event filter options on the Settings page.

4. Enable firmware updates to download firmware updates and make them available to applicable systems.
5. Configure the Dell iDRAC user name and password.

### Deploying the OMIVV OVF Using the vSphere Client

This procedure assumes that you have downloaded the zip file from the Dell Web site.

To deploy the OMIVV OVF using the vSphere Client:

1. Unzip the file containing the OMIVV virtual disk, and run **setup.exe**.
2. Double-click the Setup.exe file to agree to the EULA, extract and obtain the OVF file.
3. Copy/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 client.
5. From the VMware vSphere client, select **File → Deploy OVF Template**.
6. In the **Source** window, use the **Browse** button to locate the OVF package. The location can be a local drive, network drive, CD/DVD, or from the Internet. The OMIVV file size is approximately 1.5 GB.  
 **NOTE:** The install can take 10-30 minutes if the OVF package resides on a network share. For the quickest installation, it is recommended that you host the OVF on a local drive.
7. Click **Next**.
8. In the **OVF Template Details** window, review the information presented.
9. Click **Next**.
10. In the **Name and Location** window, do the following:
  - a. In the **Name** text box, enter the name of the template. This name can contain up to 80 characters.
  - b. In the **Inventory Location** list, select a location to store the template.
11. Click **Next**.
12. Depending on the vCenter configuration, one of the following options displays:
  - If resource pools are configured — On the Resource Pool page, select the pool of virtual servers to which the OMIVV is deployed.
  - If resource pools are *not* configured — On the Hosts/Clusters page, select the host or cluster to which the OMIVV is deployed.
13. If there is more than one datastore available on the host, the Datastore page is displayed. Select the location to store OMIVV files, and click **Next**.
14. In the **Disk Format** window, select the format in which you want to store the virtual disks:
  - a. **Thick Provision Lazy Zeroed**  
A lazy-zeroed thick disk has all the disk space allocated at the time of creation, but each block is zeroed only on first write. This results in a shorter creation time, but reduces the performance the first time a block is written to. Subsequent writes have the same performance as eager-zeroed thick disks.
  - b. **Thick Provision Eager Zeroed [Recommended]**  
An eager-zeroed thick disk has all the space allocated and zeroed out at the time of creation. This increases the time it takes to create the disk, but results in the best performance, even on the first write to each block.
  - c. **Thin Provision [Not Recommended]**

Space required for a thin-provisioned virtual disk is allocated and zeroed upon first write, as opposed to upon creation. There is a higher I/O cost (similar to that of lazy-zeroed thick disks) during the first write to an unwritten file block, but on subsequent writes thin-provisioned disks have the same performance as eager-zeroed thick disks.

15. Click **Next**.

16. Select the appropriate network for the appliance under **Destination Networks** and click **Next**.



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

17. In the **Ready to Complete** window, review the selected options for the OVF deployment task and select **Power on after deployment** and click **Finish**. The deployment job runs and provides a completion status window where you can track the 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 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 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 client.

3. Register a vCenter server in the administration console by using a user with necessary privileges. See [Registering a vCenter server by using a user with necessary 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](#).

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 a vCenter server by using a user with necessary privileges***

You can register a vCenter server for the OMIVV appliance by using a user with the required privileges. See step 21 of [Registering OMIVV within vCenter And Importing The License File](#) for more information on registering a vCenter server.

### ***Assigning Dell privileges to the role***

You can edit an existing role to assign the Dell privileges.

 **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 client with administrative rights.
2. On the vSphere client **Home** page, click **Roles**.
3. Right-click the role to edit and select **Edit Role**.

4. 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 the Security Roles and Permissions section in *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.

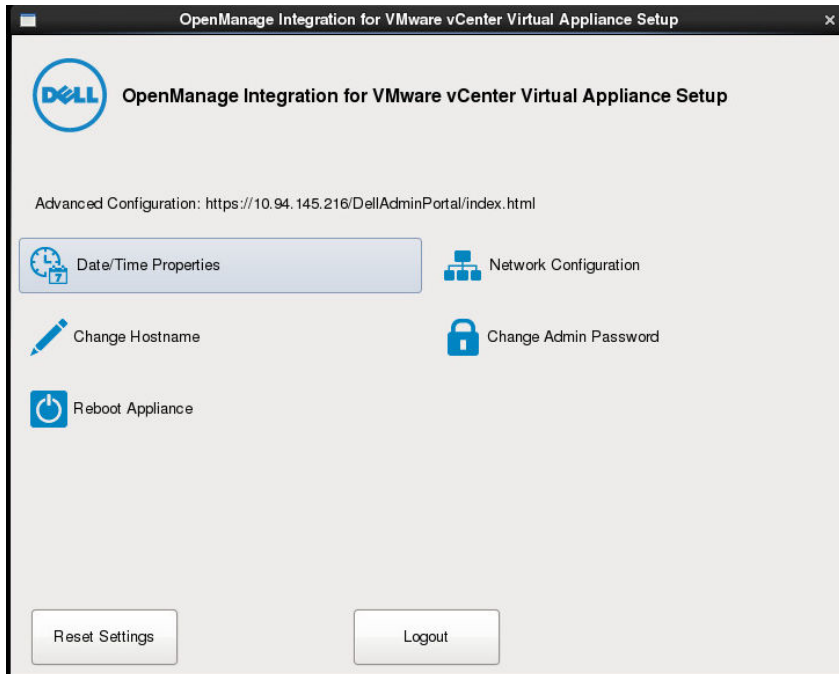


**NOTE:** For all vCenter operations, OMIVV uses the privileges of the registered user and not the privileges of the logged-in user.

### Registering OMIVV within vCenter And Importing The License File

Perform the following steps to register a vCenter server:

1. From vSphere client, select **Home** → **Hosts and Clusters**, then in the left panel, locate the deployed OMIVV, and then click **Power on the virtual machine** if not powered on already.
2. Click the **Console** tab in the main VMware vCenter window to initiate the Administration Console.
3. Allow the OMIVV to finish booting up and then enter the user name as **admin** and press **Enter**.
4. Enter a new admin password. The password must be set as per the password complexity rules displayed. Press **Enter**.
5. Re-enter the password that was provided earlier and press **Enter**.  
Press **Enter** to configure the network and time zone information in the OMIVV appliance.
6. To configure the OMIVV time zone information, click **Date/Time Properties** to set the time zone and date.



**Figure 1. Console tab**

7. In the **Date and Time** tab, select **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. Add the DNS Server detail in the **DNS Servers** field.
15. Click **Apply**.
16. To change the hostname of OMIVV appliance, click **Change Hostname**.
17. Enter a valid hostname and click **Update hostname**.
18. Open a Web browser and type the IP address or hostname of the appliance.  
For example: **https://10.210.126.120** or **https://myesxihost**. The URL is not case-sensitive.

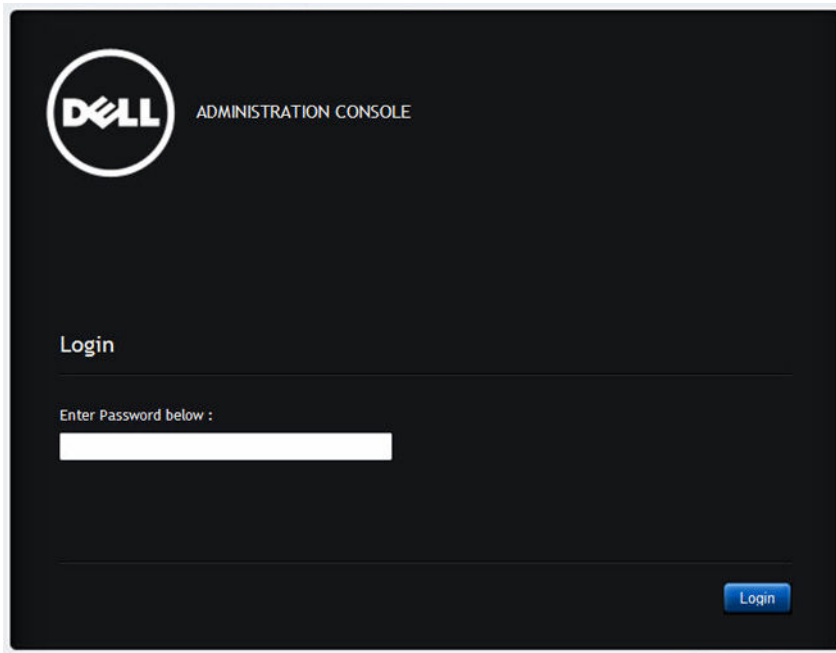


Figure 2. Administration Console

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

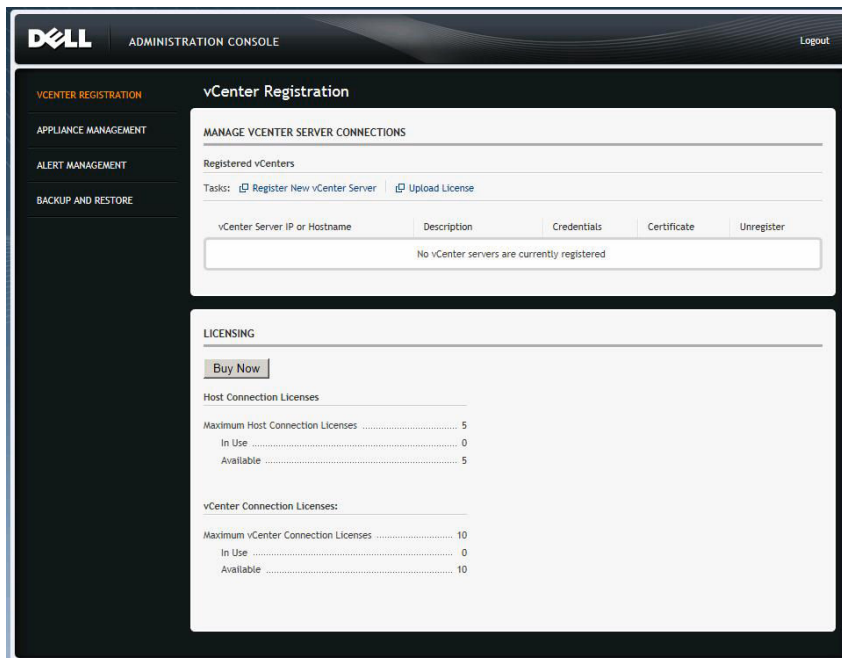


Figure 3. vCenter Registration Window from within the Administration Console

20. In the **vCenter Registration** window, click **Register a new vCenter Server**.
21. In the **Register a New vCenter** 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 description, which is optional.

- b. Under **vCenter User Account**, in the **vCenter User Name** text box, enter the Admin user name or the user name with the necessary privileges. Enter the username as domain\user or domain/user or user@domain. The Admin user account or the user name with the necessary privileges is used by the OMIVV for vCenter administration.

 **NOTE:** One instance of OMIVV can support up to 10 vCenters which are part of the same vCenter SSO. Multiple independent instances of vCenters are not currently supported.

 **NOTE:** Registering OMIVV using Fully Qualified Domain Name (FQDN) is highly recommended. For FQDN based registrations, the host name of the vCenter should be properly resolvable by the DNS server.

- c. In the **Password** text box, enter the password.  
d. In the **Verify Password** text box, enter the password again.

22. Click **Register**.

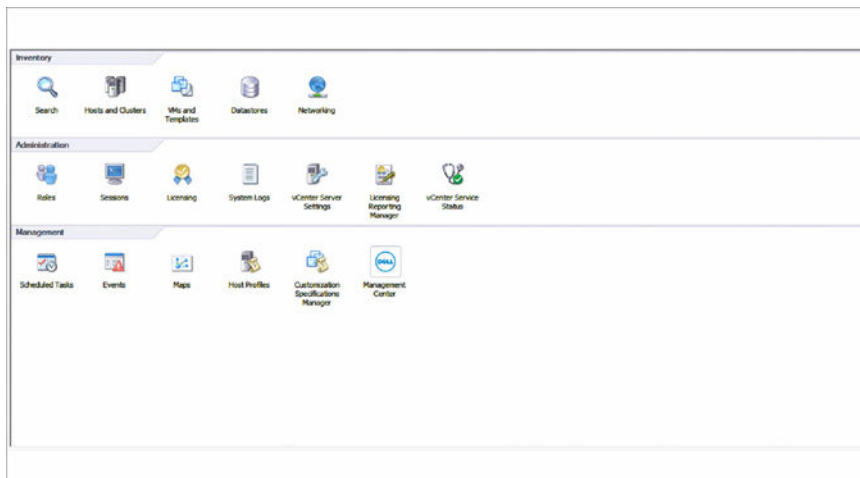
23. Do one of the following:

- If you are using the OMIVV trial version, go to step 25.
- If you are using the full product version, there is a **license.xml** file that is sent as an attachment to the registered e-mail. This file contains your product license, and you must import this license to your virtual appliance. To import the license file, click **Upload License**.

24. 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, the license file does not work.

25. Once the OMIVV is registered, the OMIVV icon is displayed under the **Management** category of the vCenter home page.



**Figure 4. The OMIVV Successfully Added to vCenter**

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

For example: Suppose, a user X with the necessary privileges registers OMIVV with vCenter and user Y has only Dell privileges. The 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 is successful:

1. Log on to vSphere client and confirm that the OMIVV icon appears inside the vSphere Client. If it does not, restart the vSphere Client and check again.
2. Check that vCenter can communicate with the OMIVV by attempting a ping command from the vCenter server to the virtual appliance IP address or hostname.
3. In **vSphere Client**, click **Plug-in** → **Managed Plug-in**. In the **Plug-in Manager** window verify that the OMIVV is installed and enabled.

## Upgrading OpenManage Integration Plugin from 3.0 version to the current version

To upgrade OpenManage Integration plug-in from version 3.0 to the current version, perform the following steps:

1. Open a web browser and enter the Administration Console URL displayed in the vSphere vCenter **Console** tab for the virtual machine you want to configure. You can also use the link displayed on the **Help and Support** page in the Dell Management Console. The URL is represented in the following format and is case-insensitive: <https://<ApplianceIPAddress>>
2. In the left pane of the **ADMINISTRATION CONSOLE** window, click **APPLIANCE MANAGEMENT**.
3. Depending on your network settings, enable proxy and provide proxy settings if your network needs proxy.
4. To upgrade OpenManage Integration plug-in from version 3.0 to the current version, do one of the following:
  - Ensure that **Update Repository Path** is set to <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> path. If the path is different, in the **Appliance Management** window, in the **APPLIANCE UPDATE** section, click **Edit** to update the path to <http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> in the **Update Repository Path** text box. Click **Apply** to save the updates.
  - 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, update the path to the offline HTTP share, and click **Apply**.
5. 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.
6. To apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
7. In the **UPDATE APPLIANCE** dialog box, click **Update**. After you click **Update**, you are logged off the **ADMINISTRATION CONSOLE** window.

 **NOTE:** While upgrading OMIVV from 3.0 to the current version, the custom certificate is not migrated and you must reapply the settings that you had applied for the certificate.

## Migration Path to migrate from 2.x to 3.1

Do the following to migrate from older version to the OMIVV 3.1 version:

1. Take a backup of the database for the older release.
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 removes all the Alarms registered on the vCenter by the plug-in and all the customization that is performed on the alarms, such as actions and so on, on the vCenter.

3. Deploy the new OpenManage Integration version 3.1 OVF.
4. Power on the OpenManage Integration version 3.1 appliance.
5. Set up the network, time zone, and so on, to the appliance. It is mandatory that the new OpenManage Integration version 3.1 appliance has the same IP address as the old appliance.



**NOTE:**

The plug-in might not work properly if the IP address for the 3.1 appliance is different from the IP address of the older appliance. In such a scenario, you should unregister and re-register all the vCenter instances.

6. Restore the database to the new appliance.
7. Verify the appliance. For more information, see **Installation Verification** in this guide to ensure the database migration is successful.
8. Run the Inventory on all the registered vCenter.



**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 **Running Inventory Jobs** in *OpenManage Integration for VMware vCenter User's Guide* available at [dell.com/support/manuals](http://dell.com/support/manuals) for steps to run the inventory on demand.

If the IP address of the new OpenManage Integration version 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 12th generation and higher generation servers, this is fixed by running the Inventory on these hosts. For hosts earlier than 12th generation that were compliant with earlier versions, this IP change shows up as noncompliant and requires you to configure OMSA.

## Recover OpenManage Integration for VMware vCenter if the older plug-in is unregistered

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



**NOTE:** Unregistering the plug-in removes all the customizations that were 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 [Migration Path to migrate from 2.x to 3.1](#).
2. Register the plug-in to the same vCenter that you had registered in the older plug-in.
3. Complete step 6 through step 8 in [Migration Path to migrate from 2.x to 3.1](#) to complete the migration.

# Configuring OpenManage Integration for VMware vCenter

After you do the basic installation of the OMIVV, it should be configured. This is typically done using the Configuration Wizard, but you can also do it using the Settings page options in the Dell Management Center.

The user interface in both the pane is similar except in the wizard, you **Save and Continue**, whereas in the **Settings** options you click **Apply**.

This section tells you how to configure using the wizard. For information about using the Dell Management Center's **Settings** options for configuring the OMIVV, see *OpenManage Integration for VMware vCenter User's Guide* available at [dell.com/support/manuals](http://dell.com/support/manuals).

## Configuration Wizard welcome page

After you install the OMVV, it must be configured.

1. In **vSphere Client**, from the **Home** page, under the **Management** tab, click the **Dell Management Center** icon.  
The first time you click the **Dell Management Center** icon, it opens the **Configuration Wizard**. You can also access this wizard on the **Dell Management Center** → **Settings** page.
2. In the **Welcome** tab, review the steps, and then click **Next**.

## Creating a new Connection Profile [Wizard]

A connection profile stores the 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 might assign multiple servers to a single connection profile. Creating the Connection Profile is similar between the Configuration Wizard and the Dell Management Center, under **Settings** option. You can configure OMIVV to connect to iDRAC and Host using Active directory credential. Prior to 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. 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:** With installations on hosts that are using 12th or later generation of the Dell PowerEdge servers, the OMSA agent installation is not required. For installations on 11th generation servers, OMSA agent is automatically installed during the deployment process.





**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, perform the following steps:

1. From the **Connection Profiles** tab, click **Create New**.
2. In the **Profile Name and Description** panel, enter the profile name, and a description that is optional that are used to help manage custom connection profiles, and then click **Next**.
3. In the **Associated Hosts** section, select the hosts to be associated with the Connection Profile, and then click **Next**.
4. View the information about credentials and connection protocols and click **Next**.
5. In the iDRAC panel, type the iDRAC credential information.
  - a. 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 configure the iDRAC local credentials. Enter **User Name**, **Password**, and **Verify Password**. The user name can contain up to 16 characters including white space. The passwords must match and use ASCII-printable characters only.
  - b. For **Certificate Check**, select **Enable** to download and store the iDRAC certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.
6. Click **Next**.
7. In the **Host Root Credentials** panel, do the following:
  - a. You must select the **Use Active Directory** check box to enable active directory credentials. Enter the User Name, Password, and Verify Password.
  - b. If you do not select **Use Active Directory**, enter the **Password**, for the **root** user and **verify password**. The passwords must match.
  - c. For **Certificate Check**, select **Enable** to download and store the OMSA/ESXi certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.
8. Click **Next**.
9. The **Test Connection** window tests the entered iDRAC and Host root Credentials on the selected servers. Test connection is optional but is recommended.
  - To begin the test, select the hosts, and click **Test Selected**. The other options are disabled.
  - To abort all the tests before completion, click **Abort All Tests**.
10. To complete the profile, click **Save**.
11. To continue on to configure Events and Alarms, click **Save and Continue**.

## Configuring Events And Alarms [Wizard]

Configure events and alarms using the Configuration Wizard or from the Dell Management Center, Settings option for Events and Alarms. In order to receive the events from the servers, OMIVV is configured as the trap destination. For 12th generation hosts and later, the SNMP trap destination is set in iDRAC. For hosts prior to 12th generation, trap generation is set in OMSA.



**NOTE:** OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later. For hosts prior to 12th generation, OMIVV supports SNMP v1 alerts.

To configure events and alarms, perform the following steps:

1. In the **Configuration Wizard**, under **Event Posting Levels**, select one of the following:
  - Do not post any events — Blocks hardware events.

- Post All Events — Posts all hardware events.
  - Post only Critical and Warning Events — Posts only critical or warning level hardware events.
  - Post only Virtualization-Related Critical and Warning Events — Posts only virtualization-related critical and warning events; this is the default event posting level.
2. To enable all hardware alarms, select the **Enable Alarms for Dell Hosts** check box.
 

 **NOTE:** Dell hosts that have alarms enabled respond to critical events by entering maintenance mode.
  3. In the dialog box that is displayed, click **Continue** to accept this change, or click **Cancel**.
 

 **NOTE:** This step is only seen if **Enable Alarms For Dell Hosts** is selected.
  4. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**.
 

It might take up to a minute before the change takes effect.
  5. To continue the wizard, click **Save and Continue**.
-  **NOTE:** Restoring the OMIIV appliance backup does not restore all the Alarm settings. However, in the OMIIV GUI, the **Alarms and Events** field displays the restored settings. To resolve this issue, in the OMIIV GUI, in the **Manage** → **Settings** tab, manually change the Events and Alarms settings.

## Setting Up A Proxy Server [Wizard]

Set the proxy server in the Configuration Wizard or later using the Dell Management Center, **Settings** → **Proxy** page.

To set up a proxy server:

1. In the **Configure HTTP Proxy window**, do one of the following:
  - To not use a proxy server, click **Save and Continue**.
  - To use a proxy server, under **Settings** enter a **Proxy Server Address**.
2. Enter the **Proxy Port number**.
3. Select the **Credentials Required** check box, if needed.
4. If you selected **Credentials Required**, do the following:
  - a. In the **Proxy User Name** text box, type the proxy user name.
  - b. In the **Proxy Password** text box, type the proxy password.
  - c. In the **Verify Password** text box, re-type the proxy password.
5. Under **Proxy**, select the **Use Proxy** check box.
6. To save these options and continue, click **Save and Continue**.

## Scheduling Inventory Jobs [Wizard]

The inventory schedule configuration is similar from the Configuration Wizard or from the **Dell Management Center** → **Settings** option. The only difference is that the wizard provides an option to select if you want to run the inventory immediately.

-  **NOTE:** To make sure that the OMIIV 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.

To schedule an inventory job:

1. In the **Configuration Wizard**, in the **Inventory Schedule** window, do one of the following:
  - To run inventory schedules, click **On Selected Days**.
  - To not run inventory schedules, select **Do not run inventory on Dell hosts**.
2. If you select **On Selected Days**, then do the following:
  - a. Select the check box next to each day of the week that you want to run the inventory.
  - 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 **Save and Continue**.

## Running A Warranty Retrieval Job [Wizard]

The warranty retrieval job configuration is similar between the wizard and from the **Dell Management Center** → **Settings** option. In addition, you can run the Warranty Retrieval Job now, from Job Queue.

To run a warranty retrieval job:

1. In the **Configuration Wizard**, on the **Warranty Schedule** window, do one of the following:
  - To run warranty schedules, click **On Selected Days**.
  - To not run warranty schedules, select **Do not retrieve Warranty Data**.
2. If you selected **On Selected Days**, then do the following:
  - a. Select the text box next to each day of the week that you want to run the warranty jobs.
  - 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 **Save and Continue**.



**NOTE:** OMIVV connects to internet to fetch the warranty information of your hosts. Depending on your network settings, you might have to configure proxy for the warranty job to run successfully.

## Configuring the Deployment Credentials [Wizard]

Deployment credentials are used to communicate securely with a bare-metal system that is discovered using AutoDiscovery. For secure communication with iDRAC, OMIVV uses deployment credentials from initial discovery until the end of the deployment process. Once deployment completes, the credentials are changed to those in the connection profile associated during deployment. If the deployment credentials are changed, all newly discovered systems from that point on are provisioned with the new credentials; however, the credentials on servers discovered prior to the change are not affected.



**NOTE:** OMIVV acts as a provisioning server. The Deployment credentials are used to communicate with iDRAC that uses the plug-in as a provisioning server in the Auto Discovery process.

To configure the deployment credentials:

1. In the **Deployment Credential** window you can view or change the credentials.
2. To change these credentials, under **Credentials for Bare Metal Server Deployment**, do the following:

- a. In the **User name** text box, edit the user name.
  - b. In the **Password** text box, edit the password.
  - c. In the **Verify Password**, text box, confirm the password.
3. To save the specified credentials and continue with the Configuration Wizard, click **Save and Continue**.

## Setting The Default Firmware Update Repository [Wizard]

Firmware repository settings contain the firmware catalog location used to update deployed servers. You can set up firmware repository initially here in the wizard or later from the Dell Management Center Settings option. In addition, you can run the firmware update later from the OpenManage Integration tab.

To set the default firmware update repository:

1. In the **Configuration Wizard**, on the **Firmware Repository** page, to choose the default repository for firmware updates, 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 they are applied as necessary.  
 **NOTE:** OMIVV connects to internet to get the catalog and firmware packages applicable to your hosts. Depending on your network settings, you might have to configure proxy for the firmware update task to run successfully from Dell online.
  - Local/shared repository  
These are created with the Dell Repository Manager application. This local repository should be a network share. OMIVV supports both NFS and CIFS shares.
2. If you selected **Local/shared repository**, do 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. If using a CIFS share, enter the **User Name**, **Password**, and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share.  
 **NOTE:** The @ character is not supported for use in shared network folder user names/ passwords.
  - c. To validate your entries click **Begin Test**.
3. To save this selection and continue the **Configuration Wizard**, click **Save and Continue**.

## Enabling The OMSA Link [Wizard]

To launch OMSA within the OMIVV virtual appliance, the OMSA Web Server must be installed and configured. See *Dell OpenManage Server Administrator Installation Guide* for instructions on how to install and configure the Web Server.

 **NOTE:** OMSA is only required on Dell servers prior to 12<sup>th</sup> Generation.

You can use OMSA to:

- Manage vCenter elements (detailed sensor/component-level health information).
  - Clear command logs and system event logs (SELs).
  - Obtain NIC statistics.
  - Make sure that the OMIVV captures events from a selected host.
1. In the **Configuration Wizard**, on the **OpenManage Server Admin** page, use the **OMSA Web Server URL** text box to enter the OMSA URL. You must include the full URL including the HTTPS.
  2. To save this URL and finish the Configuration Wizard, click **Finish**.

## Configuring Dell iDRAC Auto-Discovery

When you order servers from Dell, you can ask for the auto discovery feature enabled on the servers after you provide the provisioning server IP Address. The provisioning server IP address is the IP address of OMIVV. In such a scenario, after you receive the servers from Dell, when you power on the servers after mounting and connecting the iDRAC cable, the servers get auto discovered. The servers get listed in the first page of the Deployment wizard.

 **NOTE:** For the servers which are auto discovered, the credentials that are provided under **Dell Management Center → Settings → Deployment Credentials** are used for further communication with the server, until the OS deployment is completed. After a successful OS deployment, the iDRAC credentials that are provided in the associated connection profile are set.

 **NOTE:** Make sure that the **Server White List** is disabled or the service tag of the servers that are to be auto discovered are added in the **Server White List** under **Dell Management Center → Settings → Security**

Perform the following steps to enable Auto Discovery manually on the target machine:

1. Boot / Reboot the target system and press F2 during initial boot to go to System Setup.
2. Go to **iDRAC Settings → User Configuration** and disable the root user. Make sure that there are no other users when you are disabling the root user there should not be any user with administrator privileges active on that iDRAC.
3. Click **Back**, and click **Remote Enablement**.
4. Set the **Enable Auto-Discovery** as **Enabled** and set **Provisioning Server** as the IP address of the OMIVV.
5. Save the settings.
6. The server is auto discovered upon next server boot. After successful Auto-Discovery, the root user gets enabled, and the **Enable Auto-Discovery** flag gets disabled automatically.

## Configuring NFS Shares

To use NFS shares with the OMIVV for backup and restore operations, firmware updates, and as a staging folder, there are certain configuration items that you must complete. CIFS shares do not require additional configuration.

To configure NFS shares:

1. On the Linux or Unix OS machine hosting the NFS shares, edit **/etc/exports** to add: **/share/path <appliance IP> (rw) \*(ro)**.

This allows the virtual appliance full read and write access to the share, but limits all other users to read only.

2. Start nfs services:

```
service portmap start
service nfs start
service nfslock status
```



**NOTE:** The steps above may vary depending on the Linux distribution in use.

3. If any of the services were already running:

```
exportfs -ra
```

# Licensing in OpenManage Integration for VMware vCenter

This chapter provides details about licensing in OMIVV. There are no new licensing changes for 3.1.



**NOTE:** The Licensing for OMIVV does not alter the number of vCenter connection licenses. The maximum number of vCenter licenses is 10. If you want to register multiple vCenters, all vCenters should be part of same SSO. Separate instances of vCenters are not supported in this OMIVV release.

## License Types

With version 3.1, there are two types of licenses. An evaluation license and a standard license. These licenses restrict functionality based on time and the number of Dell 11th Generation or newer hosts.

### Evaluation License

When the OMIVV version 3.x appliance is powered on for the first time, an evaluation license is automatically installed. This evaluation license allows the OMIVV to operate and manage five Dell hosts (11th Generation and later) and newer hosts without blocking any functionality for the 90 day evaluation period from the first power on. Once a standard license is uploaded, the evaluation license is no longer used.

### Standard License

A standard license is purchased from Dell. Different purchase SKU's are used when ordering the license based on the number of Dell 11th Generation or newer servers running VMware ESXi to be managed, and the duration of product support. The license includes product support and appliance updates for a periods of either 3 or 5 years.

## Viewing Information about Uploaded Licenses

There are several locations where information about licenses can be viewed. Licenses can only be uploaded using the Upload License link in the Dell Administration Console. Information about specific licenses are not available in the 3.1 release.

- **The Dell Administration Console:**

Information about the licenses in use and consumed can be seen in the vCenter Registration page of Dell Administration console.

- **The Dell Management Console :**

Information about the license can be seen from within the integration. Licensing information is available from the Dell Management console's overview page, or if using the web client, from the OMIWV Licensing tab.

- **License Messaging:**

There are several informational, error, or warning messages that can be displayed.

- a. **License expiring soon:**

Starting within 30 days of a license expiration, a message is displayed informing how many days are remaining for that license.

- b. **License has expired and is in a grace period:**

After a license expires, it will enter a 90 day grace period.

- c. **All Licenses have expired:**

If all of the licenses have expired, a message appears within the integration. Additionally, some license enforcement, such as the inability to upgrade for standard licenses, or the loss of functionality when using an evaluation license.

- d. **Number of host licenses has been exceeded:**

When creating or editing connection profiles, if the number of hosts licenses exceeds the number of licenses available for new servers to be added to a connection profile, an error message might be displayed. To successfully add new hosts after receiving this message, ensure that you have at least one valid license, and attempt adding fewer servers at a time to the connection profile. This allows an inventory to complete on the newly added servers prior to attempting to add additional servers.

## Uploading License

When a license is purchased, an email is sent to you containing the license file. The license must be uploaded from the web administration console, accessible by using the ip address of the appliance.

1. Licenses are uploaded using the Upload License link in the vCenter Registration page.
2. After clicking the Upload License link, the Upload License dialog box appears.
3. Browse to the license XML file and click Upload.



**NOTE:** The license file might be packaged inside a zip file. Be sure to 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.

4. The Upload License file displays a success message if the license upload is successful.

## Options After Uploading Licenses

### License file for new purchases

When purchasing a new license, an email is sent from Dell containing the new license file. The license should arrive in a .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 OMIVV version 2.1, OMIVV has the ability to 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 vCenters cannot be increased by stacking, and would require 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 will 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 will continue; 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 uploading a replacement license, if a license was already uploaded with the same entitlement ID it will be replaced.

## **Enforcement**

### **Appliance Updates**

The appliance will not allow updates to newer versions when all licenses are expired. Please obtain and upload a new license prior to attempting to upgrade the appliance.

### **Evaluation Licenses**

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

### **Adding Hosts to Connection Profiles**

When attempting to add a host to a connection profile, if the number of licensed 11th Generation or newer hosts is exceeded and beyond the license number, adding additional hosts is prevented.

## More Configuration Information

For a complete guide on OMIVV configuration, management, and deployment options, see *OpenManage Integration for VMware vCenter User's Guide* available at [Dell.com/support/manuals](http://Dell.com/support/manuals).

## Related documentation and resources

In addition to this guide, you can access the other guides available at [dell.com/support/manuals](https://dell.com/support/manuals). On the Manuals page, click **View products** under the **Browse for a product** category. In the **Select a product** section, click **Software and Security** → **Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 3.1** to access the following documents:

- *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.1*
- *OpenManage Integration for VMware vCenter for Desktop Client User's Guide Version 3.1*
- *OpenManage Integration for VMware vCenter for Web Client User's Guide Version 3.1*
- *OpenManage Integration for VMware vCenter Release Notes Version 3.1*
- *OpenManage Integration for VMware vCenter Compatibility Matrix Version 3.1*

You can find the technical artifacts including white papers at [delltechcenter.com](https://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](https://dell.com/SoftwareSecurityManuals)
  - For OpenManage documents — [Dell.com/OpenManageManuals](https://dell.com/OpenManageManuals)
  - For Remote Enterprise Systems Management documents — [Dell.com/esmmanuals](https://dell.com/esmmanuals)
  - For OpenManage Connections Enterprise Systems Management documents — [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://dell.com/OMConnectionsEnterpriseSystemsManagement)
  - For Serviceability Tools documents — [Dell.com/ServiceabilityTools](https://dell.com/ServiceabilityTools)
  - For OpenManage Connections Client Systems Management documents — [Dell.com/DellClientCommandSuiteManuals](https://dell.com/DellClientCommandSuiteManuals)
  - For OpenManage Virtualization Solution documents — [Dell.com/VirtualizationSolutions](https://dell.com/VirtualizationSolutions)
- From the Dell Support site:
  - a. Go to [Dell.com/Support/Home](https://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.