

OpenManage Integration for VMware vCenter Version 5.0 Installation Guide

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.

| | |
|---|-----------|
| Chapter 1: Introduction..... | 5 |
| OpenManage Integration for VMware vCenter licensing..... | 5 |
| Buy software license..... | 5 |
| Options after uploading licenses..... | 6 |
| Enforcement..... | 6 |
| Important notes for reference..... | 7 |
| Hardware requirements..... | 7 |
| Configure deployment mode..... | 7 |
| BIOS and iDRAC with Lifecycle Controller versions | 8 |
| Supported features on PowerEdge servers..... | 10 |
| Supported features on PowerEdge chassis | 11 |
| Storage space required for provisioned storage..... | 12 |
| Software requirements..... | 12 |
| OpenManage Integration for VMware vCenter requirements..... | 12 |
| Port information..... | 13 |
| Prerequisite checklist..... | 15 |
| | |
| Chapter 2: Install and configure OMIVV..... | 16 |
| Download OpenManage Integration for VMware vCenter..... | 16 |
| Deploy OMIVV OVF using vSphere Client (HTML-5)..... | 17 |
| Configure OMIVV appliance..... | 18 |
| Set up Network Time Protocol servers..... | 20 |
| Configure OMIVV appliance with two network adapters..... | 21 |
| Generate a Certificate Signing Request (CSR)..... | 24 |
| Upload HTTPS certificate..... | 25 |
| Restore default HTTPS certificate | 25 |
| Register OpenManage Integration for VMware vCenter and import license file..... | 25 |
| Register vCenter server by non-administrator user..... | 27 |
| Required privileges for non-administrator users..... | 28 |
| Assign Dell privileges to existing role..... | 29 |
| Reconfigure OMIVV after upgrading registered vCenter version..... | 30 |
| Verify installation..... | 30 |
| Manage backup and restore..... | 30 |
| Configure backup and restore..... | 30 |
| Schedule automatic backups..... | 31 |
| Perform immediate backup..... | 31 |
| Restore OMIVV database from backup | 31 |
| Reset backup and restore settings..... | 32 |
| Update OMIVV appliance and repository location..... | 32 |
| Upgrade OMIVV appliance using RPM..... | 32 |
| Upgrade VMware tools..... | 33 |
| Upgrade OMIVV appliance using backup and restore..... | 33 |
| Unregister OpenManage Integration for VMware vCenter..... | 34 |
| Recover OMIVV after un-registration..... | 34 |

| | |
|---|-----------|
| Recover OMIVV after unregistering earlier version of OMIVV..... | 34 |
| Manage un-registration and re-registration..... | 35 |
| Chapter 3: Configure appliance for VMware vCenter..... | 36 |
| Configuration tasks using initial configuration wizard | 36 |
| Initial configuration..... | 36 |
| Create host credential profile..... | 37 |
| Schedule inventory job..... | 38 |
| Schedule warranty retrieval jobs..... | 39 |
| Configure events and alarms..... | 39 |
| Configuration tasks on the Settings page | 40 |
| Configure warranty expiration notification..... | 40 |
| Configure latest appliance version notification | 40 |
| Configure deployment credentials..... | 41 |
| Override severity of health update notification..... | 41 |
| Chapter 4: Accessing documents from the Dell EMC support site..... | 42 |
| Chapter 5: Related Documentation..... | 43 |

Introduction

This guide provides step-by-step instructions for installing and configuring OpenManage Integration for VMware vCenter (OMIVV) for use with PowerEdge servers. After the OMIVV installation, for more 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](#)
- [Important notes for reference](#)
- [Hardware requirements](#)
- [Software requirements](#)
- [Port information](#)
- [Prerequisite checklist](#)

OpenManage Integration for VMware vCenter licensing

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

- Evaluation license—when the OMIVV 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 90-day trial version is the default license that is supplied when shipped.
- Standard license—you can purchase any number of host licenses that are managed by OMIVV. This license includes product support and OMIVV Appliance updates.

The OMIVV supports up to 15 vCenters. When you upgrade from an evaluation license to a full standard license, you receive an email about the order confirmation, and you can download the license file from the Dell Digital Locker. Save the license .XML file to your local system and upload the new license file using the **Administration Console**.

Licensing presents the following information:

- Maximum vCenter Connection Licenses—up to 15 registered and in-use vCenter connections are enabled.
- 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 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.

NOTE: Any license purchased for the OpenManage Integration for VMware vCenter that is still current for its term (3 years or 5 years from purchase) is usable for the 5.x release. Backed up licensing from an existing OMIVV instance transfers over, or current licenses re-downloaded from the Digital Locker can be applied to 5.x instances.

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital Locker at [Dell Digital Locker](#). If you are unable to download your license keys, contact Dell Support by going to [Order Support](#) to locate the regional Dell Support phone number for your product.

Buy software license

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

1. Go to **Settings > Licensing > Buy License**, or **Dashboard > Buy License**, or **Admin Portal > vCenter Registration > Licensing > BUY NOW**.

2. Download and save the license file to a known location.
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.

Upload license to Administration Portal

You can use this option to upload OMIVV host license.

1. Go to <https://<ApplianceIP/hostname/>>.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **VCENTER REGISTRATION**.
The registered vCenter servers are displayed in the working pane.
4. Click **Upload License**.
5. In the **UPLOAD LICENSE** dialog box, click **Browse** to go to the license file, and then click **Upload**.
If the license file is modified or edited, the OMIVV appliance views it as corrupted and the license file does not work.

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 Locker at [Dell Digital Locker](#). 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

The 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. By default, OMIVV supports up to 15 vCenters. If you want to manage more than 15 vCenters, use multiple appliances.

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 nonexpired 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, some of the functionality may not work. 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 accordingly.

Add hosts to a host credential profile

When you attempt to add a host to a host credential profile, if the number of licensed hosts exceeds beyond the number of licenses, adding extra hosts is prevented. OMIVV does not support managing the number of hosts more than number of host license is available.

Important notes for reference

- From OMIVV 5.0 onwards, only VMware vSphere Client (HTML-5) is supported and the vSphere Web Client (FLEX) is not supported.
- To use the DNS server, the recommended practices are:
 - OMIVV supports only IPv4 IP addresses. Although both static IP assignment and DHCP assignment are supported, Dell EMC recommends that you assign a static IP address. Assign a static IP address and hostname 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 hostname 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 requirements for vSphere 6.5 and Platform Services Controller appliance](#)
- [DNS requirements for vSphere 6.7 and Platform Services Controller on Windows](#)
- For the OMIVV appliance mode, ensure that you deploy OMIVV in the appropriate mode based on your virtualization environment. For more information, see [Configure deployment mode](#) on page 7.
- Configure your network to match the port requirements. For more information, see [Port information](#) on page 13.
- Dell EMC recommends using Google Chrome to access the OMIVV features. OMIVV supports Google Chrome and Mozilla Firefox. Microsoft Internet Explorer is not supported.

Hardware requirements

OMIVV provides full support for several generations of the Dell EMC servers with full feature support for servers with iDRAC Express or Enterprise. To verify that your host servers are eligible, see information about the following in the subsequent subsections:

- [Supported server and minimum BIOS](#)
- [iDRAC supported versions \(both deployment and management\)](#)
- [Supported memory, CPU, and storage space for OMIVV](#)

OMIVV requires LAN on motherboard or Network daughter card that can access the management network of both iDRAC and CMC or OME-Modular systems management network and the vCenter management network. For more information, see [Configure OMIVV appliance](#) on page 18 and [Configure OMIVV appliance with two network adapters](#) on page 21.

Configure deployment mode

For any of the mentioned deployment modes, ensure that you reserve sufficient memory resources to the OMIVV appliance using reservations. See vSphere documentation for steps about reserving memory resources.

Ensure that the following system requirements for the required deployment modes are fulfilled by assigning these resources to the VM containing OMIVV:

Table 1. System requirements for deployment modes

| Deployment modes | Number of hosts | Number of CPUs | Memory (GB) | Minimum Storage |
|------------------|-----------------|----------------|-------------|-----------------|
| Small | Up to 250 | 2 | 8 | 95 GB |

Table 1. System requirements for deployment modes

| Deployment modes | Number of hosts | Number of CPUs | Memory (GB) | Minimum Storage |
|------------------|-----------------|----------------|-------------|-----------------|
| Medium | Up to 500 | 4 | 16 | 95 GB |
| Large | Up to 1,000 | 8 | 32 | 95 GB |
| X Large mode | Up to 2,000 | 12 | 32 | 95 GB |

NOTE: MX chassis firmware update feature is supported only on medium, large, and extra large deployment modes.

You can select an appropriate deployment mode to scale OMIVV to match the number of nodes in your environment.

1. On the **APPLIANCE MANAGEMENT** page, scroll down to **Deployment Mode**.
The configuration values of the deployment mode such as **Small, Medium, Large,** and **X Large** are displayed. By default, the mode is set to **Small**.
2. To edit a deployment mode based on an environment, click **Edit**.
3. In the **Edit** mode, ensure that the prerequisites are fulfilled and select the required deployment mode.
4. Click **Apply**.
The allocated CPU and memory are verified against the required CPU and memory for the set deployment mode, and one of more of the following events occur:
 - If the verification fails, an error message is displayed.
 - If the verification is successful, the OMIVV appliance restarts and the deployment mode is changed after you confirm the change.
 - If the required deployment mode is already set, a message is displayed.
5. If the deployment mode is changed, confirm the changes, and then the appliance is restarted to enable the deployment mode to be updated.

NOTE: During the OMIVV appliance bootup, the allocated system resources are verified against the set deployment mode. If the allocated system resources are less than the set deployment mode, the OMIVV appliance does not boot to the login page. To boot the OMIVV appliance, Close the OMIVV appliance, update the system resources to the existing set deployment mode, and complete the [downgrade deployment mode](#) task.

Downgrade deployment mode

1. Log in to the Administration Console.
2. Change the deployment mode to the required level.
3. Shut down the OMIVV appliance and change the system resources to the required level.
4. Turn on the OMIVV appliance.

BIOS and iDRAC with Lifecycle Controller versions

The BIOS and iDRAC with Lifecycle Controller versions that are required to enable the features of OpenManage Integration for VMware vCenter.

Dell EMC recommends you to use the Bootable ISO created by using Repository Manager, or Lifecycle Controller's Platform to update your servers to one of the following base versions before using OMIVV:

Table 2. Supported BIOS version for PowerEdge servers

| Server | Minimum version |
|--------|-----------------|
| T320 | 1.0.1 or later |
| T420 | 1.0.1 or later |
| T620 | 1.2.6 or later |
| M420 | 1.2.4 or later |
| M520 | 1.2.6 or later |
| M620 | 1.2.6 or later |

Table 2. Supported BIOS version for PowerEdge servers

| Server | Minimum version |
|---------------|------------------------|
| M820 | 1.2.6 or later |
| R220 | 1.0.3 or later |
| R320 | 1.2.4 or later |
| R420 | 1.2.4 or later |
| R520 | 1.2.4 or later |
| R620 | 1.2.6 or later |
| R720 | 1.2.6 or later |
| R720xd | 1.2.6 or later |
| R820 | 1.7.2 or later |
| R920 | 1.1.0 or later |
| R630 | 1.0.4 or later |
| R730 | 1.0.4 or later |
| R730xd | 1.0.4 or later |
| R430 | 1.0.4 or later |
| R530 | 1.0.2 or later |
| R830 | 1.0.2 or later |
| R930 | 1.0.2 or later |
| R230 | 1.0.2 or later |
| R330 | 1.0.2 or later |
| T630 | 1.0.2 or later |
| T130 | 1.0.2 or later |
| T330 | 1.0.2 or later |
| T430 | 1.0.2 or later |
| M630 | 1.0.0 or later |
| M830 | 1.0.0 or later |
| FC430 | 1.0.0 or later |
| FC630 | 1.0.0 or later |
| FC830 | 1.0.0 or later |
| R240 | 1.0.0 or later |
| R340 | 1.0.0 or later |
| R940 | 1.0.0 or later |
| R940xa | 1.0.0 or later |
| R740 | 1.0.0 or later |
| R740xd | 1.0.0 or later |
| R740xd2 | 1.0.0 or later |
| R640 | 1.0.0 or later |
| R840 | 1.0.0 or later |

Table 2. Supported BIOS version for PowerEdge servers

| Server | Minimum version |
|--------|-----------------|
| R440 | 1.0.0 or later |
| M640 | 1.0.0 or later |
| T140 | 1.0.0 or later |
| T340 | 1.0.0 or later |
| T640 | 1.0.0 or later |
| T440 | 1.0.0 or later |
| R540 | 1.0.0 or later |
| FC640 | 1.0.0 or later |
| R6415 | 1.0.0 or later |
| R7425 | 1.0.0 or later |
| R7415 | 1.0.0 or later |
| MX740C | 1.0.0 or later |
| MX840C | 1.0.0 or later |
| R6515 | 1.0.3 or later |
| R7515 | 1.0.3 or later |
| R6525 | 1.0.0 or later |

Table 3. Supported iDRAC and Lifecycle Controller for deployment

| Generation | iDRAC with Lifecycle Controller |
|-----------------------------------|---------------------------------|
| PowerEdge 12th generation servers | 2.50.50.50 or later |
| PowerEdge 13th generation servers | 2.50.50.50 or later |
| PowerEdge 14th generation servers | 3.00.00.00 and later |

Table 4. BIOS and iDRAC requirements for cloud server

| Model | BIOS | iDRAC with Lifecycle Controller |
|-------|----------------|---------------------------------|
| C6320 | 1.0.2 | 2.50.50.50 or later |
| C4130 | 1.0.2 | 2.50.50.50 or later |
| C6420 | 1.0.0 or later | 3.00.00.00 or later |
| C4140 | 1.0.0 or later | 3.00.00.00 or later |
| C6525 | 1.0.0 or later | 3.42.42.42 or later |

Supported features on PowerEdge servers

The following features are supported on the hosts that are managed by OpenManage Integration for VMware vCenter:

Table 5. Supported features on PowerEdge servers

| Features | Platform | |
|--------------------|--------------------|--------------------|
| | 12G and 13G | 14G |
| Hardware Inventory | Y | Y |
| Events and Alarms | Y (SNMP v1 and v2) | Y (SNMP v1 and v2) |

Table 5. Supported features on PowerEdge servers

| Features | Platform | |
|--|----------|----|
| Component wise Health Monitoring* | Y | Y |
| BIOS/Firmware Updates# | Y | Y |
| Proactive HA\$ | Y | Y |
| Warranty Information | Y | Y |
| Management Compliance | Y | Y |
| Configuration Compliance | Y | Y |
| Auto/Manual discovery of bare-metal server | Y | Y |
| Bare-Metal compliance | Y | Y |
| Hardware Configuration | Y | Y |
| OS Deployment | Y | Y |
| Blink Server LED | Y | Y |
| View/Clear SEL logs | Y | Y |
| Link and Launch iDRAC | Y | Y |
| iDRAC reset | Y | Y |
| System Lockdown Mode | N | Y |
| System Profile | Y | Y |
| Cluster Profile | Y | Y |
| Host management using unified chassis IP | N | Y@ |
| Support for OEM server | Y~ | Y |

* In Cloud with model number C6320, health monitoring is not supported for the mezzanine cards.

In Cloud with model number C6320, firmware updates are not supported for the mezzanine cards.

\$ Proactive HA feature is only applicable on vCenter 6.5 or later that has ESXi 6.0 or later. Also, Proactive HA feature is not supported on servers with embedded PSU and cloud server models.

@ Applicable only for an MX chassis host. Inventory, monitoring, Proactive HA, and firmware update features are supported.

~ Supported only for Rack servers.

Supported features on PowerEdge chassis

This topic provides information about the supported features on the PowerEdge chassis.

Table 6. Supported features on modular infrastructure

| Features | M1000e | VRTX | FX2s | MX |
|--|--------|------|------|----|
| SNMP Alerts | Y | Y | Y | Y |
| Hardware Inventory | Y | Y | Y | Y |
| Link and Launch CMC or Management Module | Y | Y | Y | Y |
| License Information | N/A | Y | Y | Y |
| Warranty Information | Y | Y | Y | Y |

Table 6. Supported features on modular infrastructure

| Features | M1000e | VRTX | FX2s | MX |
|---|--------|------|------|----|
| Health Reporting | Y | Y | Y | Y |
| Multi-chassis management group relationship information | N | N | N | Y |
| Firmware Update | N | N | N | Y |

Storage space required for provisioned storage

The OMIVV virtual appliance requires at least 95 GB of disk space for provisioned storage.

Default virtual appliance configuration

The OMIVV virtual appliance is provisioned with 8 GB of RAM and two virtual CPU (Small Deployment Mode).

Software requirements

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

Requirements for VMware vSphere Client (HTML-5)

vCenter 6.5 and later

OpenManage Integration for VMware vCenter requirements

Supported ESXi versions on managed hosts

The following table provides information about the supported ESXi versions on managed hosts:

Table 7. Supported ESXi versions

| ESXi Version | Server Generation | | |
|--------------|-------------------|------|------|
| | YX2X | YX3X | YX4X |
| 6.0 U3 | Y | Y | N |
| 6.5 | Y | Y | N |
| 6.5 U1 | Y | Y | Y |
| 6.5 U2 | Y | Y | Y |
| 6.5 U3 | Y | Y | Y |
| 6.7 | N | Y | Y |
| 6.7 U1 | N | Y | Y |
| 6.7 U2 | N | Y | Y |
| 6.7 U3 | N | Y | Y |

 **NOTE:** The PowerEdge MX host is supported only when used with ESXi 6.5 U2 and later.

The OpenManage Integration for VMware vCenter supports any of the following vCenter server versions:

Table 8. Supported vCenter server versions

| vCenter version | Client support |
|-----------------|----------------|
| 6.5 U2 | Y |
| 6.5 U3 | Y |
| 6.7 | Y |
| 6.7 U1 | Y |
| 6.7 U2 | Y |
| 6.7 U3 | Y |

The OpenManage Integration for VMware vCenter version 5.0 supports VMware vRealize Operations Manager (vROPS) version 2.0.

The OMIVV 5.0 appliance supports CentOS 7.6.1810.

Port information

This section lists all the port requirements to configure your virtual appliance and managed nodes.

Table 9. Virtual appliance (continued)

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|-------------|------------|-----------|--------------------------|-----------|----------------------------------|-------------------------|---|
| 53 | DNS | TCP | None | Out | OMIVV appliance to DNS server | DNS client | Connectivity to the DNS server or resolving the host names. |
| 80/443 | HTTP/HTTPS | TCP | None | Out | OMIVV appliance to Internet | Dell Online Data Access | Connectivity to the online (Internet) warranty, firmware, and latest RPM information. |
| 80 | HTTP | TCP | None | In | ESXi server to OMIVV appliance | HTTP server | Used in operating system deployment flow for post installation scripts to communicate with the OMIVV appliance. |
| 162 | SNMP Agent | UDP | None | In | iDRAC/ESXi to OMIVV appliance | SNMP Agent (server) | To receive SNMP traps from managed nodes. |
| 443 | HTTPS | TCP | 128-bit | In | OMIVV UI to OMIVV appliance | HTTPS server | Web services offered by OMIVV. These Web services are consumed by vSphere Client and Dell Admin portal. |
| 443 | WSMAN | TCP | 128-bit | In/Out | OMIVV appliance to or from iDRAC | iDRAC communication | iDRAC and CMC or OME-Modular communication, used to manage and monitor the managed nodes. |
| 445 | SMB | TCP | 128-bit | Out | OMIVV appliance to CIFS | CIFS communication | To communicate with Windows share. |
| 4433 | HTTPS | TCP | 128-bit | In | iDRAC to OMIVV appliance | Auto Discovery | Provisioning server that is used for auto discovering managed nodes. |
| 2049 | NFS | UDP/TCP | None | In/Out | OMIVV appliance to NFS | Public Share | NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update |

Table 9. Virtual appliance

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|--------------|------------|-----------|--------------------------|-----------|---------------------------------|---------------------|---|
| | | | | | | | and operating system deployment flows. |
| 4001 to 4004 | NFS | UDP /TCP | None | In/Out | OMIVV appliance to NFS | Public Share | These ports must be kept open to run the statd, quotd, lockd, and mountd services by the V2 and V3 protocols of the NFS server. |
| 11620 | SNMP Agent | UDP | None | In | iDRAC to OMIVV appliance | SNMP Agent (server) | Port used to receive the standard SNMP alerts by using UDP: 162. Data from iDRAC and CMC or OME-Modular are received to manage and monitor the managed nodes. |
| User-defined | Any | UDP /TCP | None | Out | OMIVV appliance to proxy server | Proxy | To communicate with the proxy server. |

Table 10. Managed nodes (ESXi)

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|-------------|-----------|-----------|--------------------------|-----------|-------------------------|---------------------|---|
| 162, 11620 | SNMP | UDP | None | Out | ESXi to OMIVV appliance | Hardware Events | Asynchronous SNMP traps that are sent from ESXi. This port have to open from ESXi. |
| 443 | WSMAN | TCP | 128-bit | In | OMIVV appliance to ESXi | iDRAC communication | Used to provide information to the management station. This port has to open from ESXi. |
| 443 | HTTPS | TCP | 128-bit | In | OMIVV appliance to ESXi | HTTPS server | Used to provide information to the management station. This port has to open from ESXi. |

Table 11. Managed nodes (iDRAC or CMC or OME-Modular)

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|-------------|---------------------------|-----------|--------------------------|-----------|--|---------------------|---|
| 443 | WSMAN/ HTTPS, REST/ HTTPS | TCP | 128-bit | In | OMIVV appliance to iDRAC or CMC or OME-Modular | iDRAC communication | Used to provide information to the management station and communicate to MX chassis by using REST or HTTPS protocols. This port has to open from iDRAC and CMC or OME-Modular. |
| 4433 | HTTPS | TCP | 128-bit | Out | iDRAC to OMIVV appliance | Auto Discovery | For auto discovering iDRAC (managed nodes) in the management station. |
| 2049 | NFS | UDP | None | In/Out | iDRAC to/ from OMIVV | Public Share | For iDRAC to access NFS public share that is exposed by OMIVV appliance. That is used for operating system deployment and firmware update. To access the iDRAC configurations from the OMIVV. Used in deployment flow. |

Table 11. Managed nodes (iDRAC or CMC or OME-Modular)

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|--------------|-----------|-----------|--------------------------|-----------|---------------------|-----------------------|--|
| 4001 to 4004 | NFS | UDP | None | In/Out | iDRAC to/from OMIVV | Public Share | For iDRAC to access NFS public share that is exposed by OMIVV appliance. This is used for operating system deployment and firmware update. To access the iDRAC configurations from the OMIVV. Used in deployment flow. |
| 69 | TFTP | UDP | 128-bit | In/Out | iDRAC to/from OMIVV | Trivial File Transfer | Used for managing the iDRAC successfully from the management station. |

Prerequisite checklist

Before you start the product installation, ensure that:

- You have user name and password for OMIVV to access the vCenter server. The user may have an administrator role that has all necessary permissions or a non-administrator user with the necessary privileges. For more information about the list of privileges that are required for OMIVV to operate, see [Required privileges for non-administrator users](#).
 - You have the root password for the ESXi host systems, or the Active Directory credentials that have administrative rights on the host.
 - You have the user name and password that is associated with iDRAC Express or Enterprise which has administrative rights on the iDRAC.
 - The vCenter server is running.
 - You determine the location of the OMIVV installation directory.
 - The OMIVV and vCenter server are on the same network.
 - There is a route between the vCenter, OMIVV, and the iDRAC networks, if vCenter, OMIVV, and iDRAC are connected to different networks. This is applicable only if the OMIVV appliance is not configured with two network adapters.
 - The VMware vSphere environment meets virtual appliance system requirements, port access, clock synchronization, and listening port requirements.
- i NOTE:** The virtual appliance functions as a regular virtual machine; any interruptions or shut downs impact overall functionality of the virtual appliance.
- i 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.

Install and configure OMIVV

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

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

1. Download the *DellEMC_OpenManage_Integration_<version number>.<build number>.zip* file from the Dell support website at Dell.com/support. For more information about downloading OMIVV, see [Download OpenManage Integration for VMware vCenter](#) on page 16.
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 Client (HTML-5). See [Deploying the OMIVV OVF](#).
4. After you deploy an OVF, set the time zone, current date, and time.
5. Upload the license file. For more information about licensing, see [Upload license to Administration Portal](#) on page 6.
6. Set the deployment mode as per the requirement. For more information, see [Configure deployment mode](#) on page 7.
7. Register the OMIVV appliance with the vCenter server by using Administration Console. See [Registering OMIVV and importing the license file](#).
8. To configure the appliance, complete the **Initial Configuration Wizard**. See [Configuration tasks through the configuration wizard](#).

Topics:

- [Download OpenManage Integration for VMware vCenter](#)
- [Deploy OMIVV OVF using vSphere Client \(HTML-5\)](#)
- [Configure OMIVV appliance](#)
- [Set up Network Time Protocol servers](#)
- [Configure OMIVV appliance with two network adapters](#)
- [Generate a Certificate Signing Request \(CSR\)](#)
- [Upload HTTPS certificate](#)
- [Register OpenManage Integration for VMware vCenter and import license file](#)
- [Register vCenter server by non-administrator user](#)
- [Reconfigure OMIVV after upgrading registered vCenter version](#)
- [Verify installation](#)
- [Manage backup and restore](#)
- [Update OMIVV appliance and repository location](#)
- [Upgrade OMIVV appliance using RPM](#)
- [Upgrade OMIVV appliance using backup and restore](#)
- [Unregister OpenManage Integration for VMware vCenter](#)
- [Recover OMIVV after un-registration](#)

Download OpenManage Integration for VMware vCenter

Do keep the Service Tag of your Dell EMC PowerEdge server handy. It is recommended that you use the Service Tag to access all support on the Dell Support Website. This ensures that you download the appropriate version of the software for your platform.

To download OMIVV:

1. Go to <https://www.dell.com/support>.
2. Perform one of the following actions:
 - Enter the Service Tag of your Dell EMC PowerEdge server, and then select search.
 - Select **Browse all products > Servers > PowerEdge**.

3. Select the appropriate model of your PowerEdge server.
4. On the support page of your server, select **Drivers & downloads**.
5. From the **Operating System** list, select the appropriate version of VMware ESXi.
6. From the **Category** list, select **Systems Management**.
The supported version of OMIVV is displayed.
7. Click **Download** or select the check box to add the software to your download list.

Deploy OMIVV OVF using vSphere Client (HTML-5)

Ensure that you have downloaded and unzipped the product .zip file, *DellEMC_OpenManage_Integration_<version number>.<build number>.zip* from the support website.

NOTE: The following tasks are recommended only if you are using vSphere Client (HTML-5). If you are using Web Client, the steps may vary.

1. Go to the location where you have downloaded OMIVV and double-click **DellEMC_OpenManage_Integration.exe** to unzip the file.
The supported client operating system version for extracting and running the exe is Windows 7 SP1 and later.
The supported server operating system 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 Client (HTML-5)**.
5. In **VMware vSphere 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 an OVF template** window, perform the following:
 - a. To download the OVF package from the Internet, select **URL**.
 - b. Select **Local file** and click **Choose Files** if you want to select the OVF package from your local system.
 - c. Click **Next**.
The **Select a Name and Folder** window is displayed.

NOTE: If the OVF package is saved on a network share, the installation process can take between 10—30 minutes. For a quick installation, Dell EMC recommends that you host the OVF on a local drive.

7. In the **Select Name and Folder** window, perform the following:
 - a. In the **Virtual machine name** field, enter the name of the template. The name can include up to 80 characters.
 - b. From the **Select a location for the Virtual Machine** list, select a location for deploying the template.
 - c. Click **Next**.
The **Select a compute resource** window is displayed.
8. From the **Select a compute resource** list, select the destination compute resource, and click **Next**.
The **Review Details** window is displayed with the following information:
 - **Publisher**—The publisher data
 - **Download Size**—The actual size of the OVF template in GBs
 - **Size on Disk**—The information about thick and thin provisioned

9. Click **Next**.
The **Select Storage** window is displayed.

10. In the **Select Storage** window, perform the following:
 - a. From the **Select Virtual Disk Format** drop-down list, select either of the following formats:
 - **Thick Provision (lazy Zeroed)**
 - **Thick Provision (Eager zeroed)**
 - **Thin Provision**

It is recommended that you select Thick Provision (Eager Zeroed).

- b. From the **VM Storage Policy** drop-down list, select a policy.
- c. Click **Next**.

The **Select Networks** window displays information about the source and destination networks.

11. In the **Select Networks** window, select destination network for each source network and click **Next**.

To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and Dell EMC OpenManage Enterprise Modular (OME-Modular)).

If vSphere network and out-of-band network are maintained as separate isolated network in your environment, OMIVV requires access for both the networks. In this case, OMIVV appliance must be configured with two network adapters. If you can access out-of-band network using the vSphere network, then, do not configure a network adapter for the OMIVV appliance. For more information about configuring two network adapters, see [Configure OMIVV appliance with two network adapters](#) on page 21.

- Out-of-band network—The management network to which an iDRAC, CMC, and OME-Modular are connected to.
- vSphere network—The management network to which ESXi hosts, vCenters, and PSCs are connected to.

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

13. Power on the VM.

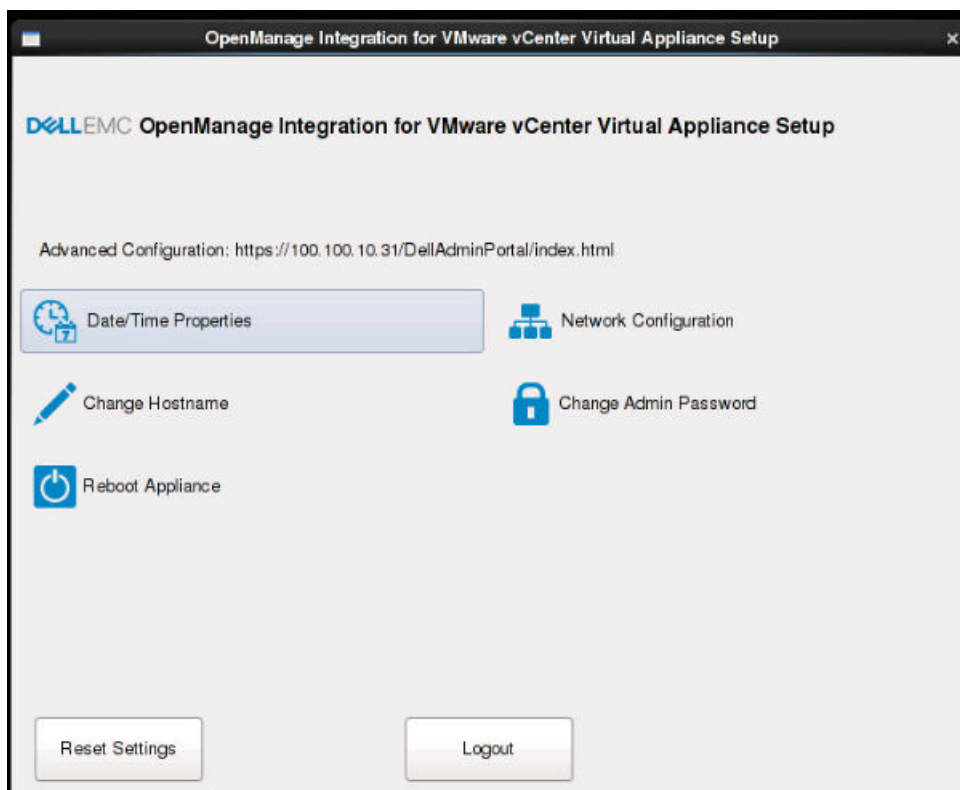
NOTE: After you deploy an OVF, you must mandatorily set the current date and time before registering to OMIVV.

Configure OMIVV appliance

1. Power on the VM.
2. In the right-pane, click **Launch Web Console**.
3. Log in as an administrator (the default user name is `admin`).
4. If you are logging in for the first time, follow the instructions on the screen to set the password (Admin and ReadOnly users).

NOTE: If you forget the administrator password, it cannot be recovered from the OpenManage Integration for VMware vCenter appliance.

5. To configure the OMIVV time zone information, click **Date/Time Properties**.



NOTE: When the OMIVV appliance is not able to retrieve an IP address from the network (DHCP), 0.0.0.0 is displayed as the IP address. To resolve this, you must manually configure the static IP.

- a. On the **Date and Time** tab, select the **Synchronize date and time over the network** check box. The **Synchronize date and time over the network** check box is enabled only after NTP is configured successfully using the Admin portal. For more information about configuring NTP, see [Set up Network Time Protocol servers](#) on page 20.
 - b. Click **Time Zone** and select the applicable time zone, and then click **OK**.
6. To configure network of the OMIVV appliance, click **Network Configuration**.

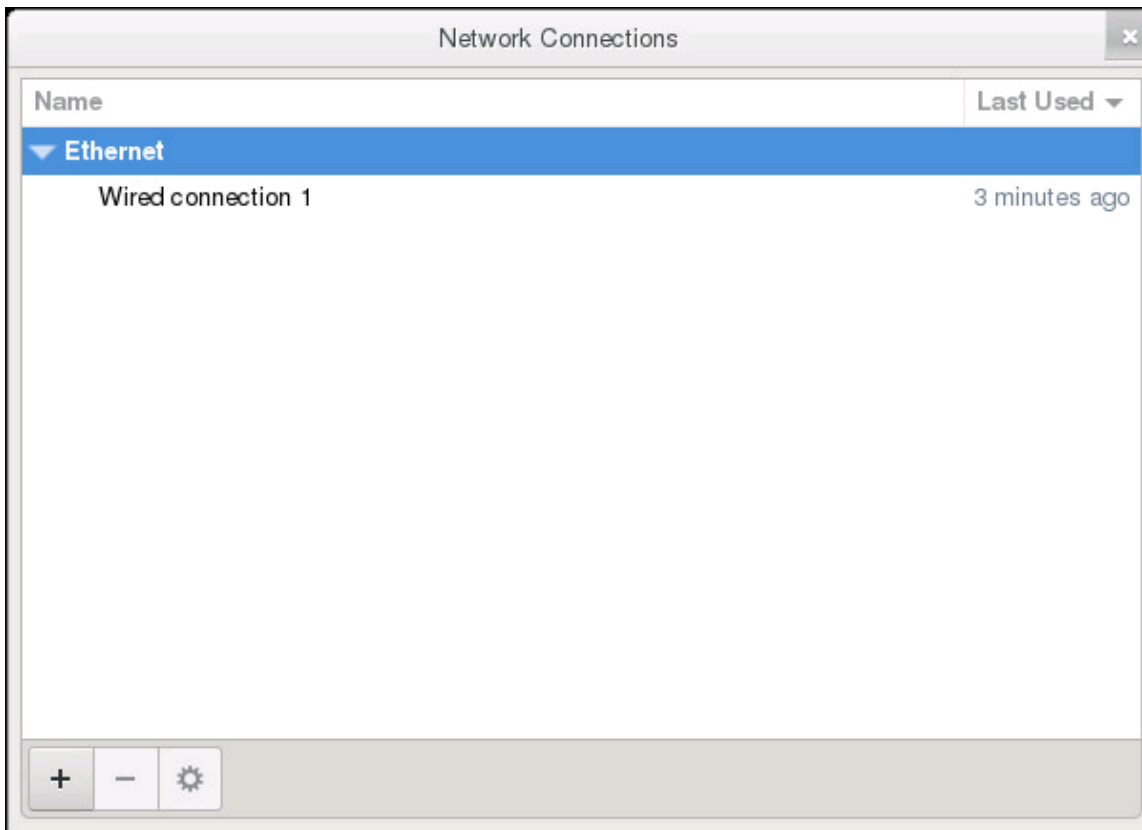
To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and OME-Modular).

If vSphere network and out-of-band network are maintained as separate isolated network in your environment, OMIVV requires access for both the networks. In this case, OMIVV appliance must be configured with two network adapters. Dell EMC recommends configuring both the networks as part of the initial configuration.

If you can access the out-of-band network using the vSphere network, do not configure two network adapters for the OMIVV appliance. For more information about configuring a second NIC, see [Configure OMIVV appliance with two network adapters](#) on page 21.



7. Select **Wired Connection 1** and click



- a. Click the **IPv4 Settings** tab, select **Manual** from the **Method** drop-down list, and click **Add**.
NOTE: If you select Automatic (DHCP), do not enter any IP address because the OMIVV appliance will automatically receive IP from the DHCP server during the next restart.
- b. Enter a valid IP, netmask (in the Classless Inter-Domain Routing (CIDR) format), and gateway information. If you enter an IP address in the **Netmask** box, it is automatically converted to its respective CIDR format.
- c. Enter the DNS server IP and domains to be searched for respectively in the **DNS Servers** and **Search Domains** boxes respectively.
- d. Select the **Require IPv4 addressing for this connection to complete** check box and click **Save**.

Editing Wired connection 1

Connection name:

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method:

Addresses

| Address | Netmask | Gateway |
|---------------|---------|-------------|
| 100.100.9.102 | 22 | 100.100.8.1 |

DNS servers:

Search domains:

DHCP client ID:

Require IPv4 addressing for this connection to complete

NOTE:

Sometimes, after you configure the OMIVV appliance with a static IP, the OMIVV terminal utility page does not immediately refresh and display the updated IP. To resolve this issue, exit the OMIVV terminal utility, and then log in again.

8. To change the hostname of the OMIVV appliance, click **Change Hostname**.
 - a. Enter a valid hostname, and click **Update hostname**.

NOTE: If any vCenter servers are already registered with the OMIVV appliance, unregister and re-register all the vCenter instances. For more information, see [Manage un-registration and re-registration](#) on page 35.

9. Restart the appliance.

Set up Network Time Protocol servers

You can use Network Time Protocol (NTP) to synchronize the OMIVV appliance clocks to that of an NTP server.

1. On the **APPLIANCE MANAGEMENT** page, click **Edit** in the **NTP Settings** area.
2. Select **Enabled**. Enter the hostname or IP address of a preferred and secondary NTP server and click **Apply**.
3. After configuring NTP, start the terminal console and select the **Synchronize date and time over the network** check box.

NOTE: It might take around 10 minutes for the OMIVV clocks to synchronize with the NTP server.

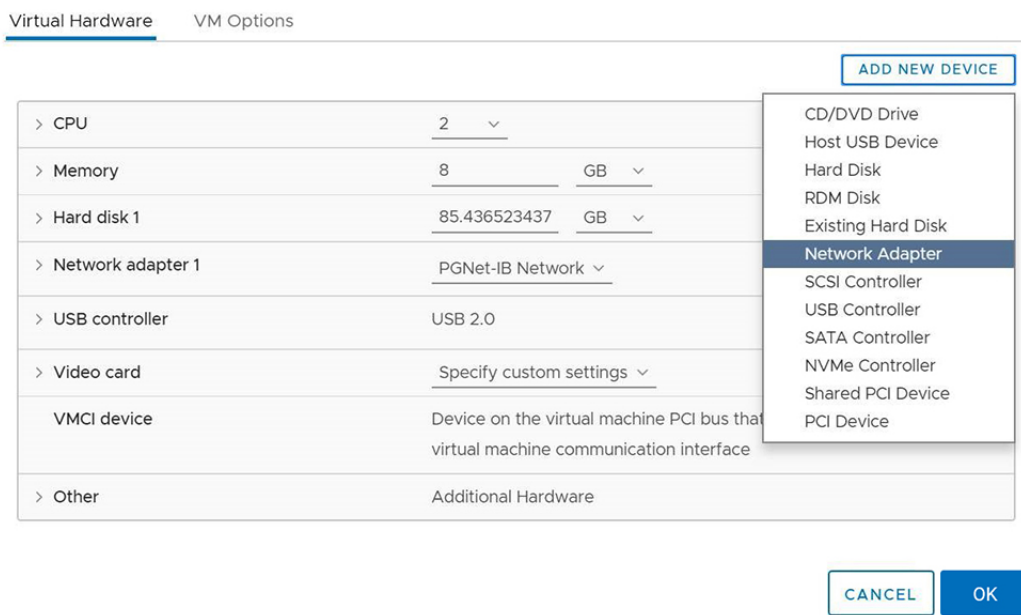
Configure OMIVV appliance with two network adapters

To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and OME-Modular). If vSphere network and out-of-band network are maintained as separate isolated network in your environment, OMIVV requires access for both the networks. In this case, OMIVV appliance must be configured with two network adapters. If the out-of-band network can be accessed using the vSphere network then, do not configure two network adapters for the OMIVV appliance.

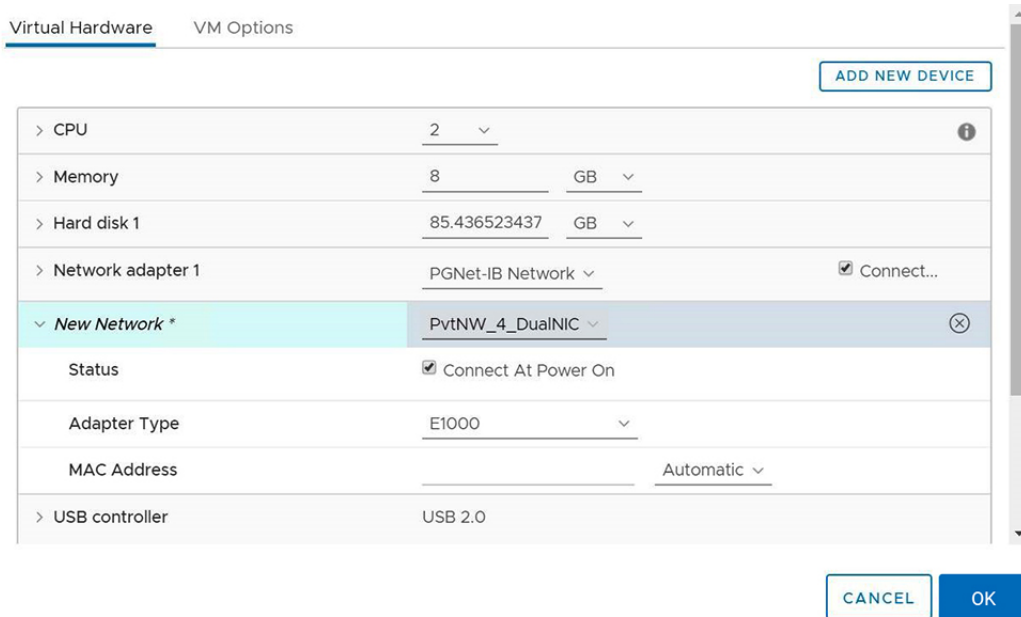
Ensure that you have the following information ready for both the out-of-band network and vSphere network:

- IP address, netmask (in the CIDR format), and gateway of the appliance (if static)
- Default gateway—It is mandatory to configure the default gateway to only one network that has an Internet connection. It is recommended to use vSphere network as the default gateway.
- Routing requirements (Network IP, Netmask, and gateway)—For other external networks that cannot be reached to either through directly or using default gateway, configure the static routes.
- DNS requirements—The OMIVV supports DNS configuration for only one network. For more information about DNS configuration, go to step 9 (b) in this topic.

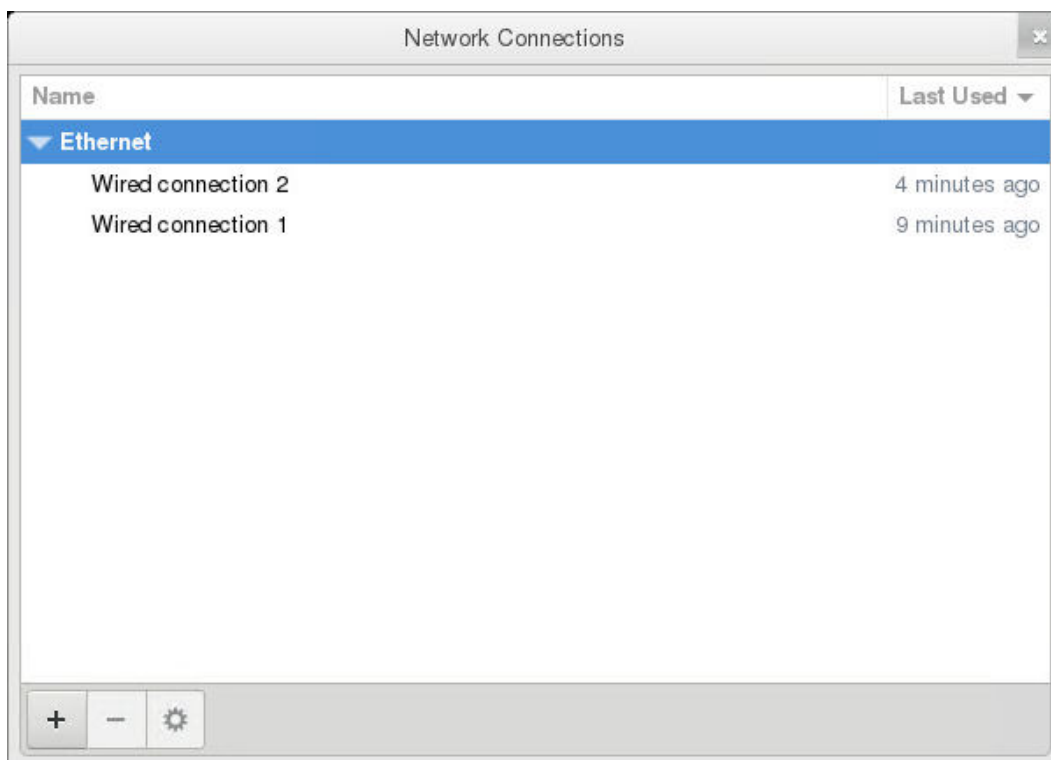
1. Shut down the OMIVV appliance.
2. Edit the VM settings using the vSphere Client (HTML-5) and add the additional Network adapter. To edit the VM settings, right-click VM, and then click **Edit Settings**.
3. Click **ADD NEW DEVICE**, select **Network Adapter**.



- a. Select the appropriate network for the network adapter, and then select the **Connect At Power On** check box.
- b. Select the **E1000** adapter type from the drop-down menu. OMIVV supports only E1000 type of network adapter.




4. Power on the VM. Log in as an administrator (the default user name is Admin), and then press **Enter**.
5. On the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, select **Network Configuration**. The **Network Connections** page displays two NICs.

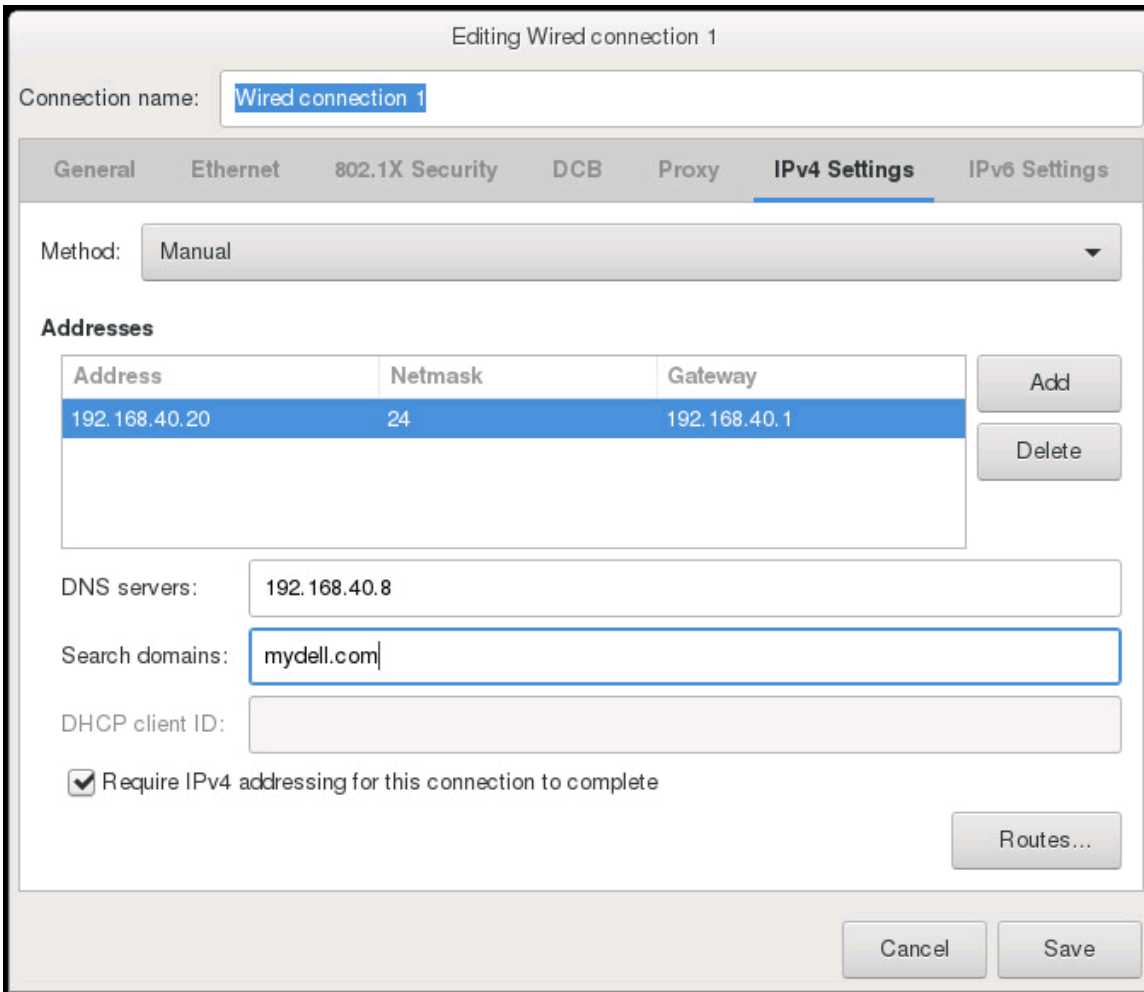


WARNING: Do not use "+" to add any new network interface. It is mandatory to use the vSphere Edit Settings to add a network adapter.

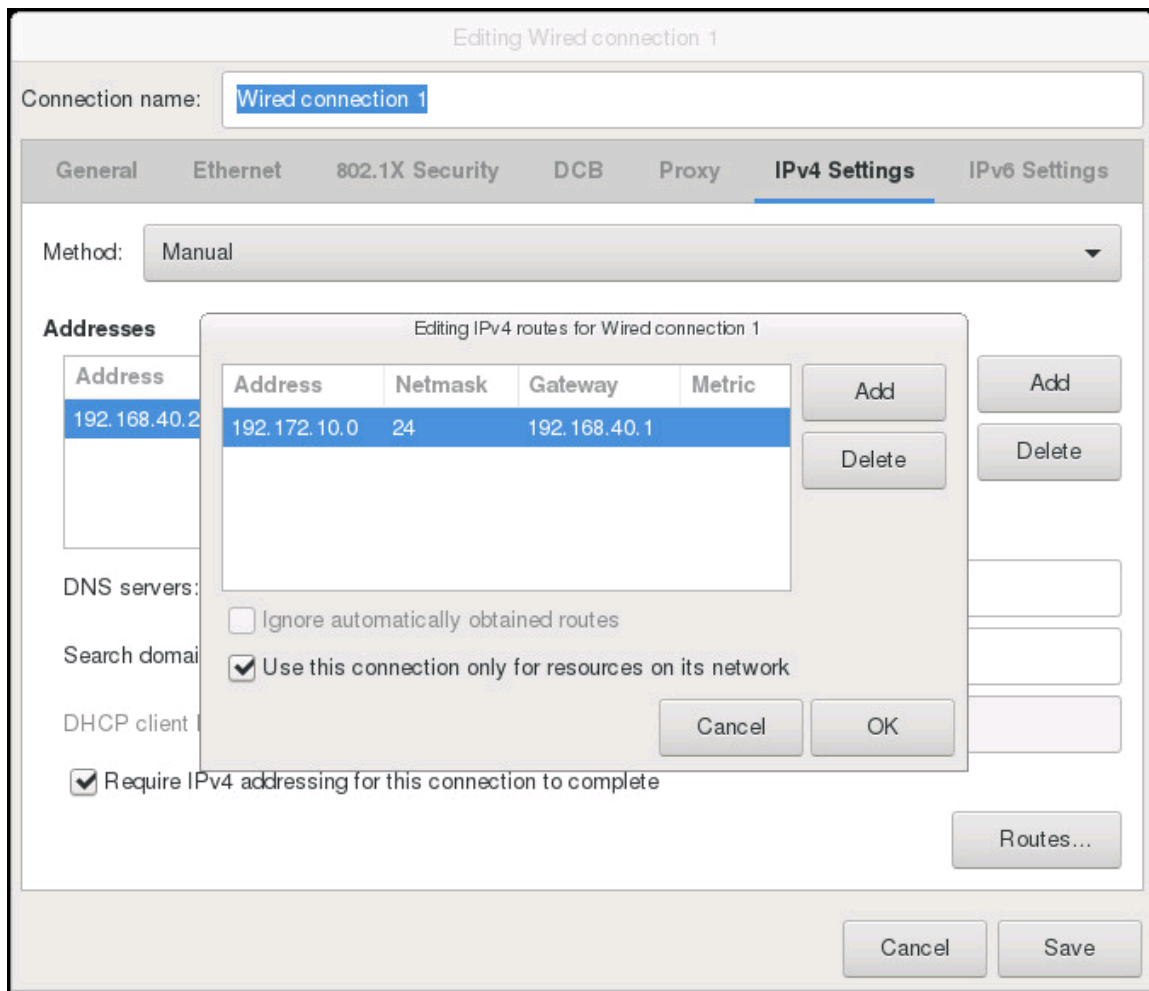


6. Select the NIC that you want to configure and click .
7. To identify the correct NIC, use the MAC ID displayed on the **Ethernet** tab, and then compare it against the MAC ID displayed in the vSphere Client (HTML-5).
Ensure that you do not change the default MAC address that is listed in the **Ethernet** tab.
8. Click the **General** tab and select the **Automatically connect to this network when it is available** check box.

9. Click the **IPv4 Settings** tab and do the following:



- a. Select **Manual** or **Automatic (DHCP)** from the **Method** drop-down list.
- b. If you select the **Manual** method, click **Add**, and then enter the valid IP address, Netmask (in the CIDR format), and gateway details. It is recommended to use the static IP in case if you want to control over the priority of the DNS servers (primary and secondary DNS entries).
Typically, vSphere elements of data center such as vCenter and ESXi hosts are managed using hostname or FQDN. iDRAC, CMC, and OME-Modular are managed using IP addresses. In this case, Dell EMC recommends you to configure the DNS settings only for the vSphere network.
If both vSphere network and iDRAC management network are managed by using hostname or FQDN, DNS server must be configured in such a manner that it resolves the hostname or FQDN for both the networks. For more information, see the CentOS documentation.
NOTE: The last configured DNS server becomes the primary DNS irrespective of which network the DNS is configured for.
- c. Enter the DNS server IP and domains to be searched for in the **DNS Servers** and **Search Domains** boxes respectively.
- d. Select the **Require IPv4 addressing for this connection to complete** check box and click **SAVE**.
- e. If you do not want to use this network as the default network (gateway), click **Routes**, and then select the **Use this connection only for resources on its network** check box.
NOTE: Adding multiple networks as default gateways may result in network issues and OMIVV functions may get affected.
- f. If you want to reach to any external network using the known gateways, click **Add** on the same page, and then add the network IP address, netmask (in the CIDR format), and gateway details.



Typically, the network that you have configured as the default gateway does not require any manual route configuration because the gateway is capable of providing the reachability. However, for networks where default gateway is not configured (the **Use this connection only for resources on its network** check box is selected), a manual route configuration may be required. Because the default gateway is not configured for this network to reach external networks, manual routing configurations are required.

NOTE: Incorrect routing configuration may abruptly stop the network interface from responding. Ensure to configure the routing entries appropriately.

- g. Click **OK**.
10. Click **Save**. To configure another NIC, repeat the tasks 6–10.
11. Go to the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Reboot Appliance**. The network configuration is complete only after restarting the OMIVV appliance.

NOTE:

After the appliance is successfully restarted, the NICs start working as configured. The status of NICs can be viewed by logging in as **readonly** user and running the following commands: `ifconfig`, `ping`, and `route -n`.

Generate a Certificate Signing Request (CSR)

Before registering an OMIVV to a vCenter, ensure that you upload the CSR.

Generating a new CSR prevents certificates that were created with the previously generated CSR from being uploaded to the appliance. To generate a CSR, do the following:

1. On the **APPLIANCE MANAGEMENT** page, click **Generate Certificate Signing Request** in the **HTTPS CERTIFICATES** area.

A message is displayed stating that if a new request is generated, certificates created using the previous CSR can no longer be uploaded to the appliance. To continue with the request, click **Continue**.

2. If you continue with the request, in the **GENERATE CERTIFICATE SIGNING REQUEST** dialog box, enter information about the common name, organization, locality, state, country, and email address. Click **Continue**.
3. Click **Download**, and then save the resulting CSR to an accessible location.

Upload HTTPS certificate

Ensure that the certificate uses the PEM format.

You can use the HTTPS certificates for secure communication between OMIVV appliance and host systems. To set up this type of secure communication, send the CSR certificate to a signing authority, and then upload the resulting CSR using the admin console. There is also a default certificate that is self-signed and can be used for secure communication—this certificate is unique to every installation.

1. On the **APPLIANCE MANAGEMENT** page, click **Upload Certificate** in the **HTTPS CERTIFICATES** area.
2. Click **OK** in the **UPLOAD CERTIFICATE** dialog box.
3. To upload the certificate, click **Browse**, and then click **Upload**.

NOTE: If you want to upload a customized CSR to OMIVV, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed on the vSphere Client (HTML-5). To fix this issue, unregister, and re-register the appliance with the vCenter. For more information, see [Manage un-registration and re-registration](#) on page 35 .

After upload HTTPS certificate task is complete, close the browser session and access admin portal in a new browser session.

Restore default HTTPS certificate

1. On the **APPLIANCE MANAGEMENT** page, click **Restore Default Certificate** in the **HTTPS CERTIFICATES** area.
2. In the **RESTORE DEFAULT CERTIFICATE** dialog box, click **Apply**.

After restore default HTTPS certificate task is complete, close the browser session and access admin portal in a new browser session.

Register OpenManage Integration for VMware vCenter and import license file

Ensure that your licenses are ready for download at [Dell Digital Locker](#). 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 vSphere Client (HTML-5). To fix this issue, unregister, and re-register the appliance with vCenter. For more information, see [Manage un-registration and re-registration](#) on page 35.

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

To open **Administration Console**, start a web browser and enter `https://<ApplianceIP or Appliance hostname or FQDN>`.

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.

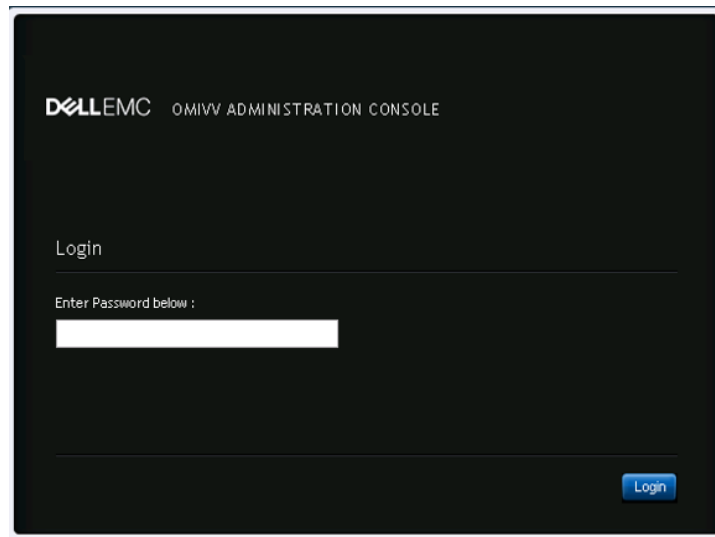


Figure 1. Administration Console

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

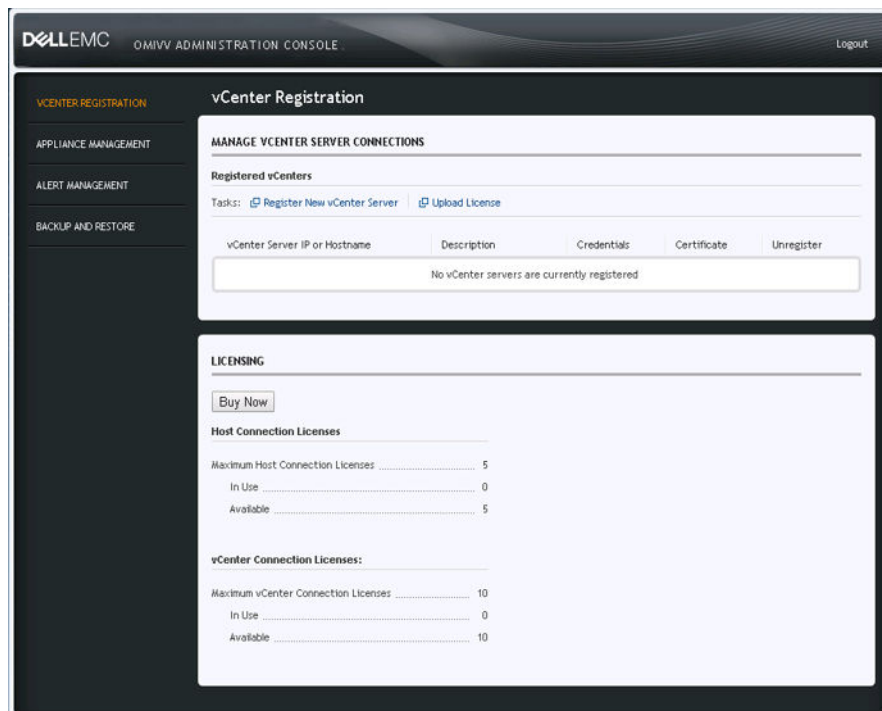


Figure 2. vCenter registration window from Administration Console

3. In the **vCenter Registration** window, click **Register a New vCenter Server**.
4. 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 FQDN, and then in the **Description** text box, enter a description. The description is optional.

NOTE: It is recommended that register 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. For more information, see [Register vCenter server by non-administrator user](#) on page 27.

- c. In **Password**, enter the password.
 - d. In **Verify Password**, enter the password again.
5. Click **Register**.

NOTE: OpenManage Integration for VMware vCenter currently supports up to 2000 hosts for extra large deployment mode with a single vCenter instance or multiple vCenter servers by using the linked mode.

6. 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 Locker at [Dell Digital Locker](#), and you can import this license to your virtual appliance. To import the license file, click **Upload License**.

7. In the **Upload License** window, click **Browse** to go 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 Locker. If you are unable to download your license keys, contact Dell Support by going to [Contact Technical Support](#) to locate the regional Dell Support phone number for your product.

After OMIVV is registered, the OMIVV icon is displayed on the vSphere Client (HTML-5) home page.

To verify the installation, see [Verify installation](#) on page 30.

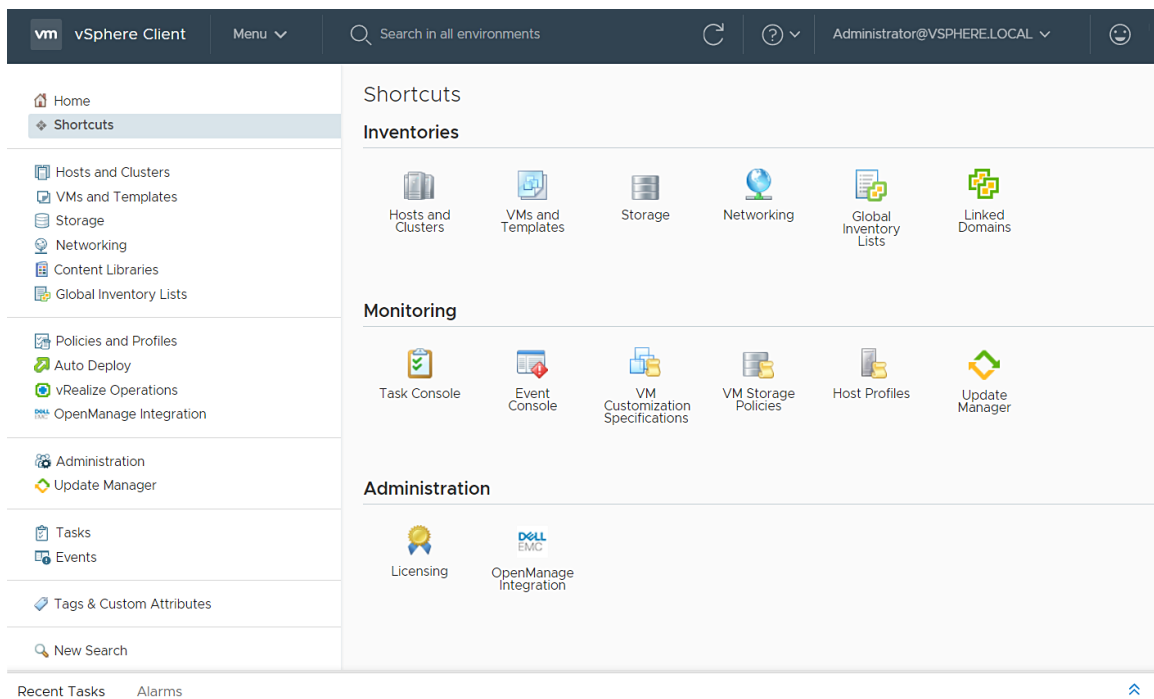


Figure 3. OpenManage Integration for VMware vCenter successfully added to vCenter

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.

Register vCenter server by non-administrator user

To perform the following tasks, ensure that you have vCenter Administrator privileges.

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

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



1. Create a role or modify existing role with a required privileges for the role.
For more information about the list of privileges required for the role, see [Required privileges for non-administrator users](#).
For the steps required to create or modify a role and select privileges in the vSphere Client (HTML-5), see the VMware vSphere documentation
2. Assign a user to the newly created role after you define a role and select privileges for the role.
For more information about assigning a role to privilege, see the VMware vSphere documentation.
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 using a non-administrator user with the required privileges.
4. After registration is complete, assign the Dell privileges to the role created or modified in step 1. See [Assign Dell privileges to existing role](#) on page 29.

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

Required privileges for non-administrator users

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

While registering a vCenter server with OMIVV by a non-administrator user, a 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
 - Change settings
 - Connection
 - Maintenance
 - Network configuration
 - Query patch
 - Security profile and firewall
-  **NOTE:** If you are using vCenter 6.5 or upgrading to vCenter 6.5 or later, ensure that you assign the modify cluster privilege.
 - Host.Config

- Advanced settings
 - Connection
 - Maintenance
 - Network configuration
 - Query patch
 - Security profile and firewall
- o Inventory
 - Add host to cluster
 - Add standalone host
 - Modify cluster
- i** **NOTE:** If you are using vCenter 6.5 or upgrading to vCenter 6.5 or later, ensure that you assign the modify cluster privilege,
- Host profile
 - o Edit
 - o View
 - Permissions
 - o Modify permission
 - o Modify role
 - Sessions
 - o Validate session
 - Task
 - o Create task
 - o Update task
- i** **NOTE:** If a vCenter server is registered using non-administrator user to access any OMIVV features, non-administrator user must have Dell privileges. For more information about assigning Dell privileges, see [Assign Dell privileges to existing role](#) on page 29.

Assign Dell privileges to existing role

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

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

1. Log in to the vSphere Client (HTML-5) with administrative rights.
2. In vSphere Client (HTML-5), expand **Menu**, click **Administration** → **Roles**.
3. From the **Roles provider** drop-down list, select a vCenter server.
4. From the **Roles** list, select **Dell-Operational**, and then click **PRIVILEGES**.
5. To assign the Dell privileges, click the edit icon []. The **Edit Role** page is displayed.
6. In the left pane, click **Dell**, and then select the following Dell privileges for the selected role, and then click **NEXT**:
 - Dell.Configuration
 - Dell.Deploy-Provisioning
 - Dell.Inventory
 - Dell.Monitoring
 - Dell.Reporting

For more information about the available OMIVV roles within vCenter, see the Security roles and permissions topic in the User's Guide.

7. Edit the role name and enter description for the selected role, if required.
8. Click **FINISH**.
Log out and log in from the vCenter. The user with necessary privileges can now perform the OMIVV operations.

Reconfigure OMIVV after upgrading registered vCenter version

After upgrading a registered vCenter, perform the following tasks:

- For non-administrator users:
 1. Assign extra privileges to non-administrator users, if necessary. See [Required privileges for non-administrator users](#) on page 28.
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.

Verify installation

The following steps verify that the OMIVV installation is successful:

1. Close any vSphere client windows, and start a new vSphere Client (HTML-5).
2. Ensure that vCenter can communicate with OMIVV by attempting a PING command from the vCenter server to the virtual appliance IP address or hostname.
3. In vSphere Client, expand **Menu**, click **Administration > Solutions > Client Plug-ins**.
For more information about the access restrictions for **Plug-In Management** or **Client Plug-Ins** page, see VMware documentation.
4. On the **Client Plug-Ins** page, verify the version, and ensure that OMIVV is installed and enabled.
If OMIVV is not enabled, wait for sometime and then log out and log in from vCenter.
5. To confirm that the OMIVV icon appears inside vSphere client (HTML-5), in vSphere Client, expand **Menu**.
The OpenManage Integration icon is displayed.

Manage backup and restore

By using the Administrator Console, you can perform backup and restore related tasks.


- [Configure backup and restore](#)
- [Schedule automatic backups](#)
- [Perform an immediate backup](#)
- [Restore the database from backup](#)
- [Reset backup and restore settings](#) on page 32

In OpenManage Integration for VMware vCenter, perform the following steps to access the **BACKUP AND RESTORE SETTINGS** page through the Administration Console:

1. Go to `https://<ApplianceIP|hostname>`.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **BACKUP AND RESTORE**.

Configure backup and restore

The backup and restore function backs up the OMIVV database to a remote location (NFS and CIFS) from which it can be restored later. The profiles, configuration, and host information are in the backup. Dell EMC recommends you to schedule automatic backups to guard against data loss.

 **NOTE:** The NTP settings are not saved and restored.

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Edit**.
2. On the highlighted **SETTINGS AND DETAILS** area, do the following:
 - a. In **Backup Location**, type the path of the backup files.

- b. In **Username**, enter the user name.
 - c. In **Password**, enter the password. The % sign is not supported at the end of the password.
 - d. In **Enter the password used to encrypt backups**, type the encrypted password in the box.
The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, \$, %, and *”.
 - e. In **Verify Password**, retype the encrypted password.
3. To save these settings, click **Apply**.
 4. Configure the backup schedule. See [Scheduling automatic backups](#).

After this procedure, configure a backup schedule.

Schedule automatic backups

For more information about configuring the backup location and credentials, see [Configuring backup and restore](#).

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Edit Automatic Scheduled Backup**.
The relevant fields are enabled.
2. To enable the backups, click **Enabled**.
3. Select the **Days for Backup** check boxes for the days of the week on which you want to run the backup jobs.
4. In **Time for Backup (24 Hour, HH: mm)**, enter the time in the HH: mm format.
The **Next Backup** is populated with the date and time of the next scheduled backup.
5. Click **Apply**.

Perform immediate backup

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Backup Now**.
2. To use location and encryption password from the backup settings, in the **BACKUP NOW** dialog box, select the **Use location and encryption password from the Backup settings** check box.
3. Enter values for **Backup Location**, **Username**, **Password**, and **Password for Encryption**.
The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, \$, %, and *”. There is no character limitation for forming a password.
4. Click **Backup**.

Restore OMIVV database from backup

After restoring OMIVV from a previous version:

- 11G bare-metal servers are not supported. Only the 12G and later generations servers are retained after restore.
 - Hardware Profiles and Deployment Templates are not supported. Dell EMC recommends using System Profile for deployment.
 - Deployment tasks that are scheduled on 11G servers and/or using Hardware Profile based Deployment Templates are canceled.
 - All 11G servers are removed from Credential Profiles and consumed licenses are relinquished.
 - Repository Profiles will use only 64-bit bundles.
- NOTE:** If you perform backup and restore from 4.x to 5.x, a warning symbol is displayed against the cluster profile name because OMIVV does not support 32-bit firmware bundle in 5.x. To use the latest changes for the cluster profile, edit the cluster profile.
- Firmware Update jobs that are scheduled on 11G servers are canceled.

The restore operation causes the OMIVV appliance to reboot after restoration is complete.

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Restore Now**.
2. In the **RESTORE NOW** dialog box, enter the path for **File Location** along with the backup .gz file in the CIFS or NFS format.
3. Enter the **Username**, **Password**, and **Encryption Password** for the backup file.
The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, \$, %, and *”.
4. To save your changes, click **Apply**.
The appliance is restarted. To verify the installation, see [Verify installation](#) on page 30.

After restore is complete, close the browser and clear the browser cache before logging in to the admin portal.


Reset backup and restore settings

Using reset settings feature, you can reset settings to the unconfigured state.

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Reset Settings**.
2. In the **Reset Settings** dialog box, click **Apply**.
The appliance is restarted.

Update OMIVV appliance and repository location

- To ensure that all data is protected, perform a backup of the OMIVV database before updating the OMIVV appliance. See [Manage backup and restore](#) on page 30.
 - The OMIVV appliance requires Internet connection to display the available upgrade mechanisms and perform the RPM upgrade. Ensure that the OMIVV appliance has Internet connection. If you require a proxy network, based on the environment network settings, enable the proxy settings, and enter the proxy data. See the Setting up the HTTP proxy topic in User's Guide.
 - Ensure that the **Update Repository Path** is valid.
 - Ensure that you log out from all vSphere Client (HTML-5) sessions to the registered vCenter servers.
 - Before logging into to any of the registered vCenter servers, ensure that you update all appliances simultaneously under the same Platform Service Controller (PSC) before logging in to any of the registered vCenter servers. Else, you may see inconsistent information across OMIVV instances.
1. In the **APPLIANCE UPDATE** section of the **APPLIANCE MANAGEMENT** page, verify the current and available OMIVV version.

For the available OMIVV appliance version, the applicable RPM and OVF OMIVV appliance upgrade mechanisms are displayed with a tick mark [].


The following are the possible upgrade mechanism options available for you to perform either of the tasks for the upgrade mechanism:

| Option | Description |
|--------|--|
| 1 | If a tick mark is displayed against RPM, you can do an RPM upgrade from the existing version to the latest available version. See Upgrade OMIVV appliance using RPM on page 32. |
| 2 | If a tick mark is displayed against OVF, you can take a backup of the OMIVV database from the existing version, and restore it in the latest available appliance version. See Upgrade OMIVV appliance using backup and restore on page 33. |
| 3 | If a tick mark is displayed against both RPM and OVF, you can perform either of the mentioned options to upgrade your appliance. In this scenario, the recommended option is RPM upgrade. |

2. To update the OMIVV appliance, perform the mentioned tasks for the upgrade mechanisms as applicable from the version of OMIVV.

Upgrade OMIVV appliance using RPM

Ensure that you are upgrading to a version of the appliance that is greater than the current one.

1. On the **APPLIANCE MANAGEMENT** page, based on your network settings, enable proxy and enter proxy setting data, if necessary. See .
For the available OMIVV appliance version, the applicable RPM and OVF OMIVV appliance upgrade mechanisms are displayed with a tick mark [].
2. To upgrade the OMIVV plug-in from an existing version to the available version, perform one of the following steps:
 - To upgrade using RPM that is available in **Update Repository Path**, ensure that **Update Repository Path** is set to the path: <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>

If the path is different, in the **Appliance Management** window, in the **APPLIANCE UPDATE** area, click **Edit** to update the path to <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/> in the **Update Repository Path** text box, and click **Apply**.

3. Compare the available OMIVV appliance version and current OMIVV appliance version.
4. To apply the update to the OMIVV appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
5. In the **UPDATE APPLIANCE** dialog box, click **Update**.
After you click **Update**, you are logged out from the **ADMINISTRATION CONSOLE** window.
6. Close the web browser.
Once the appliance is RPM upgraded, ensure that you clear the browser cache before logging in to the Dell admin portal.

NOTE: During the upgrade process, the appliance restarts once or twice.

NOTE: After the RPM upgrade is complete, you can view the login screen in the OMIVV console. Open a browser, enter the `https://<ApplianceIP>/hostname` link, and go to the **APPLIANCE UPDATE** area. You can verify that the available and current OMIVV appliance versions are same. If you have enabled Proactive HA on clusters, OMIVV unregisters the Dell Inc provider for those clusters and re-registers the Dell Inc provider after upgrade. Health updates for the Dell EMC hosts are not available until upgrade is complete.

Upgrade VMware tools

1. Right-click the OMIVV appliance.
2. Hover over **Guest OS**, and then click **Install/Upgrade VMware Tools**.
3. In the **Install/Upgrade VMware Tools** dialog box, click **Automatic Tools Upgrade**, and then click **OK**.
You can view the installation status in the **Recent Tasks** section.

Upgrade OMIVV appliance using backup and restore

Dell EMC recommends not to change or remove cluster or host that is managed by OMIVV after taking backup and before restoring the backup file. If the cluster or host that is managed by OMIVV is changed or removed, reconfigure profiles (for example, Host credential profile, cluster profile) associated with those clusters and hosts after restore.

Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes Dell health update provider for Proactive HA clusters that are registered on vCenter by the OMIVV plugin.

To update the OMIVV appliance from an older version to current version, perform the following steps:

1. Back up the data of earlier releases.
2. Turn off the older OMIVV appliance from vCenter.
3. Deploy the new OpenManage Integration appliance OVF.
4. Power on the OpenManage Integration new appliance.
5. Set up the network and time zone for the new appliance.

NOTE: Dell EMC recommends retaining the identity (IP or FQDN) of the earlier OMIVV appliance for the new OMIVV appliance.

NOTE: If the IP address for the new appliance is different from the IP address of the older appliance the Proactive HA feature may not work properly. In such a scenario, disable and enable the Proactive HA for each cluster where Dell EMC host is present.

6. The OMIVV appliance comes with default certificate. If you want to have a custom certificate for your appliance, update the same. See [Generate a Certificate Signing Request \(CSR\)](#) on page 24 and [Upload HTTPS certificate](#) on page 25. Else, skip this step.
7. Restore the database to the new OMIVV appliance. See [Restoring the OMIVV database from a backup](#).
8. Verify the appliance. For more information, see [Verify installation](#) on page 30.
9. After the upgrade, Dell EMC recommends running the inventory again on all the hosts that the OMIVV plugin manages.
The events and alarms settings are not enabled after restoring the appliance. You can enable the Events and Alarms settings again from the **Settings** tab.

If you upgrade from an earlier version of OMIVV to the available version, all the scheduled job continues to run.

NOTE: If the identity (IP or FQDN) of the new OMIVV version Y is changed from the OMIVV version X, configure the trap destination for the SNMP traps to point to the new appliance. For 12G and later servers, the identity change is fixed by running the inventory on these hosts. While running the inventory on 12G hosts, if SNMP traps do not point to the new IP, those hosts are listed as noncomplaint. To fix host compliance issues, see Management compliance section in User's Guide.

After backing up and restoring from an earlier version of OMIVV to an updated version, if you observe that the 200000 message is displayed, or the Dell EMC logo is not displayed, or the OMIVV UI is not responding on the vCenter UI, do the following:

- Restart vSphere Client services for both vSphere Client (HTML-5) and vSphere Web Client (FLEX) on the vCenter server.
- If the issue persists:
 - For VMware vCenter Server Appliance: Go to `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`. For Windows vCenter, go to the following folders in the vCenter appliance and check if the old data corresponding to the earlier version exists—`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance.

An example old data is `com.dell.plugin.OpenManage—com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`.
 - Manually delete the folder corresponding to the earlier OMIVV version and restart vSphere Client services for both vSphere Client (HTML-5) and Web Client (FLEX).

Unregister OpenManage Integration for VMware vCenter

Ensure that you do not unregister OMIVV from the vCenter server when an inventory, warranty, or deployment job is running.

If you have enabled Proactive HA on clusters, ensure that Proactive HA is disabled on the clusters. For disabling Proactive HA, access the **Proactive HA Failures and Responses** screen of a cluster by selecting **Configure > Services > vSphere Availability**, and then click **Edit**. To disable Proactive HA, in the **Proactive HA Failures and Responses** screen, clear the check box against **Dell Inc** provider.

To remove OpenManage Integration for VMware vCenter, unregister OMIVV from the vCenter server by using the Administration Console.

1. Go to `https://<ApplianceIP/hostname/>`.

2. On the **VCENTER REGISTRATION** page, in the **vCenter Server IP or Hostname** table, click **Unregister**.

NOTE: Ensure to select the correct vCenter because OMIVV can be associated with more than one vCenter.

3. To confirm the unregistration of the selected vCenter server, in the **UNREGISTER VCENTER** dialog box, click **Unregister**.

NOTE: After unregistering OMIVV, log out and log in from the vSphere Client (HTML-5). If the OMIVV icon is still visible, then restart the Client services for both vSphere Client (HTML-5) and Web Client (FLEX).

Recover OMIVV after un-registration

Recover 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 plugin removes all the customization that was implemented on the registered alarms and Dell health update provider for PHA cluster. The following steps do not restore the customization. However, it re-registers the alarms in their default state.

NOTE: Dell EMC recommends retaining the identity (IP or FQDN) of the earlier OMIVV appliance for the new OMIVV appliance.

NOTE: If the IP address for the new appliance is different from the IP address of the older appliance the Proactive HA feature may not work properly. In such a scenario, disable and enable the PHA for each clusters where Dell host is present.

Perform the tasks from 3–9 listed in [Upgrade OMIVV appliance using backup and restore](#) on page 33.

Manage un-registration and re-registration

Dell EMC recommends you to take backup before performing un-registration.

NOTE: Unregistering the plugin removes all the customization that was implemented on the registered alarms and Dell health update provider for PHA cluster. The following steps do not restore the customization. However, it re-registers the alarms in their default state.

1. Take a backup of OMIVV.
2. Unregister vCenter from OMIVV.
3. Perform any planned configuration change. For example, hostname change, new configuration change.
4. Restart the OMIVV appliance.
5. Restore the backup file. For more information, see [Upgrade OMIVV appliance using backup and restore](#) on page 33.

Configure appliance for VMware vCenter

You can configure the OMIVV appliance by using any one of the following methods:

- Using the **Initial Configuration Wizard**.

After you complete the basic installation of OMIVV and registration of the vCenters, the Initial Configuration Wizard is displayed automatically for the first time, when you launch OMIVV in vCenter.

If you want to launch the initial configuration wizard later, go to:

- **Settings > Initial Configuration Wizard > START INITIAL CONFIGURATION WIZARD**
- **Dashboard > Quick References > START INITIAL CONFIGURATION WIZARD**

- Using the **Settings** tab.

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

Topics:

- [Configuration tasks using initial configuration wizard](#)
- [Configuration tasks on the Settings page](#)

Configuration tasks using initial 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 vSphere Client (HTML-5) and then log in again.

Using the initial configuration wizard, you can view and perform the following tasks:

- Select vCenters
- Create host credential profile. For more information, see [Create host credential profile](#) on page 37.
- Configure events and alarms. For more information, see [Configure events and alarms](#) on page 39.
- Schedule inventory jobs. For more information, see [Schedule inventory job](#) on page 38.
- Schedule warranty retrieval job. For more information, see [Schedule warranty retrieval jobs](#) on page 39.

Initial configuration

After you complete the basic installation of OMIVV and registration of the vCenters, the Initial Configuration Wizard is displayed automatically for the first time, when you launch OMIVV in vCenter.

If you want to launch the initial configuration wizard later, go to:

- **Settings > Initial Configuration Wizard > START INITIAL CONFIGURATION WIZARD**
- **Dashboard > Quick References > START INITIAL CONFIGURATION WIZARD**

1. On the **Welcome** page, read the instructions, and then click **GET STARTED**.
2. On the **Select vCenter** page, from the **vCenters** drop-down menu, select a specific vCenter or **All Registered vCenters**, and then click **NEXT**.

NOTE: If you have multiple vCenter servers that are part of the same PSC registered with the same OMIVV appliance, and if you choose to configure a single vCenter server, repeat step 2 until you configure each vCenter.

3. On the **Create Host Credential Profile** page, click **CREATE HOST CREDENTIAL PROFILE**. For more information about creating a host credential profile, see [Create host credential profile](#) on page 37.

After hosts are added to a host credential profile, the IP address of OMIVV is automatically set as SNMP trap destination for host's iDRAC. OMIVV automatically enables the WBEM service for hosts running ESXi 6.5 and later.

OMIVV uses the WBEM service to properly synchronize the ESXi host and the iDRAC relationships. If configuring the SNMP trap destination fails for particular hosts, and/or enabling the WBEM service fails for particular hosts, those hosts are listed as non-complaint. To view and fix the non-compliance, see the Management Compliance section in User's Guide.

4. On the **Configure Additional Settings** page, do the following:
 - a. Schedule inventory jobs. For more information about scheduling the inventory job, see [Schedule inventory job](#) on page 38.
 - b. Schedule warranty retrieval job. For more information about scheduling the warranty retrieval job, see [Schedule warranty retrieval jobs](#) on page 39.
If you want to modify the inventory job schedule, go to **Settings > vCenter Settings > Data Retrieval Schedule > Inventory Retrieval** or **Jobs > Inventory**.
If you want to modify the warranty retrieval job schedule, go to **Settings > Warranty Retrieval > Jobs > Warranty**.
 - c. Configure events and alarms. For information about configuring events and alarms, see [Configure events and alarms](#) on page 39.
 - d. To apply individual settings, click the **Apply** button separately, and then click **NEXT**.
It is highly recommended to enable all the additional settings. If any of the additional settings are not applied, a message is displayed indicating that the all the additional settings are mandatory.
5. On the **Next Steps** page, read the instructions, and then click **FINISH**.
Dell EMC recommends associating your OMIVV hosts with a configuration baseline because it enables you to closely monitor the configuration changes happening in hosts and associated clusters. Configuration baseline can be created for any cluster once the hosts are successfully managed by OMIVV. To create a configuration baseline, do the following:
 - Create Repository Profile for Firmware and Driver—This helps you to define baselined firmware and driver versions.
 - Create System Profile—This helps you to define baselined hardware configurations for hosts.
 - Create Cluster Profile—To create successful baseline, select clusters and associate firmware, drivers, and hardware configurations.
 - The hosts present in a PowerEdge MX chassis with an iDRAC IPv4 disabled has to be managed using a chassis credential profile.

Create host credential profile

If the number of added hosts exceeds the license limit for creating a host credential profile, you cannot create a host credential profile.

Before using the Active Directory (AD) credentials with a host credential profile, ensure that:

- The user account exists in AD.
 - The iDRAC or host is configured for an AD-based authentication.
1. On the OMIVV home page, click **Compliance & Deployment > Host Credential Profile**.
 2. On the **Create Host Credential Profile** page, click **CREATE NEW PROFILE**.
 3. On the **Host Credential Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
 4. On the **Name and Credentials** page, do the following:
 - a. Enter the profile name and description. The description field is optional.
 - b. From the **vCenter Name** list, select an instance of vCenter on which you want to create the host credential profile.

NOTE: If you select **All Registered vCenters** while creating the host credential profile, test connection fails for all hosts running ESXi 6.5 or later that have the WBEM service disabled. In such case, Dell EMC recommends completing the host credential profile wizard actions, run the inventory on hosts, and then test the host credential profile again.
 - c. In the **iDRAC Credentials** area, enter the iDRAC local credentials or AD credentials.
 - To enter the local credentials of iDRAC, perform the following tasks:
 - Enter the user name in the **User Name** box. The user name is limited to 16 characters. For information about defining user names, see the *iDRAC User's Guide* available at dell.com/support.
 - Enter password. For more information about the recommended characters in user names and passwords, see the *iDRAC User's Guide* available at dell.com/support.
 - To download and store the iDRAC certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.
 - To enter the credentials for an iDRAC that is already configured and enabled for AD, select the **Use Active Directory** check box.

NOTE: The iDRAC account requires administrative privileges for updating firmware and deploying an OS.

- o Enter the user name in the **Active Directory User Name** box. Enter the user name in one of the formats such as `domain\username` or `username@domain`. The user name is limited to 256 characters. See the *Microsoft Active Directory Documentation* for user name restrictions.
- o Enter password.

The AD credential can be either same or separate for both the iDRAC and hosts.

- o To download and store the iDRAC certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.

d. In the **Host Root** area, enter the host local credentials or AD credentials.

- To enter the local credentials of ESXi host, perform the following tasks:
 - o The default username is **root**. You cannot edit it.
 - o Enter password.
 - o To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
- To enter the credentials for hosts that are already configured and enabled for AD, select the **Use Active Directory** check box.
 - o Enter the user name in the **Active Directory User Name** box. Enter the user name in one of the formats such as `domain\username` or `username@domain`. The user name is limited to 256 characters. See the *Microsoft Active Directory Documentation* for user name restrictions.
 - o Enter password.
 - o To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.

NOTE: For hosts running ESXi 6.5 U2 and later versions, OMIVV can obtain the iDRAC information even if incorrect host credentials are entered.

5. Click **Next**.

The **Select Hosts** page is displayed.

NOTE: If you try to manage all the OMIVV-managed hosts in a single host credential profile, it may take few minutes to display the Dell inventory notification in vCenter. This delay might be seen when you add large number of hosts to a host credential profile for the first time. Subsequent inventory runs normally.

6. On the **Select Hosts** page, expand the tree view and select the hosts, and then click **OK**.

- Click **ADD HOST** to add or remove hosts from the **Associated Hosts** page.

NOTE: Do not add a PowerEdge MX server with a disabled iDRAC IPv4 to a host credential profile. These servers are managed using a chassis credential profile.

The selected hosts are displayed on the **Associated Hosts** page.

7. To test the connection, select one or more hosts, and click **BEGIN TEST**. Dell EMC recommends you to test the connection for all configured hosts.

NOTE: Even after entering valid credentials, the test connection operation may fail for host, and a message is displayed indicating that invalid credentials are entered. This issue is observed if ESXi is blocking the access. Multiple attempts to connect the ESXi by using incorrect credentials blocks you from accessing ESXi for 15 minutes. Wait 15 minutes and retry the operation.

- To stop the test connection process, click **ABORT TEST**.

You can view the test connection results in the **TEST RESULTS** section.

NOTE: If the WBEM service is disabled for any hosts running the ESXi 6.5 or later versions, WBEM is automatically enabled when you perform the test connection or while running inventory on those hosts.

NOTE: Testing iDRAC connectivity in a host credential profile using an incorrect password locks the iDRAC access to the appliance until the penalty time configured in iDRAC. Retry with the correct password after the penalty time specified in the IP filtering and blocking settings in iDRAC.

8. Click **Finish**.

Schedule inventory job

To view the latest inventory data on OMIVV, you must schedule an inventory job to run periodically to ensure that inventory information of hosts or the chassis is up-to-date. Dell EMC recommends running the inventory job on a weekly- basis.

NOTE: The chassis is managed in OMIVV context. There is no context of vCenter in chassis management. After scheduled host inventory is complete, the chassis inventory is triggered for all the chassis that are managed using OMIVV.

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. On the OMIVV home page, click **Settings > vCenter Settings > Data Retrieval Schedule > Warranty Retrieval**.
2. Select the **Enable Inventory Data Retrieval (Recommended)** check box.
In PSC environment with multiple vCenter servers, if the schedule for individual vCenter is different and you select the **All Registered vCenters** option to update the inventory schedule, the inventory schedule settings page displays the default schedule.
3. Select the inventory data retrieval day and time, and click **APPLY**.

NOTE: In PSC environment with multiple vCenter servers, if you update the inventory schedule of **All Registered vCenters**, the update overrides the individual vCenter inventory schedule settings.

Schedule warranty retrieval jobs

1. Ensure that the inventory is run successfully on hosts and chassis.
2. To use the warranty features of OMIVV, you must have an Internet connection. If your environment requires proxy to reach Internet, ensure that you configure the proxy settings in the Admin portal.

Hardware warranty information is retrieved from Dell Online and displayed by OMIVV. Only the Service Tag is sent and not stored by Dell Online.

In PSC 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 credential 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. On the OMIVV home page, click **Settings > vCenter Settings > Data Retrieval Schedule > Warranty Retrieval**.
2. Select the **Enable Warranty Data Retrieval (Recommended)** check box.
In PSC environment with multiple vCenter servers, if the schedule for individual vCenter is different and you select the **All Registered vCenters** option to update the warranty schedule, the warranty schedule settings page displays the default schedule.
3. Select the warranty data retrieval day and time, and click **APPLY**.

NOTE: In PSC environment with multiple vCenter servers, if you update the warranty schedule of **All Registered vCenters**, the update overrides the individual vCenter warranty schedule settings.

Configure events and alarms

To receive events from the servers, ensure that the SNMP trap destination is set in iDRAC. OMIVV supports SNMP v1 and v2 alerts.

1. On the OMIVV home page, click **Settings > vCenter Settings > Events and Alarms**.
2. To enable alarms for all hosts and its chassis, click **Enable Alarms for all hosts and its chassis**.
The **Enable the Dell EMC Alarm Warning** page displays the clusters and non-clustered host that might be impacted after enabling the Dell EMC alarms.

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

NOTE: In vCenter 6.7 U1 and 6.7 U2, the edit option fails. For editing alarm definitions, Dell EMC recommends using Web Client (FLEX).

NOTE: BMC Traps do not have Message IDs, so alerts will not have these details in OMIVV.

3. To accept the change, click **CONTINUE**.

The alarms for all hosts and its chassis are enabled.


4. Select any one of the following event posting levels:

- **Do not post any events**—Do not forward any events or alerts into its associated vCenters.
- **Post all Events**—Post all the events including informational events, and events received from the managed hosts and chassis into its associated vCenters. Dell EMC recommends selecting the Post all Events option as an event posting level.
- **Post only Critical and Warning Events**—Post only the critical and warning level events into its associated vCenters.
- **Post only Vitalization-Related Events**—Post the virtualization-related events received from hosts into its associated vCenters. Virtualization-related events are those that are most critical to hosts running VMs.

5. To save the changes, click **APPLY**.

To restore the default vCenter alarm settings for all hosts and its chassis, click **RESTORE ALARMS**. It might take up to a minute before the change takes effect.

The **RESTORE ALARMS** option is a convenient way to restore the default alarm configuration without uninstalling and reinstalling the product. If any Dell EMC alarm configurations are changed since installation, those changes are reverted using the **RESTORE ALARMS** option.

 **NOTE:** The events and alarms settings are not enabled after restoring the appliance. You can enable the Events and Alarms settings again from the Settings tab.

Configuration tasks on the Settings page

On the **Settings** page, you can perform the following tasks:

- [Configure warranty expiration notification](#)
- [Configure latest appliance version notification](#)
- [Configure deployment credentials](#)
- [Override severity of health update notification](#)
- [Initial Configuration](#)

Configure warranty expiration notification

Enable the warranty expiration notification to get notified if warranties for any of the hosts are nearing expiration.

1. On the OMIVV home page, click **Settings > Notifications > Warranty Expiration Notification**.
2. Select **Enable Warranty Expiration Notification for hosts**.
3. Select the number of days to be notified before the warranty expires.
4. Click **APPLY**.

Configure latest appliance version notification

To get notified about the availability of a new OMIVV version, select the **Enable Latest Version Notification (Recommended)** check box. Dell EMC recommends checking it on weekly basis. To use the latest appliance version notification features of OMIVV, you must have an Internet connection. If your environment requires a proxy to connect to Internet, ensure that you configure the proxy settings on the Admin portal.

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. On the OMIVV home page, click **Settings > Appliance Settings > Notifications > Latest Version Notification**.
2. Select the **Enable Latest Version Notification (Recommended)** check box.
3. To receive the latest appliance version notification, select the day and time.
4. Click **APPLY**.

Configure deployment credentials

OMIVV acts as a provisioning server. The deployment credentials enable you to communicate with iDRAC that uses the OMIVV plugin as a provisioning server in the auto discovery process. The deployment credentials enable you to set up iDRAC credentials to communicate securely with a bare-metal server that is discovered using auto discovery until the OS deployment is complete.

After the OS deployment process is successfully complete, OMIVV changes the iDRAC credentials as provided in the host credential profile. If you change the deployment credentials, all newly discovered systems using auto discovery are provisioned with the new iDRAC credentials from that point onwards. However, the credentials on servers that are discovered before the change of deployment credentials are not affected by this change.

1. On the OMIVV home page, click **Settings > Appliance Settings > Deployment Credentials**.
2. Enter the user name and password. The default user name is **root** and password is **calvin**. Ensure that you provide only the iDRAC supported characters and iDRAC local credentials.
3. Click **APPLY**.

Override severity of health update notification

You can configure to override the existing severity of the Dell Proactive HA events for the Dell EMC host and its components with customized severity, which is aligned to your environment.

The following are the severity levels that apply to each of the Proactive HA events:

- **Info**
- **Moderately Degraded**
- **Severely Degraded**

 **NOTE:** You cannot customize the severity of the Proactive HA components with the **Info** severity level.

1. In OpenManage Integration for VMware vCenter, click **Settings > Appliance Settings > Override Severity for Proactive HA**.
The data grid displays all the supported Proactive HA events and includes columns; events id, event description, component type, default severity, and override severity column for customizing the severity of the host and its components.
2. To change severity of a host or its component, in the **Override Severity** column, select the required status from the drop-down list.
This policy applies to all the Proactive HA hosts across all vCenter servers that are registered with OMIVV.
3. Repeat step 2 for all the events that must be customized.
4. Perform any one of the following actions:
 - a. To save the customization, click **APPLY**.
 - b. To cancel the override severity settings, click **CANCEL**.
To reset the override severity settings to default, click **RESET TO DEFAULT**.

Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — www.dell.com/SoftwareSecurityManuals
- For Dell EMC OpenManage documents — www.dell.com/OpenManageManuals
- For Dell EMC Remote Enterprise Systems Management documents — www.dell.com/esmmanuals
- For iDRAC documents — www.dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- For Dell EMC Serviceability Tools documents — www.dell.com/ServiceabilityTools
- 1. Go to www.support.dell.com .
- 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**
 - **Public Sector Solutions**
 - **Utilities**
 - **Mainframe**
 - **Serviceability Tools**
 - **Virtualization Solutions**
 - **Operating Systems**
 - **Support**
- 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.

Related Documentation

In addition to this guide, you can access the other guides available at www.dell.com/support/. Click **Browse all products**, then click **Software > Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 5.0** to access the following documents:

- *OpenManage Integration for VMware vCenter Version 5.0 User's Guide*
- *OpenManage Integration for VMware vCenter Version 5.0 Release Notes*
- *OpenManage Integration for VMware vCenter Version 5.0 Compatibility Matrix*

You can find the technical artifacts including white papers at <https://www.dell.com/support>.