OpenManage Integration for VMware vCenter Version 4.0

Web Client Installation Guide

February 2017
Rev. A00

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

1

Introduction

This guide provides step-by-step instructions for installing and configuring OpenManage Integration for VMware vCenter (OMIVV) on the Dell PowerEdge servers. After the OMIVV installation, for information about all aspects of administration including—inventory management, monitoring and alerting, firmware updates, and warranty management; see *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals`.

Topics:

OpenManage Integration for VMware vCenter licensing

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

- Evaluation license—when the OMIVV version 4.x 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. 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. If you are unable to download your license key(s), contact Dell Support by going to 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.
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. 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.

Important notes for reference

- From OMIVV 4.0 onwards, only VMware vSphere Web client is supported and the vSphere Desktop client is not supported.
- For vCenter 6.5 and later, the OMIVV appliance is only available for the flash version. The OMIVV appliance is not available for the HTML5 version.
- For using the DNS server, the recommended practices are:
  - OMIVV supports only IPv4 IP addresses. Although both static IP assignment and DHCP assignment are supported, Dell recommends you to assign a static IP address. Assign a static IP address and host name when you deploy an OMIVV appliance with a valid DNS registration. A static IP address ensures that during the system restart, the IP address of the OMIVV appliance remains same.
  - Ensure that OMIVV host name entries are present in both forward and reverse lookup zones in your DNS server.

  For more information about the DNS requirements for vSphere, see the following VMware links:

  - DNS requirments for vSphere 5.5
  - DNS requirements for vSphere 6.0
  - DNS requirements for vSphere 6.5 and Platform Services Controller appliance
- For the OMIVV appliance mode, ensure that you deploy OMIVV in the appropriate mode based on your virtualization environment. For more information, see System requirements for deployment modes on page 6.
- Configure your network to match the port requirements. For more information, see Port information on page 7.

Hardware requirements

OMIVV provides full support for several generations of the Dell servers with full feature support for servers with iDRAC Express or Enterprise. Extensive information on the platform requirements is available in *OpenManage Integration for VMware vCenter Release Notes* available at `Dell.com/support/manuals`. To verify that your host servers are eligible, see information about the following in *OpenManage Integration for VMware vCenter Compatibility Matrix* available at `Dell.com/support/manuals`:

- Supported server and minimum BIOS
- iDRAC supported versions (both deployment and management)
- OMSA support for 11th generation and older servers, and the ESXi version support (both deployment and management)

OMIVV requires LAN on motherboard/Network daughter card that can access both iDRAC/CMC systems management network and the vCenter management network.

System requirements for deployment modes

Ensure that the following system requirements for the desired deployment modes are met:

Table 1. System requirements for deployment modes

Deployment modes	Number of hosts	Number of CPUs	Memory—in GB
Small	up to 250	2	8
Medium	up to 500	4	16
Large	up to 1000	8	32

NOTE: For any of the mentioned deployment modes, ensure that you reserve sufficient amount of memory resources to the OMIVV virtual appliance by using reservations. See vSphere Documentation for steps about reserving memory resources.

Software requirements

Ensure that the vSphere environment fulfills virtual appliance, port access, and listening port requirements.

Requirements for VMware vSphere web client

- Supports vCenter 5.5 and later. For all supported vCenter versions, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at `Dell.com/support/manuals`.
- Requires web client services from vCenter (vSphere Desktop client is not supported)

For specific software requirements, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at `Dell.com/support/manuals`.

Space required for provisioned storage

The OMIVV virtual appliance requires at least 44 GB of disk space for provisioned storage.

Default virtual appliance configuration

The OMIVV virtual appliance is provisioned with 8 GB of RAM and 2 virtual CPU.

Port information

Virtual appliance and managed nodes

In OMIVV, when you deploy the OMSA agent by using the *Fix non-compliance hosts* link available in the **Fix Non-compliant vSphere Hosts** wizard, OMIVV performs the following action:

- Starts the HTTP Client service
- Enables port 8080
- Makes the port available for ESXi 5.0 or later to download and install OMSA VIB

After the OMSA VIB installation is complete, the service automatically stops and the port is closed.

Table 2. Virtual appliance

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
53	DNS	TCP	None	Out	DNS client	No
80	HTTP	TCP	None	Out	Dell Online Data Access	No
80	HTTP	TCP	None	In	Administration Console	No
162	SNMP Agent	UDP	None	In	SNMP Agent (server)	No
443	HTTPS	TCP	128-bit	In	HTTPS server	No
443	WSMAN	TCP	128-bit	In/Out	iDRAC/OMSA communication	No

Table 2. Virtual appliance

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
4433	HTTPS	TCP	128-bit	In	Auto Discovery	No
2049	NFS	UDP/TCP	None	In/Out	Public Share	No
4001-4004	NFS	UDP/TCP	None	In/Out	Public Share	No
5432	Postgres	TCP	128-bit	In/Out	PostgreSQL	No
11620	SNMP Agent	UDP	None	In	SNMP Agent (server)	No

Table 3. Managed nodes

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162, 11620	SNMP	UDP	None	Out	Hardware Events	No
443	WSMAN	TCP	128-bit	In	iDRAC/OMSA communication	No
4433	HTTPS	TCP	128-bit	Out	Auto Discovery	No
2049	NFS	UDP	None	In/Out	Public Share	No
4001-4004	NFS	UDP	None	In/Out	Public Share	No
443	HTTPS	TCP	128-bit	In	HTTPS server	No
8080	HTTP	TCP		In	HTTP server; downloads the OMSA VIB and fixes noncompliant vSphere hosts	No
50	RMCP	UDP/TCP	128-bit	Out	Remote Mail Check Protocol	No
51	IMP	UDP/TCP	None	N/A	IMP Logical Address Maintenance	No
5353	mDNS	UDP/TCP		In/Out	Multicast DNS	No
631	IPP	UDP/TCP	None	Out	Internet Printing Protocol (IPP)	No
69	TFTP	UDP	128-bit	In/Out	Trivial File Transfer	No
111	NFS	UDP/TCP	128-bit	In	SUN Remote Procedure Call (Portmap)	No
68	BOOTP	UDP	None	Out	Bootstrap Protocol Client	No

Prerequisite checklist

Checklist before you start the product installation:

- Verify that you have user name and password for OMIVV to access the vCenter server. The user can have an administrator role that has all necessary permissions or a non-administrator user with the necessary privileges. 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`.
- Check that you have the root password for the ESXi host systems, or the Active Directory credentials that has administrative rights on the host.
- Check whether you have the user name and password associated with iDRAC Express or Enterprise.
- Check if the vCenter server is running.
- Determine the location of the OMIVV installation directory.
- Check to ensure that VMware vSphere environment meet virtual appliance, port access, and listening port requirements. Also, install Adobe Flash Player on a client system, if necessary. For more information on the supported Flash Player version, see *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 OMIVV appliance or anytime later, if necessary.

ⓘ **NOTE:** Dell recommends that OMIVV and vCenter server are on the same network.

ⓘ **NOTE:** The OMIVV appliance network should have access to iDRAC, host, and vCenter.

Installing, configuring, and upgrading OMIVV

Ensure that the hardware requirements are met and you are running the required VMware vCenter software.

The following high-level steps outline the overall installation and configuration procedure for OMIVV:

1. Download the *Dell_OpenManage_Integration_<version number>.<build number>.zip* file from the Dell support website at `Dell.com/support`.
2. Navigate to the location where you have downloaded the file, and extract its contents.
3. Deploy the Open Virtualization Format (OVF) file that contains the OMIVV appliance by using the vSphere web client. See Deploying the OMIVV OVF.
4. Upload the license file. For more information about licensing, see Uploading license.
5. Register the OMIVV appliance with the vCenter server by using Administration Console. See Registering OMIVV and importing the license file.
6. To configure the appliance, complete the **Initial Configuration Wizard**. See the Configuration tasks through the configuration wizard.

Deploying OMIVV OVF using vSphere web client

Ensure that you have downloaded and extracted the product .zip file, *Dell_OpenManage_Integration_<version number>.<build number>.zip* from the dell website.

1. Locate the OMIVV virtual disk that you downloaded and extracted and run **Dell_OpenManage_Integration.exe**.

   The supported client OS version for extracting and running the exe is Windows 7 SP1 and later.

   The supported server OS version for extracting and running the exe is Windows 2008 R2 and later.
2. Accept **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 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, perform the following subtasks:

a. Select **URL** if you want to download the OVF package from Internet.
b. Select the **Local file** and click **Browse** if you want to select the OVF package from your local system.

ⓘ **NOTE:** The installation process can take between 10-30 minutes if the OVF package resides on a network share. For a quick installation, Dell recommends that you host the OVF on a local drive.

7. Click **Next**.
   The **Review Details** window is displayed with the following information:
   - **Product**—The OVF template name is displayed.
   - **Version**—The version of the OVF template is displayed.
   - **Vendor**—The vendor name is displayed.
   - **Publisher**—The publisher details are displayed.
   - **Download Size**—The actual size of the OVF template in gigabytes is displayed.
   - **Size on Disk**—Details of thick and thin provisioned details are displayed.
   - **Description**—The comments are displayed here.
8. Click **Next**.
   The **Select Name and Folder** window is displayed.
9. In the **Select Name and Folder** window, perform the following substeps:
   a. In **Name**, enter the name of the template. The name can include up to 80 characters.
   b. In the **Select a folder or datacenter** list, select a location for deploying the template.
10. Click **Next**.
    The **Select Storage** window is displayed.
11. In the **Select Storage** window, perform the following substeps:
    a. In the **Select Virtual Disk Format** drop-down list, select either of the following formats:
    - `Thick Provision (lazy Zeroed)`
    - `Thick Provision (Eager zeroed`
    - `Thin Provision`

    Dell recommends that you select, Thick Provision (Eager Zeroed).

    b. In the **VM Storage Policy** drop-down list, select a policy.
12. Click **Next**.
    The **Setup Networks** window is displayed that includes details about the source and destination networks.
13. In the **Setup Networks** window, click **Next**.

    ⓘ **NOTE:** Dell recommends that the OMIVV appliance and the vCenter server are located in the same network.

14. 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 the job progress.

Registering vCenter server by non-administrator user

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

To enable a non-administrator user with the required privileges to register a vCenter server, perform the following steps:

1. To change the privileges selected for a role, add the role and select the required privileges for the role or modify an existing role.

   See VMware vSphere documentation for the steps required to create or modify a role and select privileges in the vSphere web client. To select all the required privileges for the role, see the Required privileges for non-administrator users.

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

2. Assign a user to the newly created role after you define a role and select privileges for the role.

   See VMware vSphere documentation for more information on assigning permissions in the vSphere web client.

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

   A vCenter server non-administrator user with the required privileges can now register and/or unregister vCenter, modify credentials, or update the certificate.

3. Register a vCenter server by using a non-administrator user with the required privileges. See Registering a vCenter server by a non-administrator user with the required privileges.
4. Assign the Dell privileges to the role created or modified in step 1. See Assigning Dell privileges to the role in vSphere web client.

A non-administrator user with the required privileges can now use the OMIVV features with the Dell hosts.

Required privileges for non-administrator users

To register OMIVV with vCenter, a non-administrator user requires the following privileges:

> **NOTE:** While registering a vCenter server with OMIVV by a non-administrator user, an error message is displayed if the following privileges are not assigned.

- Alarms
  - Create alarm
  - Modify alarm
  - Remove alarm
- Extension
  - Register extension
  - Unregister extension
  - Update extension
- Global
  - Cancel task
  - Log event
  - Settings

  > **NOTE:** Assign the following health update privileges, if you are using VMware vCenter 6.5 or upgrading to vCenter 6.5 or later:
- Health Update Provider
  - Register
  - Unregister
  - Update
- Host
  - CIM
    - CIM Interaction
  - Configuration
    - Advanced settings
    - Connection
    - Maintenance
    - Query patch
    - Security profile and firewall

    > **NOTE:** Assign the following privileges, if you are using VMware vCenter 6.5 or upgrading to vCenter 6.5 or later:
    > - Host.Config
    >   - Advanced settings
    >   - Connection
    >   - Maintenance
    >   - Query patch
    >   - Security profile and firewall
  - Inventory
    - Add host to cluster
    - Add standalone host
    - Modify cluster

      > **NOTE:** Ensure that you assign the modify cluster privilege, if you are using vCenter 6.5 or upgrading to vCenter 6.5 or later.
- Host profile
  - Edit

    - View
- Permissions
    - Modify permission
    - Modify role
- Sessions
    - Validate session
- Task
    - Create task
    - Update task

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 on page 12 for information on registering a vCenter server through a non-administrator user or as an administrator.

Assigning Dell privileges to existing 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.

1. Log in to the vSphere web client with administrative rights.
2. Browse to **Administration → Roles** in the vSphere web client.
3. Select a vCenter server system from the **Roles provider** drop-down list.
4. Select the role from the **Roles** list, and click the ✏ icon.
5. Select the following Dell privileges for the selected role and click **OK**:
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting

    See Security roles and permissions in *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals` for more information about 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.

ⓘ **NOTE:** If specific pages of OMIVV are accessed with no Dell privileges assigned to the logged-in user, the 2000000 error is displayed.

Registering OpenManage Integration for VMware vCenter and importing license file

Ensure that your licenses are ready for download at http://www.dell.com/support/licensing. If you have ordered more than one license, they might be shipped separately at different times. You can check the status of other license items at Order status. The license file is available as an .XML format.

ⓘ **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. Ensure that the admin password complies with 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**.

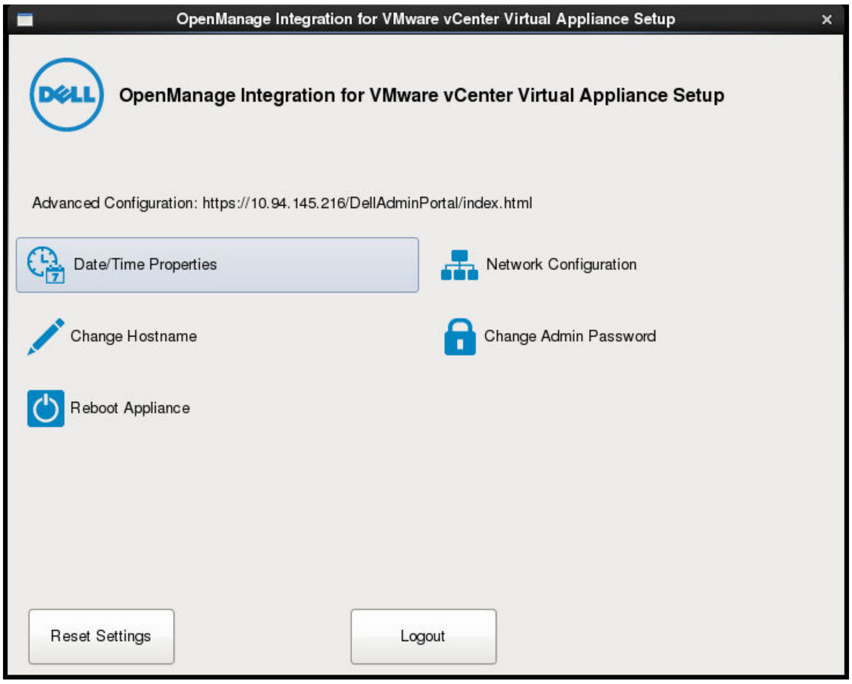

OpenManage Integration for VMware vCenter Virtual Appliance Setup
OpenManage Integration for VMware vCenter Virtual Appliance Setup
Advanced Configuration: https://10.94.145.216/DellAdminPortal/index.html
Date/Time Properties
Network Configuration
Change Hostname
Change Admin Password
Reboot Appliance
Reset Settings
Logout

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 then add a valid IP, 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 or Appliance hostname>` 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` or `Https://myesxihost`
The URL is not case-sensitive.

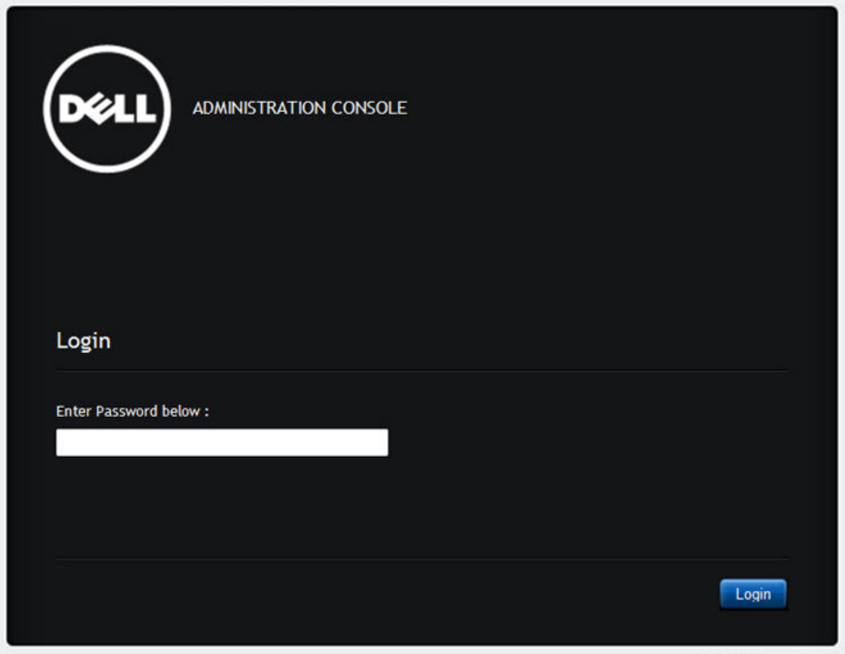
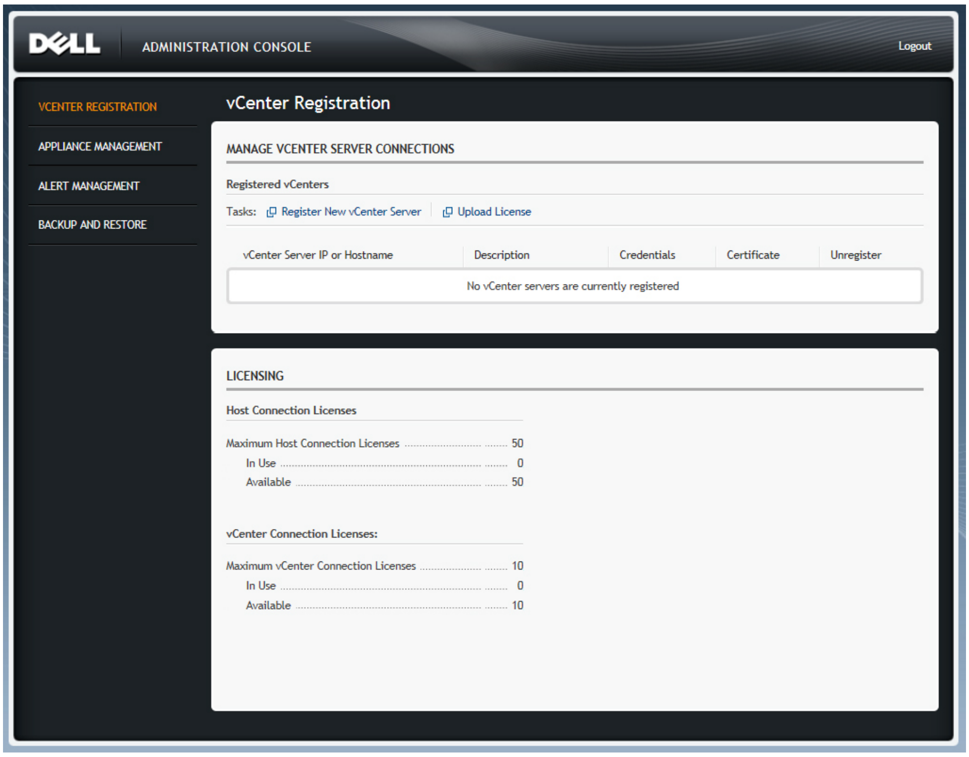


Figure 2. Administration Console

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



vCenter Server IP or Hostname	Description	Credentials	Certificate	Unregister
No vCenter servers are currently registered				

LICENSING

Host Connection Licenses

Maximum Host Connection Licenses	50
In Use	0
Available	50

vCenter Connection Licenses:

Maximum vCenter Connection Licenses	10
In Use	0
Available	10

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 can be downloaded from the Dell Digital store, 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 (.XML file) does not work and you can download the .XML file (license key) through the Dell Digital store. If you are unable to download your license key(s), contact Dell Support by going to www.dell.com/support/softwarecontacts to locate the regional Dell Support phone number for your product.

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

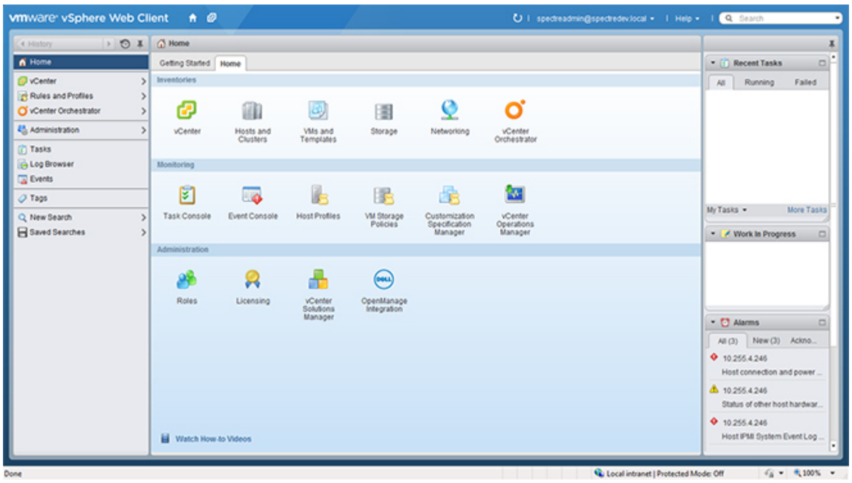


Figure 4. OpenManage Integration for VMware vCenter successfully added to vCenter

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.

Upgrading registered vCenter

You can upgrade a registered vCenter for non-administrator users or administrator users. Before upgrading a registered vCenter, see the VMware Documentation if you upgrade to the latest version of the vCenter server, such as vCenter 6.5. Perform the tasks in either of the following options after upgrading a registered vCenter, as applicable:

- For non-administrator users:
  1. Assign extra privileges to non-administrator users, if necessary. See Required privileges for non-administrator users on page 11.

     For example, when you upgrade from vCenter 6.0 to vCenter 6.5, assign the extra privileges.
  2. Reboot the registered OMIVV appliance.
- For administrator users:
  1. Reboot the registered OMIVV appliance.

Verifying installation

The following steps verify that the OMIVV installation is 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. Ensure that vCenter can communicate with OMIVV by attempting a PING command from the vCenter server to the virtual appliance IP address or host name.
4. In **vSphere Web Client**, click **Plug-ins** > **Managed Plug-ins**.
5. In the **Plug-in Manager** window, verify if OMIVV is installed and enabled.

Migrating from 3.x to 4.0

You can start with a fresh deployment of the v4.0 OVF after uninstalling the old version and then migrate the data from older version (3.x) to 4.0 version by using backup and restore path.

To migrate from an older version to the OMIVV 4.0 version, perform the following steps:

1. Take a backup of the database for the older (v3.x) release.

   For more information, see *OpenManage Integration for VMware vCenter User's Guide* available at `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 4.0 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 4.0 appliance.
5. Set up the network and time zone on the appliance.

   Ensure that the new OpenManage Integration version 4.0 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 4.0 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`.

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 plug-in 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 4.0 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 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`.

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 3.x to 4.0.
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 3.x to 4.0.

2

Appliance configuration for VMware vCenter

After you complete the basic installation of OMIVV and registration of the vCenters, the **Initial Configuration Wizard** is displayed when you click the OMIVV icon. You can proceed to configure the appliance by using one of the following methods:

- Configuring the appliance through the **Initial Configuration Wizard**.
- Configuring the appliance through the **Settings** tab in OMIVV.

You can use the **Initial Configuration Wizard** to configure the OMIVV appliance settings on first launch. For subsequent instances, use the **Settings** tab.

ⓘ **NOTE:** The user interface in both the methods is similar.

Topics:

Configuration tasks through configuration wizard

ⓘ **NOTE:** If you view a web communication error while performing OMIVV-related tasks after changing the DNS settings; clear the browser cache, and log out from the web client and then log in again.

By using the configuration wizard, you can view and perform the following tasks:

- View configuration wizard welcome page
- Select vCenters. See Selecting vCenters.
- Create a connection profile. See Creating a connection profile.
- Configure events and alarms. See the Configuring events and alarms.
- Schedule inventory jobs. See the Scheduling inventory jobs.
- Run a warranty retrieval job. See Running a warranty retrieval job.

Viewing configuration wizard welcome dialog box

To configure OMIVV after installing and registering with the vCenter, perform the following steps to view the **Initial configuration Wizard**:

1. In vSphere web client, click **Home**, and then click the **OpenManage Integration** icon.

   You can perform any one of the following options to access the initial configuration wizard:

   - The first time you click the **OpenManage Integration** icon, **Initial Configuration Wizard** is displayed automatically.
   - From **OpenManage Integration** > **Getting Started**, click **Start Initial Configuration Wizard**.
2. In the **Welcome** dialog box, review the steps, and then click **Next**.

Selecting vCenters

In the **vCenter Selection** dialog box, you can configure the following vCenters:

- A specific vCenter
- All registered vCenters

To access the **vCenter Selection** dialog box:

1. In the **Initial Configuration Wizard**, in the **Welcome** dialog box, click **Next**.
2. Select one vCenter or all registered vCenters from the **vCenters** drop-down list.

Select a vCenter that is not configured yet or if you have added a vCenter to your environment. The vCenter selection page allows you to select one or more vCenters to configure settings.

3. To proceed with the **Connection Profile Description** dialog box, click **Next**.

   ⓘ **NOTE:** If you have multiple vCenter servers that are part of the same single sign-on (SSO), and if you choose to configure a single vCenter server, repeat steps 1 through 3 until you configure each vCenter.

Creating connection profile

Before using the Active Directory credentials with a connection profile, ensure that:

- The Active Directory user's account exist in Active Directory.
- The iDRAC and host are configured for Active Directory based authentication.

A connection profile stores the iDRAC and host credentials that OMIVV uses to communicate with the Dell servers. Each Dell server must be associated with a connection profile to be managed by OMIVV. You might assign multiple servers to a single connection profile. You can create a connection profile by using the configuration wizard or from the **OpenManage Integration for VMware vCenter** > **Settings** tab. You can log in to iDRAC and the host by using the Active Directory credentials.

ⓘ **NOTE:** The Active Directory credential can be either same or separate for both iDRAC and the host.

ⓘ **NOTE:** You cannot create a connection profile if the number of added hosts exceeds the license limit for creating a connection profile.

All hosts that are running ESXi 6.5 or later have the Web-Based Enterprise Management (WBEM) service disabled by default. OMIVV requires this service to be running for retrieving iDRAC IP through hosts. This service can be enabled from the connection profile wizard. Alternatively, the WBEM service is automatically enabled if you install OMSA on the host.

ⓘ **NOTE:** OMIVV does not depend on OMSA for its work-flows from 12th and later generations of the Dell servers.

1. In the **Connection Profile Description** dialog box, click **Next**.
2. In the **Connection Profile Name and Credentials** dialog box, enter the connection **Profile Name** and connection profile **Description**, which is optional.
3. In the **Connection Profile Name and Credentials** dialog box, under **iDRAC Credentials**, do either of the following actions, depending on configuring iDRAC with or without Active Directory:

   ⓘ **NOTE:** The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.

   - The iDRACs that are already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**; otherwise scroll down to configure the iDRAC credentials.
     a. In Active Directory **User Name**, type the user name. Type the user name in one of these formats: `domain\username` or username@domain. The user name is limited to 256.
     b. In Active Directory **Password**, type the password. The password is limited to 127 characters.
     c. In **Verify Password**, type the password again.
     d. Depending on your requirement, 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**.
   - To configure the iDRAC credentials without Active Directory, perform the following tasks:
     a. 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 the version of iDRAC that you are using.
     b. In **Password**, type the password. The password is limited to 20 characters.
     c. In **Verify Password**, type the password again.
     d. 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 **Host Root**, perform one of the following steps:

- The hosts that are already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**, and perform the following steps; otherwise configure your host credentials:
  a. In Active Directory **User Name**, type the user name. Type the user name in one of these formats: `domain\username` or username@domain. The user name is limited to 256 characters.

     NOTE: For host user name and domain restrictions, see the following:

     Host user name requirements:

     - Between 1 and 64 characters long
     - No nonprintable characters
     - No Invalid characters, such as " / \ [ ] : ; | = , + * ? < > @

     Host domain requirements:

     - Between 1 and 64 characters long
     - First character must be alphabetical
     - Cannot contain a space
     - No Invalid characters, such as " / \ [ ] : ; | = , + * ? < > @

  b. In Active Directory **Password**, type the password. The password is limited to 127 characters.
  c. In **Verify Password**, type the password again.
  d. 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 iDRAC certificate check during all future connections, clear **Enable Certificate Check**.
- To configure host credentials without Active Directory, perform the following tasks:
  a. In **User Name**, the user name is **`root`**, which is the default user name and you cannot change the user name. However, if the Active directory is set, you can choose any Active directory user and not root.
  b. In **Password**, type the password. The password is limited to 127 characters.

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

  c. In **Verify Password**, type the password again.
  d. 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 **Connection Profile Associated Hosts** dialog box, select the hosts for the connection profile and click **OK**.

   NOTE: If you select hosts that are running ESXi 6.5 or later, ensure that you click the icon for enabling the WBEM service on all those hosts.

7. To test the connection profile, select one or more hosts and click **Test Connection**.

   NOTE: This step is optional and checks whether the host and iDRAC credentials are correct or not. Although this step is optional, Dell recommends you to test the connection profile.

   NOTE: The test connection fails if the WBEM service is disabled on hosts with ESXi 6.5 or later.

8. To complete the creation of profile, click **Next**.
   After you click next, all details that you provide in this wizard is saved and you cannot modify the details from the wizard. You can modify or create more connection profiles for this vCenter detail from the **Manage** > **Profiles Connection Profiles** page after completing the configuration from the configuration wizard. See **Modifying connection profile** in *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals`.

NOTE: The servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result is not applicable for this system.

Scheduling inventory jobs

You can configure inventory schedule by using the configuration wizard or OpenManage Integration under the **OpenManage Integration** > **Manage** > **Settings** tab.

ⓘ **NOTE:** To ensure that OMIVV continues to display updated information, Dell recommends that you schedule a periodic inventory job. The inventory job consumes minimal resources and does not degrade host performance.

ⓘ **NOTE:** The chassis gets discovered automatically after the inventory for all hosts is run. If the chassis is added to a chassis profile, the chassis inventory automatically runs. In an SSO environment with multiple vCenter servers, the chassis inventory runs automatically with every vCenter when the inventory for any vCenter is run at a scheduled time.

ⓘ **NOTE:** The settings in this page are reset to default each time the configuration wizard is invoked. If you have previously configured a schedule for inventory, ensure that you replicate the previous schedule in this page before completing the wizard functions so that the previous schedule is not overridden by the default settings.

1. In the **Initial Configuration Wizard**, from the **Inventory Schedule** dialog box, select **Enable Inventory Data Retrieval**, if it is not enabled. By default, **Enable Inventory Data Retrieval** is enabled.
2. Under **Inventory Data Retrieval Schedule**, perform the following steps:
    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 **Data Retrieval Time**, 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.

    c. To apply the changes and continue, click **Next**.

    Once you click next, all details that you provide in this wizard is saved and you cannot modify the details from this wizard. You can modify inventory schedule details of the hosts from the **Manage** > **Settings** tab after completing the configuration from the configuration wizard. See **Modifying inventory job schedules** in the *OpenManage Integration for VMware vCenter User's Guide* at `Dell.com/support/manuals`.

Running warranty retrieval jobs

The warranty retrieval job configuration is available from the Settings tab in OMIVV. In addition, you can also run or schedule warranty retrieval job from **Job Queue** > **Warranty**. The scheduled jobs are listed in the job queue. In an SSO environment with multiple vCenter servers, the chassis warranty runs automatically with every vCenter when the warranty for any vCenter is run. However, warranty does not automatically run if it is not added to chassis profile.

ⓘ **NOTE:** The settings in this page are reset to default each time the configuration wizard is invoked. If you have previously configured a warranty retrieval job, ensure that you replicate that schedule warranty retrieval job in this page before completing the wizard functions so that the previous warranty retrieval is not overridden by the default settings.

1. In the **Warranty Schedule** dialog box, select **Enable Warranty Data Retrieval**.
2. In **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. 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**, and then proceed with the **Event and Alarm** settings.
    Once you click next, all details that you provide in this wizard is saved and you cannot modify the details from the wizard. You can modify warranty job schedules from the **Settings** tab after completing the configuration from the configuration wizard. See **Modifying warranty job schedules** in the *OpenManage Integration for VMware vCenter User's Guide* at `Dell.com/support/manuals`.

Configuring events and alarms

You can configure events and alarms by using the **Initial Configuration Wizard** or from the **Settings** tab for events and alarms. To receive events from the servers, OMIVV is configured as trap destination. For 12th generation hosts and later, ensure that the SNMP trap destination is set in iDRAC. For hosts earlier than 12th generation, ensure that the trap destination is set in OMSA.

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

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 event, which is the default event posting level
2. To enable all hardware alarms and events, select **Enable Alarms for Dell Hosts**.

   > **NOTE:** The Dell hosts that have alarms enabled respond to some specific critical events by entering in to maintenance mode and you can modify the alarm, when required.

   The **Enabling Dell Alarm Warning** dialog box is displayed.
3. To accept the change, click **Continue**, or to cancel the change, click **Cancel**.

   > **NOTE:** Ensure that you complete this step only if you select **Enable Alarms For Dell Hosts**.

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.

   > **NOTE:** After restoring the appliance, the events and alarms settings are not enabled even if the GUI shows as enabled. You can enable the **Events and Alarms** settings again from the **Settings** tab.

5. Click **Apply**.

Configuration tasks through settings tab

By using the settings tab, you can view and perform the following configuration tasks:

- Enable the OMSA link. See Enabling OMSA link.
- Configure warranty expiration notification settings. See the Configuring warranty expiration notification settings.
- Set up the firmware update repository. See Setting up the firmware update repository.
- Configure the latest appliance version notification. See Configuring the latest appliance version notification.
- Configure and view events and alarms. See the Configuring events and alarms.
- View data retrieval schedules for inventory and warranty. See the Viewing data retrieval schedules for inventory and warranty.

Appliance settings

In this section, configure the following for the OMIVV appliance:

- Warranty expiration notification
- Firmware update repository
- Latest appliance version notification
- Deployment credentials

Configuring warranty expiration notification settings

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings**, click **Warranty Expiration Notification**.
2. Expand **Warranty Expiration Notification** to view the following:
   - **Warranty Expiration Notification**—whether the setting is enabled or disabled
   - **Warning**—number of days for the first warning setting
   - **Critical**—number of days for the critical warning setting
3. To configure warranty expiration thresholds for warning about warranty expiration, click the ✎ icon at the right side of **Warranty Expiration Notification**.

4. In the **Warranty Expiration Notification** dialog box, do the following:
    a. If you want to enable this setting, select the **Enable warranty expiration notification for hosts**.
       Selecting the check box enables warranty expiration notification.
    b. Under **Minimum Days Threshold Alert**, do the following:
        i. In the **Warning** drop-down list, select the number of days before you want to be warned of the warranty expiration.
        ii. In the **Critical** drop-down list, select the number of days before you want to be warned of the warranty expiration.
5. Click **Apply**.

Setting up firmware update repository

You can set up the firmware update repository on the OMIVV **Settings** tab.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings** at the right side of **Firmware Update Repository**, click the ✏ icon.
2. In the **Firmware Update Repository** dialog box, select one of the following:
    - **Dell Online**—you can access the location that uses the firmware update repository of Dell (Ftp.dell.com). The OpenManage Integration for VMware vCenter downloads selected firmware updates from the Dell repository and updates the managed hosts.

      NOTE: Based on the network settings, enable proxy settings if network needs proxy.
    - **Shared Network Folder**—you can have a local repository of the firmware in a CIFS-based or NFS-based network share. This repository can either be a dump of Server Update Utility (SUU) that Dell releases periodically or a custom repository created using DRM. This network share should be accessible by OMIVV.

      NOTE: If you are using CIFS share, the repository passwords cannot exceed 31 characters.
3. If you select **Shared Network Folder**, enter the **Catalog File Location** by 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: If you are using CIFS share, OMIVV prompts you to enter the user name and password. The @, %, and , characters are not supported for use in shared network folder user names or passwords.
4. Click **Apply** after downloading is complete.

NOTE: It might take up to 20 minutes to read the catalog from the source and update the OMIVV database.

Configuring latest appliance version notification

To receive periodic notification about the availability of latest version (RPM, OVF, RPM/OVF) of OMIVV, perform the following steps to configure the latest version notification:

1. In the OpenManage Integration for VMware vCenter, on the **Manage → Settings tab**, under **Appliance Settings**, at the right side of **Latest Version Notification**, click the ✏ icon.
   By default, the latest version notification is disabled.
2. In the **Latest Version Notification and Retrieval Schedule** dialog box, perform the following actions:
    a. If you want to enable latest version notification, select the **Enable Latest Version notification** check box.
    b. Under **Latest Version Retrieval Schedule**, select the days of the week for this job.
    c. In **Latest Version Retrieval Time**, specify the required local time.
       The time you provide is your local time. Ensure that you calculate any time difference for running this task at a proper time on the OMIVV appliance.
3. To save the settings, click **Apply**, to reset the settings, click **Clear**, and to abort the operation, click **Cancel**.

Configuring deployment credentials

The deployment credentials allow you to set up credentials to communicate securely with a bare-metal system that is discovered using auto discovery until the OS deployment is complete. For secure communication with iDRAC, OMIVV uses deployment credentials from initial discovery until the end of the deployment process. Once the OS deployment process is successfully complete, OMIVV changes the iDRAC credentials as provided in the connection profile. If you change the deployment credentials, all newly discovered systems from that point onwards are provisioned with the new credentials. However, the credentials on servers that are discovered prior to the change of deployment credentials are not affected by this change.

NOTE: OMIVV acts as a provisioning server. The deployment credentials allow you to communicate with iDRAC that uses the OMIVV plug-in as a provisioning server in the auto discovery process.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings**, at the right side of **Deployment Credentials**, click the ✎ icon.
2. In **Credentials for Bare Metal Server Deployment**, under **Credentials**, enter the values for the following:
   - In the **User Name** text box, enter the user name.

     The user name should be 16 characters or less (only ASCII printable characters).
   - In the **Password** text box, enter the password.

     The password should be 20 characters or less (only ASCII printable characters).
   - In the **Verify Password** text box, enter the password again.

     Ensure that the passwords match.
3. To save the specified credentials, click **Apply**.

vCenter settings

In this section, configure the following vCenter settings:

- Enable the OMSA link. See Enabling the OMSA link.
- Configure events and alarms. See the Configuring events and alarms.
- Configure the data retrieval schedules for inventory and warranty. See the Viewing data retrieval schedules for inventory and warranty.

Enabling OMSA link

Install and configure an OMSA web server before enabling the OMSA link. See the *OpenManage Server Administrator Installation Guide* for the version of OMSA in use and for instructions on how to install and configure the OMSA web server.

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

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **vCenter Settings** and at the right side of the OMSA web server URL, click the ✎ icon.
2. In the **OMSA Web Server URL** dialog box, type the URL.

   Ensure that you include the complete URL, along with the HTTPS and port number 1311.

   https://<OMSA server IP or fqdn>:1311
3. To apply the OMSA URL to all vCenter servers, select **Apply these settings to all vCenters**.

   NOTE: If you do not select the check box, the OMSA URL is applied only to one vCenter.
4. To verify that the OMSA URL link that you provided works, navigate to the **Summary** tab of the host and check that the OMSA console link is live within the **Dell Host Information** section.

Configuring events and alarms

The Dell Management Center events and alarms dialog box enables or disables all hardware alarms. The current alert status is displayed on the vCenter alarms tab. A critical event indicates actual or imminent data loss or system malfunction. A warning event is not necessarily significant, but can indicate a possible future problem. The events and alarms can also be enabled by using the VMware Alarm Manager. The events are displayed on the vCenter tasks and events tab in the hosts and clusters view. To receive the events from the servers, OMIVV is configured as the SNMP trap destination. For 12th generation hosts and later, the SNMP trap destination is set in iDRAC. For hosts earlier than 12th generation, trap destination is set in OMSA. You can configure events and alarms using the OpenManage Integration for VMware vCenter from the **Management** > **Settings** tab. Under vCenter **Settings**, expand the **Events and Alarms** heading to display the vCenter alarms for Dell Hosts (Enabled or Disabled), and the event posting level.

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

> **NOTE:** To receive the Dell events, enable both alarms and events.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **vCenter settings**, expand **Events and Alarms**.
   The current **vCenter Alarms for Dell Hosts** (Enabled or Disabled) or all vCenter alarms, and **Event Posting Level** are displayed.
2. Click the ✏ icon at the right side of **Events and Alarms**.
3. To enable all hardware alarms and events, select **Enable Alarms for all Dell Hosts**.

   > **NOTE:** The Dell hosts that have alarms enabled respond to critical events by entering into maintenance mode and you can modify the alarm, as needed.

4. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**.
   This step can take up to a minute before the change takes effect and is available only if **Enable Alarms For Dell Hosts** is selected.
5. In **Event Posting Level**, select either “Do not post any events”, “Post All Events”, “Post only Critical and Warning Events”, or “Post only Virtualization-Related Critical and Warning Events”. For more information, see the **Events, alarms, and health monitoring** section in *OpenManage Integration for VMware vCenter User’s Guide*.
6. If you want to apply these settings to all vCenters, select **Apply these settings to all vCenters**.

   > **NOTE:** Selecting the option overrides the existing settings for all vCenters.

   > **NOTE:** The option is not available, if you have already selected **All Registered vCenters** from the drop-down list on the **Settings** tab.

7. To save, click **Apply**.

Viewing data retrieval schedules for inventory and warranty

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **vCenter Settings**, click **Data Retrieval Schedule**.
   On clicking, data retrieval schedule expands to expose the edit options for inventory and warranty.
2. Click the ✏ icon against **Inventory Retrieval** or **Warranty Retrieval**.
   In the **Inventory/Warranty Data Retrieval** dialog box, you can view the following information for inventory or warranty retrieval:
   - Whether the inventory and/or warranty retrieval option is enabled or disabled?
   - The weekdays for which it is enabled.
   - The time of day it is enabled.
3. To edit the data retrieval schedules, perform the following steps:
   a. Under **Inventory/Warranty Data**, select the **Enable Inventory/Warranty Data Retrieval** check box.
   b. Under **Inventory/Warranty Data Retrieval Schedule**, select the days of the week for your job.
   c. In the **Inventory/Warranty Data Retrieval Time** text box, type the local time for this job.

      You might need to consider the time difference between job configuration and job implementation.

   d. To save the settings, click **Apply**, to reset the settings, click **Clear**, and to abort the operation, click **Cancel**.
4. Click **Data Retrieval Schedule** again to contract the inventory and warranty schedules and display a single line.

Creating chassis profile

A chassis profile is required to monitor the chassis. A chassis credential profile can be created and associated with a single or multiple chassis.

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

1. In OpenManage Integration for VMware vCenter, click **Manage**.

2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand **Credential Profiles**, and click the **Chassis Profiles** tab.
4. In the **Chassis Profiles** page, click the ✚ icon to create a **New Chassis Profile**.
5. In the **Chassis Profile Wizard** page, do the following:

   In the **Name and Credentials** section, under **Chassis Profile**:

   a. In the **Profile Name** text box, enter the profile name.

   b. In the **Description** text box, enter description, which is optional.

   Under **the Credentials** section:

   a. In the **User Name** text box, type the user name with administrative rights, which is typically used to log in 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 the 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.

6. 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.

7. 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, then 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.

8. Click **OK**.

   The **Associated Chassis** page is displayed.

9. To test the chassis connectivity, select the chassis and click the **Test Connection** icon, which verifies the credentials, and the result is displayed in the **Test Result** column as **Pass** or **Fail**.
10. To complete the profile, click **Finish**.

3

Accessing documents from the Dell EMC support site

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

- Using the following links:
  - For Dell EMC Enterprise Systems Management, Dell EMC Remote Enterprise Systems Management, and Dell EMC Virtualization Solutions documents — https://www.dell.com/esmmanuals
  - For Dell EMC OpenManage documents — https://www.dell.com/openmanagemanuals
  - For iDRAC documents — https://www.dell.com/idracmanuals
  - For Dell EMC OpenManage Connections Enterprise Systems Management documents — https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Dell EMC Serviceability Tools documents — https://www.dell.com/serviceabilitytools
- From the Dell EMC Support site:
  1. Go to https://www.dell.com/support.
  2. Click **Browse all products**.
  3. From **All products** page, click **Software**, and then click the required link from the following:
     - **Analytics**
     - **Client Systems Management**
     - **Enterprise Applications**
     - **Enterprise Systems Management**
     - **Mainframe**
     - **Operating Systems**
     - **Public Sector Solutions**
     - **Serviceability Tools**
     - **Support**
     - **Utilities**
     - **Virtualization Solutions**
  4. To view a document, click the required product and then click the required version.
- Using search engines:
  - Type the name and version of the document in the search box.

4

Related Documentation

In addition to this guide, you can access the other guides available at `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 4.0** to access the following documents:

- *OpenManage Integration for VMware vCenter Version 4.0 Web Client User's Guide*
- *OpenManage Integration for VMware vCenter Version 4.0 Release Notes*
- *OpenManage Integration for VMware vCenter Version 4.0 Compatibility Matrix*

You can find the technical artifacts including white papers at **delltechcenter.com**. On the Dell TechCenter Wiki home page, click **Systems Management** > **OpenManage Integration for VMware vCenter** to access the articles.