OpenManage Integration for VMware vCenter

Version 5.2 Installation Guide

October 2020
Rev. A00

Notes, cautions, and warnings

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

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

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

Contents

1

Introduction

This guide provides instructions to install and configure OpenManage Integration for VMware vCenter (OMIVV). OMIVV is used to discover, monitor, and manage PowerEdge servers running VMware vCenter. After successfully completing the installation of OMIVV, to perform inventory management, monitoring and alerts, firmware updates, and warranty management, see *OpenManage Integration for VMware vCenter User's Guide* available at **https://www.dell.com/support**.

Topics:

OpenManage Integration for VMware vCenter (OMIVV) licensing

OMIVV 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 OMIVV. 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 standard license is available for periods of three or five years. Any additional licenses bought extend the period of the existing license.

License duration for a single XML key is calculated based on the sales date of the original order. Any uploaded new licenses will be reflected in the count after the 90 day grace period ends for any prior, expiring licensing.

OMIVV supports up to 15 vCenter instances. 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**.

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital Locker at **https://www.dell.com/support**. If you are unable to download your license keys, contact Dell Support by going to **Contact Order Support** at **https://www.dell.com/support** to locate the regional Dell Support phone number for your product.

Licensing presents the following information in the OMIVV Administration Console:

- 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 (with a maximum of 2000 hosts supported for a single OMIVV instance).
- 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.

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.

NOTE: Any active license can be used for OMIVV 5.x versions. Licenses backed up from previous instances of OMIVV, or downloaded again from the Digital Locker can be used for current instances of OMIVV.

Buy software license

1. Go to **Settings** > **Licensing** > **Buy License**, or **Dashboard** > **Buy License**, or **Admin Portal** > **vCenter Registration** > **Licensing** > **BUY NOW**.
   The DellEMC support page is displayed.
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.

Manage Licenses

License file for new purchases

When you order a new license, an email is sent from Dell EMC after the order confirmation. You can download the new license file from the Dell EMC Digital Locker at **https://www.dell.com/suppot**. The license is sent to you as an XML file. If you receive a ZIP file instead, extract the XML file first before uploading it.

Stacking licenses

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 when 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 EMC, 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.

Important notes for reference

- From OMIVV 5.0 onwards, only VMware vSphere Client (HTML5) 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, it is recommended 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 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 18.
- Configure your network to match the port requirements. For more information, see Port information on page 12.

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

Hardware requirements

OMIVV supports full support for Dell EMC PowerEdge servers with full feature support for iDRAC Express and Enterprise. To verify that your host servers are eligible, see information about the following in the subsequent subsections:

- Supported BIOS and iDRAC versions
- Supported iDRAC versions (both deployment and management)
- Supported memory, CPU, and disk space for provisioned storage

OMIVV requires LAN on motherboard or Network daughter card that can access the management network of iDRAC, CMC or OME-Modular systems management network, and the vCenter management network.For more information, see Configure OMIVV appliance on page 25 and Configure OMIVV appliance with two Network Interface Controllers (NICs) on page 28.

Supported BIOS versions

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

It is recommended that you 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 1. Supported BIOS version for 12G PowerEdge servers

Server	Minimum BIOS 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
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

Table 1. Supported BIOS version for 12G PowerEdge servers

Server	Minimum BIOS Version
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

Table 2. Supported BIOS version for 13G PowerEdge servers

Server	Minimum BIOS Version
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

Table 3. Supported BIOS version for iDRAC9-based PowerEdge servers

Server	Minimum BIOS Version
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
R440	1.0.0 or later

Table 3. Supported BIOS version for iDRAC9-based PowerEdge servers

Server	Minimum BIOS Version
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
XR2	2.2.11 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
R7525	1.2.4 or later
XE2420	1.0.0 or later

Table 4. Supported BIOS version for vSAN Ready Nodes

vSAN Ready Node	Minimum BIOS Version
R740xd	1.0.0 or later
R640	1.0.0 or later
R440	1.0.0 or later
R6415	1.0.0 or later
C6420	1.0.0 or later
R840	1.0.0 or later

Supported iDRAC with Lifecycle Controller versions

Table 5. Supported iDRAC with Lifecycle Controller for deployment

Servers	iDRAC with Lifecycle Controller
12G	2.50.50.50 or later
13G	2.50.50.50 or later
iDRAC9-based servers	3.00.00.00 and later

Table 6. BIOS and iDRAC requirements for cloud server

Model	BIOS	iDRAC with Lifecycle Controller
C6320	1.0.2	2.50.50.50 or later

Table 6. BIOS and iDRAC requirements for cloud server

Model	BIOS	iDRAC with Lifecycle Controller
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 7. Supported features on PowerEdge servers

Features	12G and 13G	iDRAC9-based Servers
Hardware Inventory	Y	Y
Events and Alarms	Y (SNMP v1 and v2)	Y (SNMP v1 and v2)
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
vSphere Lifecycle Manager	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.

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

~ Supported only for Rack servers.

^ Only platforms certified for vSphere 7.0 and 7.0 U1

Supported features on PowerEdge chassis

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

Table 8. 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
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. For more information about port requirements, see Port information on page 12.

To display OpenManage Integration for VMware vCenter, a system must have a minimum 1024 x 768 screen resolution and a web browser that meets minimum requirements based on the operating system.

It is recommended that you use Google Chrome to access the OMIVV features. OMIVV supports Google Chrome and Mozilla Firefox. Microsoft Internet Explorer is not supported.

It is recommended to use the latest version of the supported browsers. For specific browser versions, see the VMware Documentation for the vCenter version that you are using.

Requirements for VMware vSphere Client (HTML-5)

vCenter 6.5 U2 and later

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

Table 9. Supported vCenter server versions

vCenter version	Client support
6.5 U2	Y
6.5 U3	Y

Table 9. Supported vCenter server versions

vCenter version	Client support
6.7	Y
6.7 U1	Y
6.7 U2	Y
6.7 U3	Y
7.0	Y
7.0 U1	Y

Use the latest patch build 13638625 or later for vCenter 6.5 U2.

The OMIVV 5.2 appliance runs on CentOS version 7.7.

Supported ESXi versions on managed hosts

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

Table 10. Supported ESXi versions

ESXi Version	12G	13G	iDRAC9-based servers
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
7.0	N	Y	Y
7.0 U1	N	Y	Y

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

Port information

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

Table 11. Virtual appliance

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.
68	DHCP	UDP	None	In	DHCP server to OMIVV appliance	Dynamic network configuration	To get the network details such as IP, gateway, Netmask, and DNS.

Table 11. Virtual appliance

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
69	TFTP	UDP	128-bit	Out	OMIVV to iDRAC	Trivial File Transfer	Used to update the bare-metal server to minimum supported firmware version.
123	NTP	UDP	None	In	NTP to OMIVV appliance	Time Synchronization	To sync with specific time zone.
162	SNMP Agent	UDP	None	In	iDRAC or CMC, or OME-Modular to OMIVV appliance	SNMP Agent (server)	To receive SNMP traps from managed nodes.
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.
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	HTTPS	TCP	128-bit	In	ESXi server to OMIVV appliance	HTTPS server	Used in operating system deployment flow for post installation scripts to communicate with the OMIVV appliance.
443	HTTPS	TCP	128-bit	In	iDRAC to OMIVV appliance	Auto Discovery	Provisioning server that is used for auto discovering managed nodes.
443	WSMAN	TCP	128-bit	In/Out	OMIVV appliance to or from iDRAC	iDRAC communication	iDRAC, or CMC, or OME-Modular communication, used to manage and monitor the managed nodes.
445/139	SMB	TCP	128-bit	Out	OMIVV appliance to CIFS	CIFS communication	To communicate with Windows share.
2049 /111	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 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.
User-defined	Any	UDP/TCP	None	Out	OMIVV appliance to proxy server	Proxy	To communicate with the proxy server.

Table 12. Managed nodes (ESXi)

Table 12. Managed nodes (ESXi)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
162	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.

For more information about the iDRAC and CMC port information, see the *Integrated Dell Remote Access Controller User's Guide* and *Dell Chassis Management Controller User's Guide* available at **https://www.dell.com/support**.

For more information about the OME-Modular port information, see the *Dell EMC OME-Modular User's Guide* available at **https://www.dell.com/support**.

Dell Online destination URL

Table 13. Dell Online destination URL

Feature	Destination URL
Warranty details	https://apigtwb2c.us.dell.com
Warranty key	https://downloads.dell.com/catalog/CatalogIndex.gz
Firmware Update	https://downloads.dell.com
RPM Upgrade	https://linux.dell.com

2

Install and configure OMIVV

Ensure that all requirements are met and you are running the required VMware vCenter. For more information, see Hardware requirements on page 7 and Software requirements on page 11.

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 **https://www.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. For more information, see Configure Network Time Protocol (NTP) and set local time zone on page 33.
5. Configure the network settings. For more information, see Configure OMIVV appliance on page 25.
6. Upload the license file. For more information about licensing, see Upload license to OMIVV Administration Console on page 24.
7. Set the deployment mode as per the requirement. For more information, see Configure deployment mode on page 18.
8. Register the OMIVV appliance with the vCenter server by using Administration Console. See Register new vCenter server on page 21.
9. Complete the appliance configuration settings. For more information, see Configure OMIVV appliance on page 25.

Topics:

Prerequisite checklist

Before you start the product installation, ensure that:

- You have username 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 6.5 U3 and earlier ESXi host systems, or the Active Directory credentials that have administrative rights on the host.
- You have the username and password that is associated with iDRAC Express or Enterprise which has administrative rights on the iDRAC.
- You have administrator privilege in iDRAC.
- The Simple 2FA and Smart Card log-On are disabled in iDRAC for iDRAC9-based servers.
- 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 NICs.
- The VMware vSphere environment meets virtual appliance system requirements, port access, clock synchronization, and listening port requirements.

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

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* available at **https://www.dell.com/support**.

1. Go to the locations 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. If you want to select the OVF package from your local system, select **Local file** and, then click **Choose Files**.
   c. Select the files (.mf, .ovf, and .vmdk).
   d. 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, it is recommended 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**.

   It is mandatory to select destination compute resource to proceed further. The compatibility check is performed to validate whether the destination compute resource is selected or not.

   The **Review Details** window is displayed with the following information:
   - **Publisher**—The publisher data
   - **Download Size**—The 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, 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 Interface Controllers (NICs) on page 28.

    - 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.

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**.
   To check the status, go to **Event Console** of vSphere Client of registered vCenters.

While uploading certificate, OMIVV administration console becomes unresponsive for up to 3 minutes. 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**.

While restoring certificate, OMIVV administration console becomes unresponsive for up to 3 minutes. After restore default HTTPs certificate task is complete, close the browser session and access admin portal in a new browser session.

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 14. 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
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.

To integrate the OpenManage Mangement Pack for vRealize operations (vROPS) with OMIVV, the minimum required deployment mode is **Medium**.

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.
   - 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, turn off the OMIVV appliance, update the system resources to the existing set deployment mode, and turn on the OMIVV appliance.

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.

Register vCenter server using a non-administrative account

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 20.

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
- Health Update Provider

- Register
- Unregister
- Update

- Host
  - CIM
    - CIM Interaction
- Host.Config
  - Advanced settings
  - Change Settings
  - Connection
  - Maintenance
  - Network configuration
  - Query patch
  - Security profile and firewall
- Inventory
  - Add host to cluster
  - Add standalone host
  - Modify cluster
- Lifecycle Manager: General Privileges
  - Read

  NOTE: The vSphere Lifecycle Manager General Privileges are applicable only for vCenter 7.0 and later.
- Host profile
  - Edit
  - View
- Permissions
  - Modify permission
  - Modify role
- Sessions
  - Validate session
- Task
  - Create
  - Update

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 20.

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.

Read-only user role

There is a unprivileged user called "readonly" with shell access for diagnostic purposes. The read-only user has limited privileges to run few commands.

Register new vCenter server

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

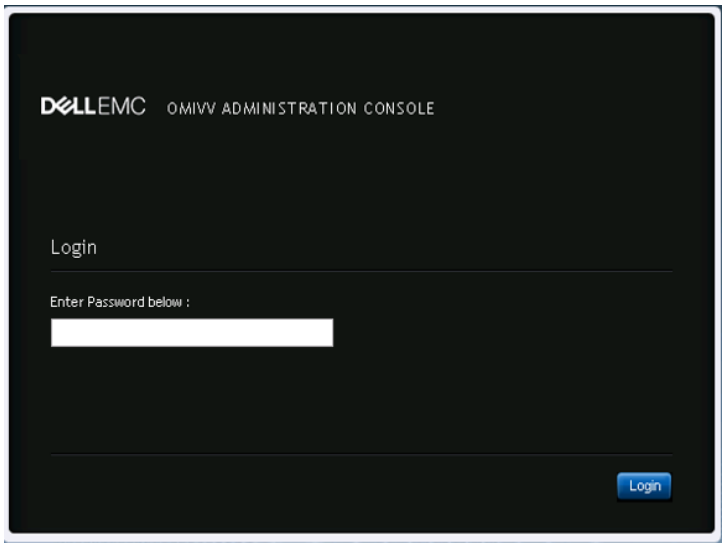


Figure 1. Administration Console

   If you are logging in for the first time you are prompted to accept the EULA.
3. On the **Dell EMC End-User License Agreement** page, do the following:
   a. Read the terms and conditions, and then select the **I accept the terms in the license agreement** check box.
   b. Click **Accept**.
   For more information about Telemetry EULA, click **DELL EMC Telemetry EULA**.

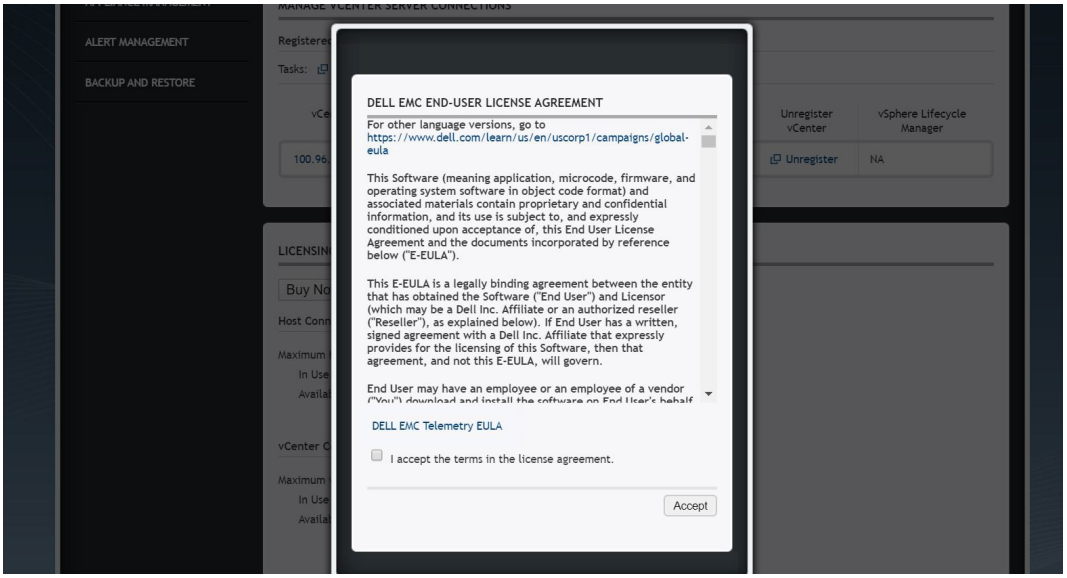


Figure 2. Dell EMC EULA agreement

4. In the **vCenter Registration** window, click **Register a New vCenter Server**.

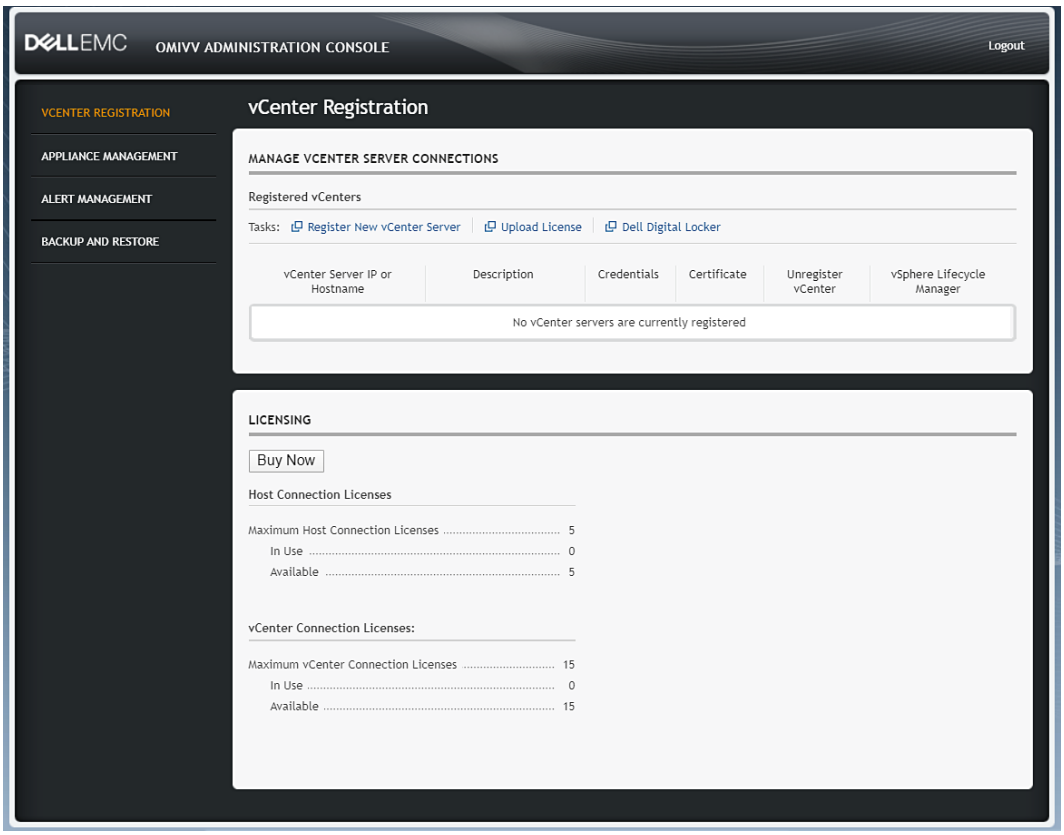


Figure 3. vCenter Registration

5. 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,

      NOTE: It is recommended that you register OMIVV 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. In the **Description** text box, enter a description. The description is optional.

c. Under **vCenter User Account**, in **vCenter User Name**, enter the user name of administrator or a non-administrator user name with the required 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 using a non-administrative account on page 19.

d. In the **Password** box, enter the password.

e. In the **Verify Password**, enter the password again.

f. Select the **Register vSphere Lifecycle Manager (vCenter 7.0 and later)** check box. Selecting the **Register vSphere Lifecycle Manager** check box allows you to use vSphere Lifecycle Manager feature from vCenter 7.0 and later.

   You can modify (register or unregister) the vSphere Lifecycle Manager status after the vCenter registration is complete. For more information, see Register vSphere Lifecycle Manager in Dell EMC administration console on page 24 and Unregister vSphere Lifecycle Manager in Dell EMC administration console on page 24.

6. Click **Register**.

   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 24.

   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.

7. 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 **https://www.dell.com/support**, and you can import this license to your virtual appliance. To import the license file, click **Upload License**. For more information about uploading a license, see Upload license to OMIVV Administration Console on page 24.

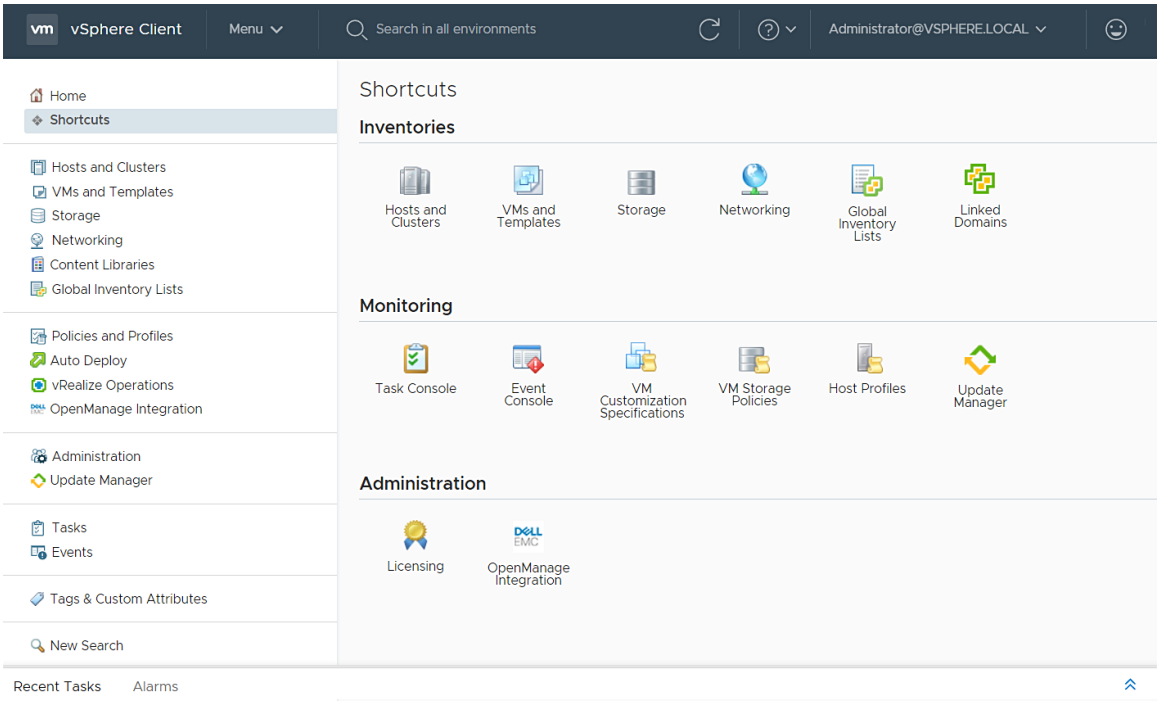


Figure 4. OpenManage Integration for VMware vCenter successfully added to vCenter

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

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

Upload license to OMIVV Administration Console

Ensure that your licenses are ready for download at Dell Digital Locker at **https://www.dell.com/support**. 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 at **https://www.dell.com/support**. The license file is available as an .XML format.

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**.

   NOTE: If you modify or edit the license file, the license file (.XML file) does not work. 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 at **https://www.dell.com/support** to locate the regional Dell Support phone number for your product.

Register vSphere Lifecycle Manager in Dell EMC administration console

The vCenter must be 7.0 and later version.

1. Go to https://<ApplianceIP/hostname/>.
2. On the **VCENTER REGISTRATION** page, under **vSphere Lifecycle Manager**, click **Register**.
   The **REGISTER VSPHERE LIFECYCLE MANAGER** <vCenter Name> dialog box is displayed.
3. Click **Register vSphere Lifecycle Manager**.
   A message displays that indicates the successful registration of vSphere Lifecycle Manager.

   For information about managing cluster using vSphere Lifecycle Manager, see the OMIVV User's Guide available at **https://www.dell.com/support**.

Unregister vSphere Lifecycle Manager in Dell EMC administration console

The vCenter must be 7.0 and later version.

1. Go to https://<ApplianceIP/hostname/>.
2. On the **VCENTER REGISTRATION** page, under **vSphere Lifecycle Manager**, click **Unregister**.
   The **UNREGISTER VSPHERE LIFECYCLE MANAGER** <vCenter Name> dialog box is displayed.
3. Click **Unregister**.
   A message is displays that indicates the successful unregistration of vSphere Lifecycle Manager. The **DellEMC OMIVV** is removed from the **Hardware Support Manager** list in vSphere Lifecycle Manager. There is no impact on the OMIVV functions.

   For information about managing cluster using vSphere Lifecycle Manager, see the OMIVV User's Guide available at **https://www.dell.com/support**.

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.

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**.

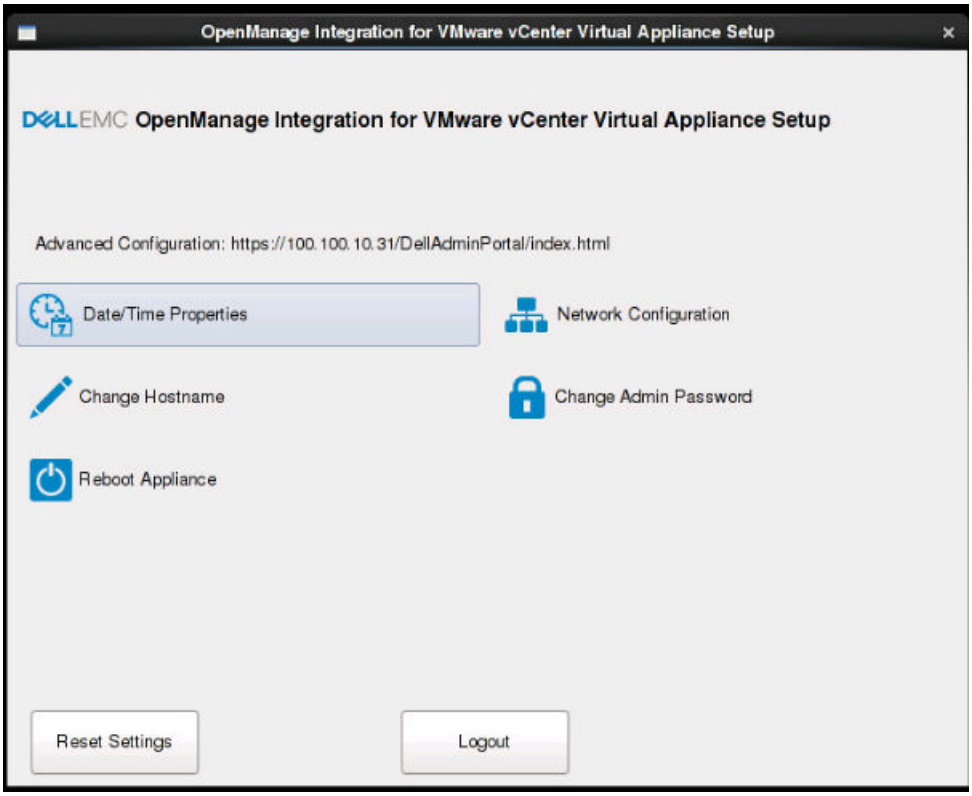
   NOTE: After unregistering OMIVV, log out and log in from the vSphere Client (HTML-5). If the OMIVV icon is still visible, then restart the Client services for both vSphere Client (HTML-5) and Web Client (FLEX).

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 (NTP) servers on page 33.

b. Click **Time Zone** and select the applicable time zone, and then click **OK**.

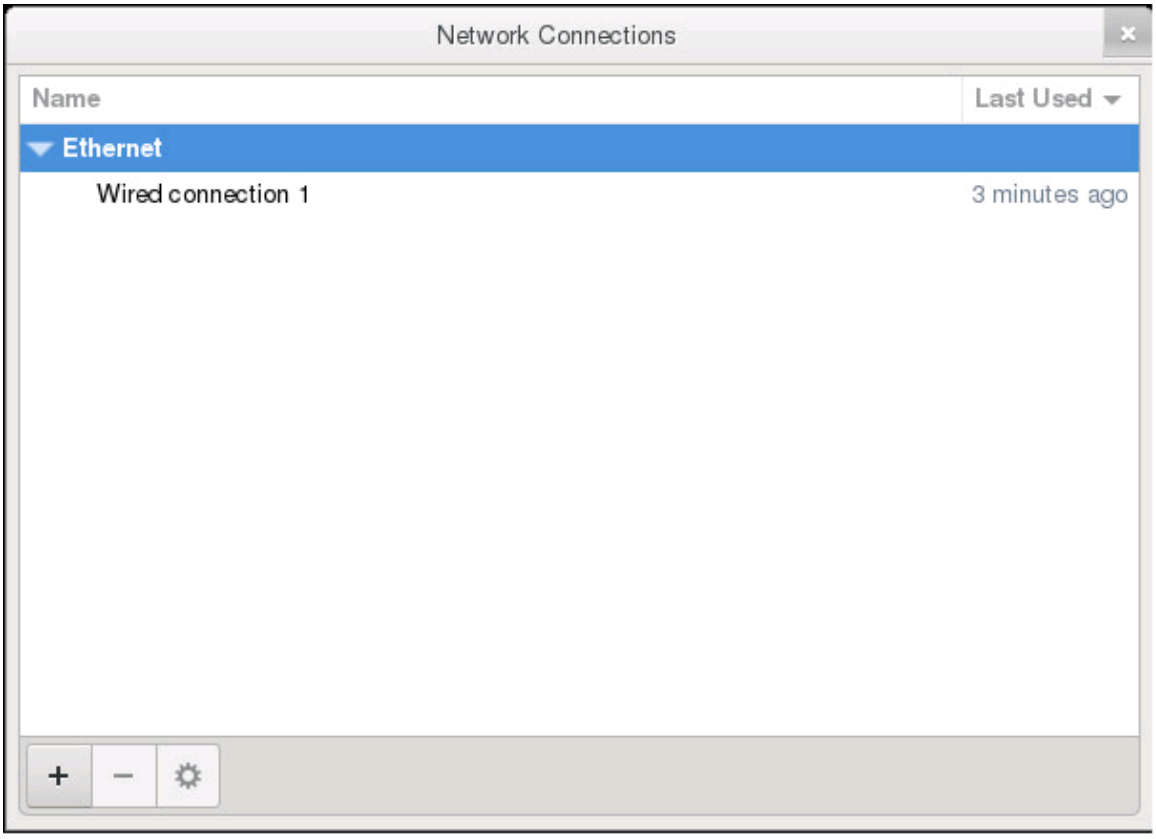
6. To configure network of the OMIVV appliance, click **Network Configuration**.

   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. It is recommended that you configure 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 Interface Controllers (NICs) on page 28.

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



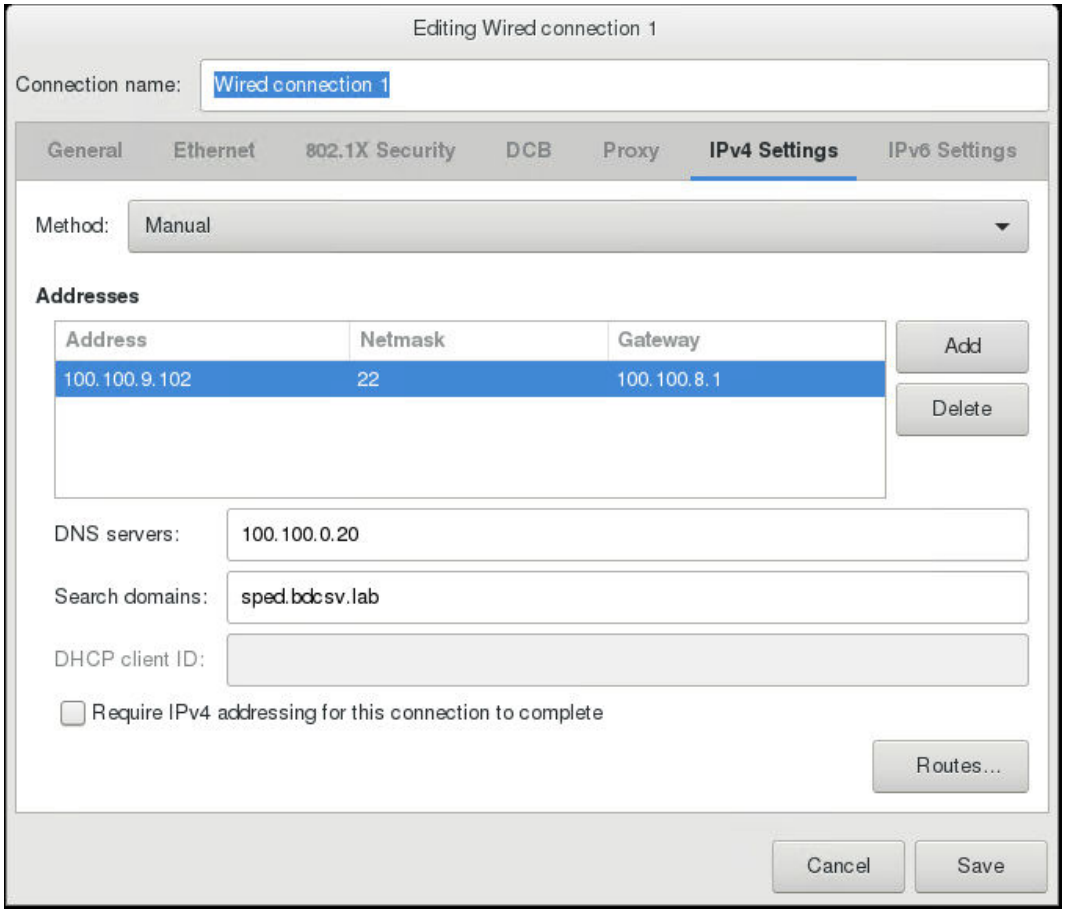
a. Click the **IPv4 Settings** tab, select **Manual** from the **Method** drop-down list, and click **Add**.

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**.



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 34.

9. Restart the appliance.

Configure OMIVV appliance with two Network Interface Controllers (NICs)

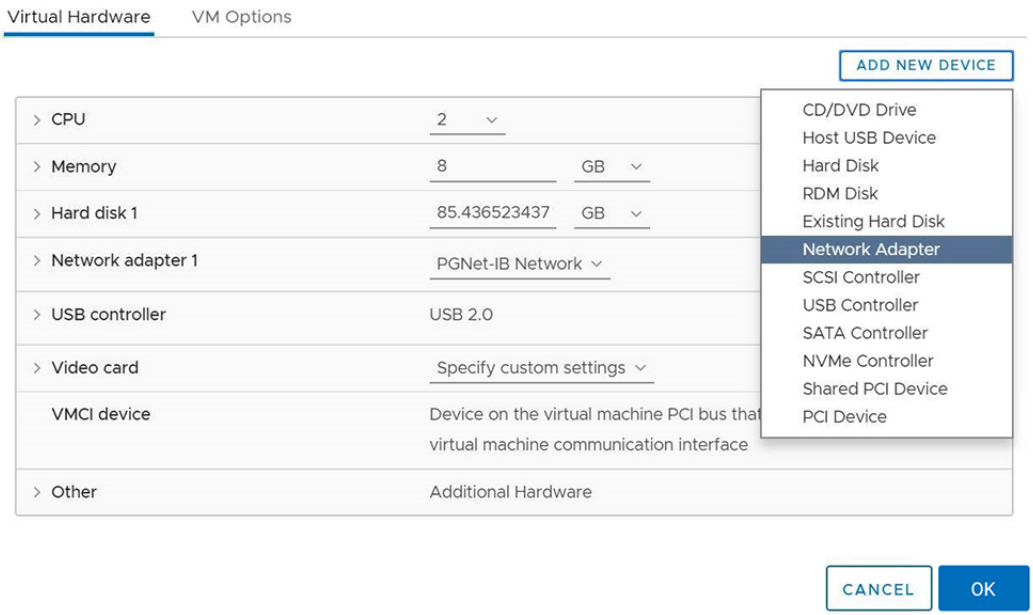
To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and OME-Modular). If vSphere network and out-of-band network are maintained as separate isolated network in your environment,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

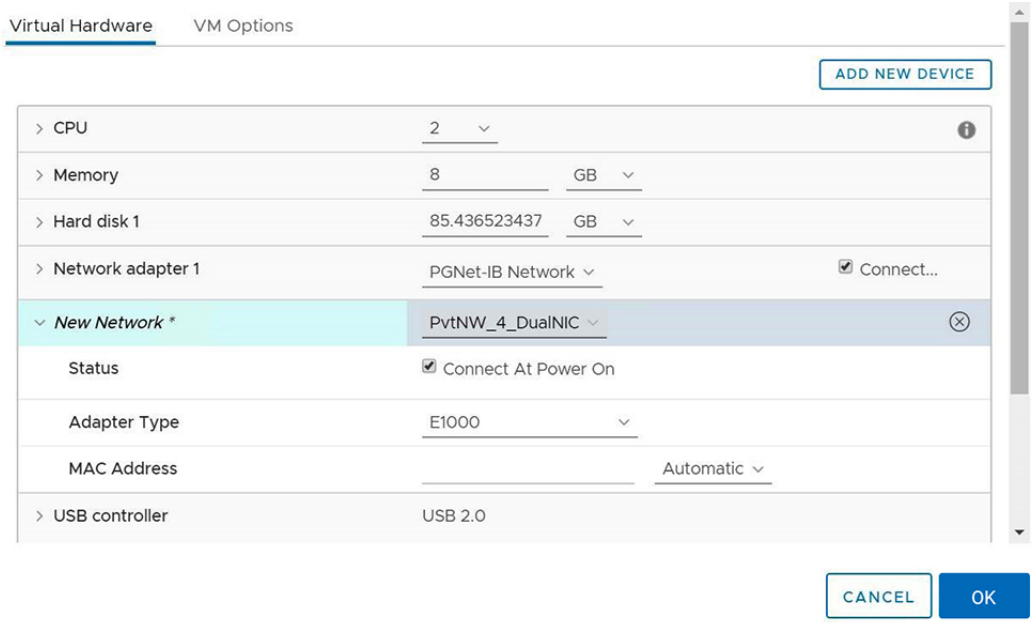
- DNS requirements—The OMIVV supports DNS configuration for only one network. For more information about DNS configuration, go to step 9 (b) in this topic.

1. Turn off 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**.

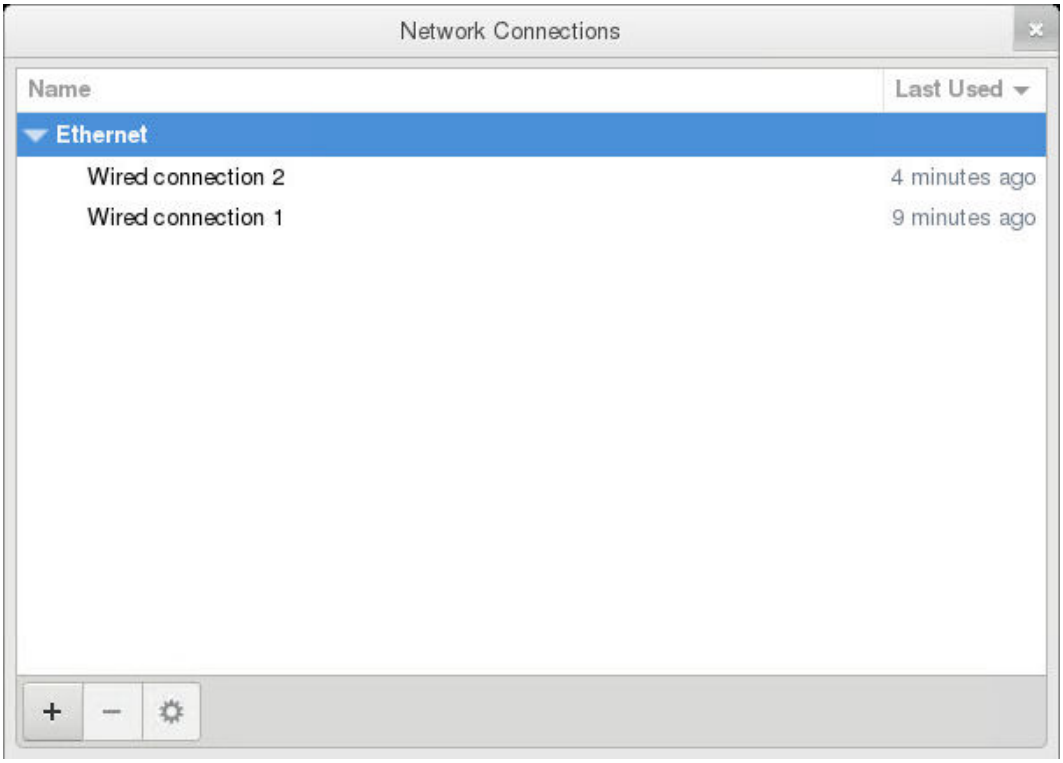


   a. Select the appropriate network for the NIC, and then select the **Connect At Power On** check box.
   b. Select the **VMXNET3** adapter type from the drop-down menu.

   NOTE: OMIVV supports VMXNET3 type of NIC.



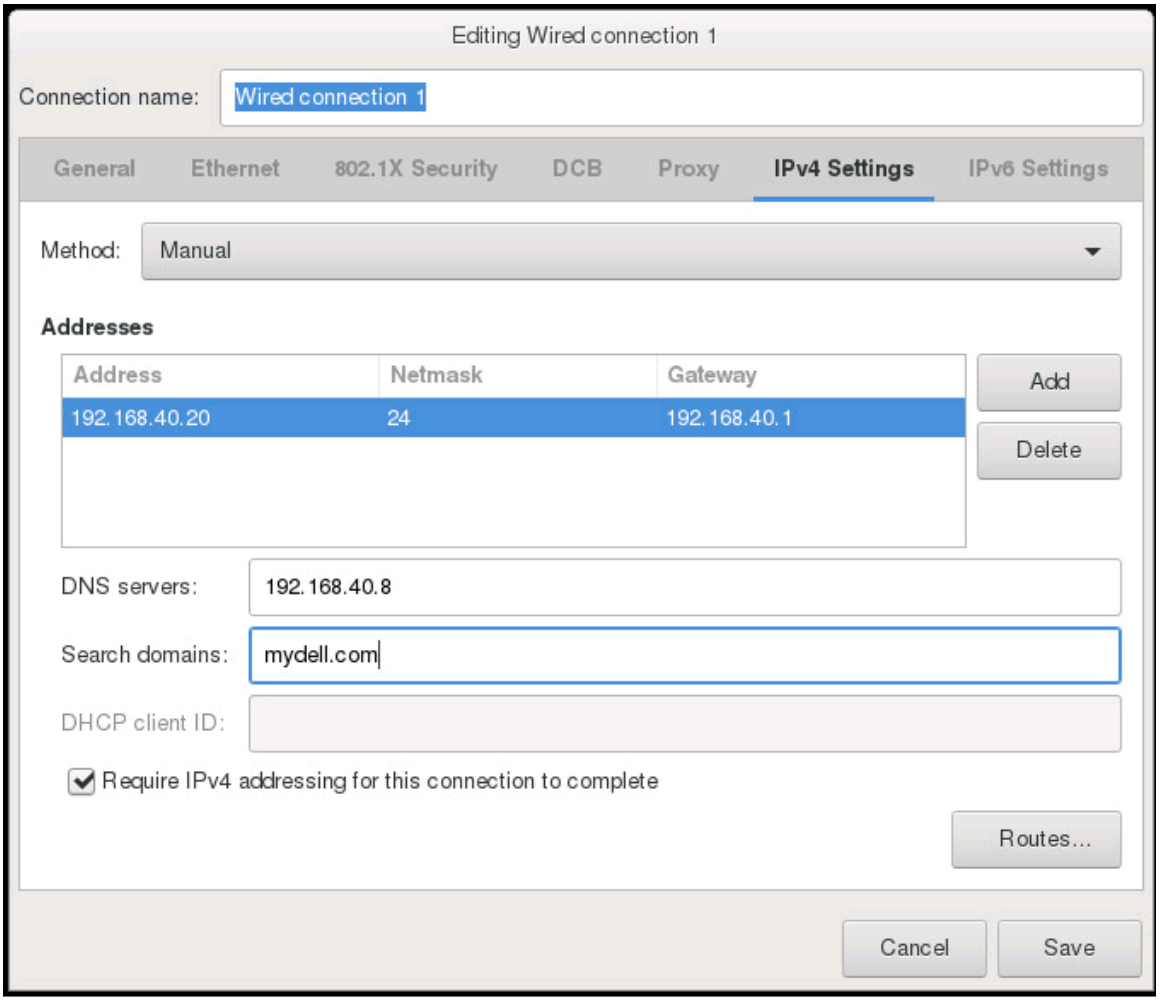
4. Turn on the OMIVV appliance. Log in as an administrator (the default username is Admin), and then press **Enter**.
5. On the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, select **Network Configuration**. The **Network Connections** page displays two NICs.



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

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 that you 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, It is recommended that you 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.

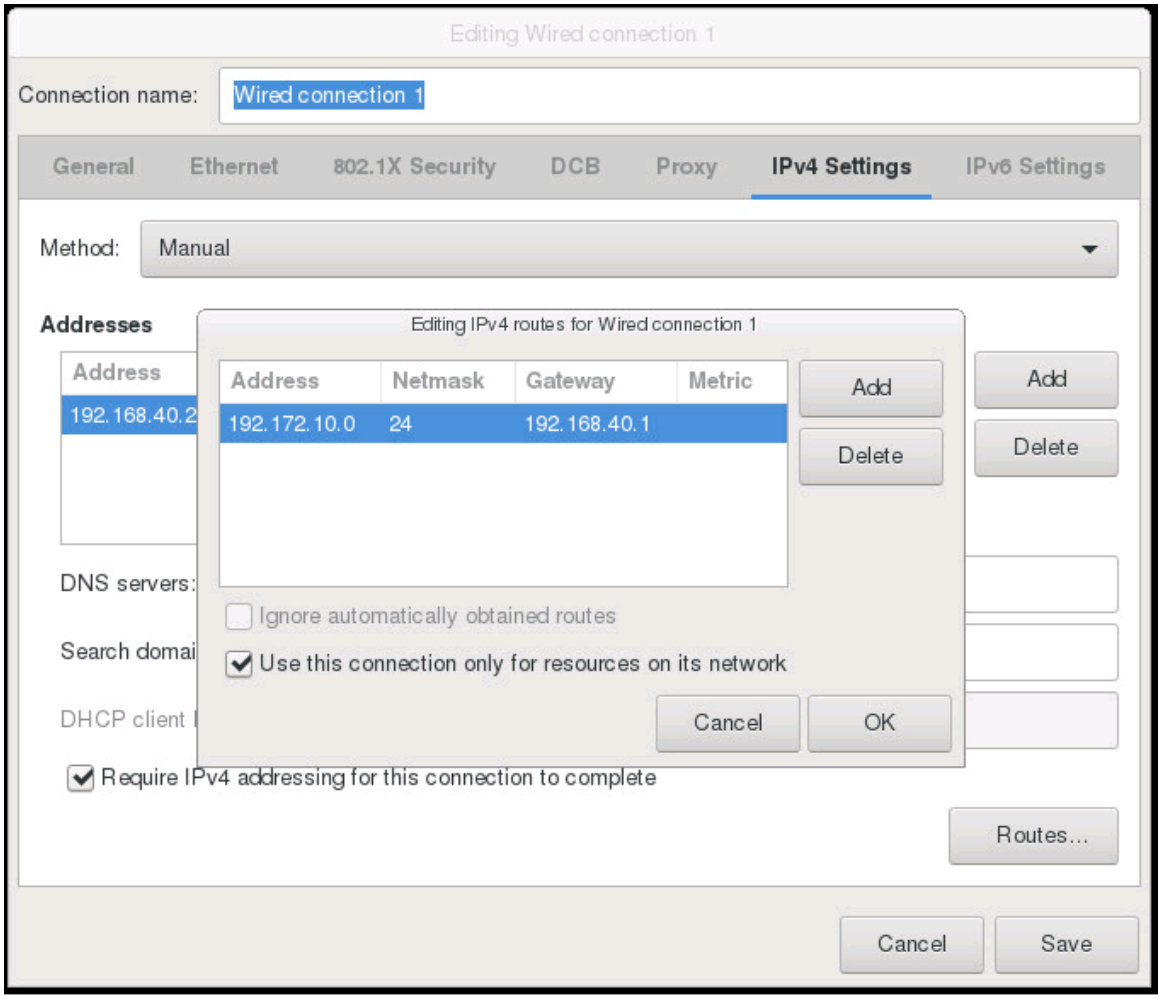
c. Enter the DNS server IP and domains to be searched for in the **DNS Servers** and **Search Domains** boxes respectively.

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.

    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`.

Change OMIVV appliance password

You can change the OMIVV appliance password in the vSphere Client by using the console.

1. Open the OMIVV web console.
2. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Change Admin Password**.
3. In the **Current Password** text box, enter the current admin password.

   The admin password should be at least eight characters and should include one special character, one number, one uppercase, and one lowercase letter.
4. Enter a new password in the **New Password** text box.

5. Retype the new password in the **Confirm New Password** text box.
6. Click **Change Admin Password**.

Configure Network Time Protocol (NTP) and set local time zone

1. Open the OMIVV web console.
2. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Date/Time Properties**.
   Ensure to enter the NTP details in Admin console. For more information, see Set up Network Time Protocol (NTP) servers on page 33.
3. On the **Date and Time** tab, select **Synchronize date and time over the network**.
   The **NTP Servers** window is displayed.
4. To add another NTP server IP or hostname (if required), click the **Add** button, and then press **TAB**.
5. Click **Time Zone**, select the applicable time zone, and then click **OK**.

Set up Network Time Protocol (NTP) servers

You can use NTP to synchronize the OMIVV appliance clocks to that of an NTP server.

1. In the Administration Console, 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 **Sychronize date and time over the network** check box.

NOTE: It might take few minutes for the OMIVV clock to synchronize with the NTP server.

NOTE: If the OMIVV admin portal is taking a long time to load information, ensure that NTP settings are correct and the NTP server is reachable by the OMIVV virtual machine.

Change hostname of OMIVV appliance

1. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Change Hostname**.

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

2. Enter an updated hostname.
   Type the domain name in the format: *<hostname>*.
3. Click **Update Hostname**.
   The appliance hostname is updated and main menu page is displayed.
4. To reboot the appliance, click **Reboot Appliance**.

NOTE: Ensure that you manually update all references to the virtual appliance across its environment such as provisioning server in iDRAC and Dell EMC Repository Manager (DRM).

Reboot OMIVV appliance

1. Open the OMIVV web console.
2. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Reboot Appliance**.
3. To reboot the appliance, click **Yes**.

Reset OMIVV appliance to factory settings

1. Open the OMIVV web console.
2. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Reset Settings**.

The following message is displayed:

```
All the settings in the appliance will be Reset to Factory Defaults and the appliance
will be rebooted. Do you still wish to continue?
```

3. To reset the appliance, click **Yes**.
   If you click **Yes**, the OMIVV appliance is reset to the factory default settings and all other settings and existing data is deleted.

   After the factory reset is complete, register vCenters to OMIVV appliance again.

NOTE: When the OMIVV appliance is reset to factory default settings, any updates that you had done on the network configuration are preserved. These settings are not reset.

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 19.

     For example, when you upgrade from vCenter 6.0 to vCenter 6.5, assign the extra privileges.
  2. Reboot the registered OMIVV appliance.
  3. If the registered vCenter is 7.0 or later, enable the vSphere LifeCycle Manager in the OMIVV administration console.
- For administrator users:
  1. Reboot the registered OMIVV appliance.
  2. If the registered vCenter is 7.0 or later, enable the vSphere LifeCycle Manager OMIVV administration console.

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: It is recommended that you retain 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 39.

Manage un-registration and re-registration

It is recommended that 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 39.

3

Upgrade 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 37.
- 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 (using Internet) on page 36.
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 39.
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.

Topics:

Upgrade OMIVV appliance using RPM (using Internet)

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.

   During the upgrade process, the appliance restarts once or twice. Once the appliance is RPM upgraded, ensure that you clear the browser cache before logging in to the Dell admin portal.

   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.

   All the customization that is done on the registered Dell alarms and Dell health update provider for PHA cluster will be restored to default after RPM upgrade.

Upgrade OMIVV appliance using RPM (without Internet)

Create HTTP or HTTPS share. Ensure that the HTTP or HTTPS share supports file name which includes special character such as ++ and space.

OMIVV supports only HTTP and HTTPS shares.

OMIVV supports upgrading from version 5.1 to 5.2 without having an Internet connection.

1. Download the RPM .zip package available at **https://www.dell.com/support**.
2. Extract the RPM .zip package and copy the files and folders from extracted location to HTTP or HTTPS share.
3. On the **APPLIANCE MANAGEMENT** page, in the **APPLIANCE UPDATE** area, click **Edit**, and then enter the shared location path in **Update Repository Path**.
4. Click **Apply**.
5. Compare the available OMIVV appliance version and current OMIVV appliance version.
6. To apply the update to the OMIVV appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
7. In the **UPDATE APPLIANCE** dialog box, click **Update**.
   After you click **Update**, you are logged out from the **OMIVV ADMINISTRATION CONSOLE** window.

   It may take approximately 40 minutes to complete the update depending on your network speed.
8. Close the web browser.
   Once the appliance upgrade is complete, ensure that you clear the browser cache before logging in to the **OMIVV ADMINISTRATION CONSOLE**.

Manage backup and restore

By using the Administration 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 39

In OMIVV, perform the following steps to access the **BACKUP AND RESTORE SETTINGS** page using 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. It is recommended that you 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 username.
   c. In **Password**, enter 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.

NFS requirements

The following settings are required for OMIVV while configuring NFS:

- Ensure that you have read and write permission to NFS.
- For Windows share, in the **NFS Advanced Sharing** window, do the following:
  - Select the **Allow Anonymous Access** and then set the UID and GID values to 91.
  - Select **Allow unmapped user Unix access**.

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 servers are not supported. Only the 12G and later servers are retained after restore.
- Hardware Profiles and Deployment Templates are not supported. It is recommended that you use 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.

Ensure that the correct deployment mode is configured before performing the restore operation. For more information about configuring the deployment mode, see Configure deployment mode on page 18.

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 restore operation causes the OMIVV appliance to reboot after restoration is complete. To verify the installation, see Verify installation on page 24 .

   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.

Upgrade OMIVV appliance using backup and restore

It is recommended that you do not 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: It is recommended that you retain the identity (IP or FQDN) of the earlier OMIVV appliance for the new OMIVV appliance.

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 17 and Upload HTTPS certificate on page 18. 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 24.
9. After the upgrade, it is recommended that you run 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.

   All the customization that is done on the registered Dell alarms and Dell health update provider for PHA cluster will be restored to default after you perform backup and restore.

   After backup and restore from an earlier OMIVV version to a later OMIVV version, perform the following tasks if you observe any of the following issues:
   - 200000 message
   - Dell EMC logo missing
   - OMIVV UI is not responding
   - OMIVV plugin is not removed from vCenter
   - SSL certificate is not valid

   Resolution:

   - 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-ui/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-ui\vc-packages\vsphere-client-serenity` folder in the vCenter appliance and see if the old data such as com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX exists.
     - 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).

   If the IP address for the new appliance is different from the IP address of the older appliance, perform the following:

   - 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.
   - Configure the trap destination for the SNMP traps to point to the new appliance. The identity change is fixed by running the inventory on these hosts. While running the inventory on 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.

4

Configure OMIVV appliance using 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.

You can also launch the initial configuration wizard using the following:

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

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

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 42.
- Configure events and alarms. For more information, see Configure events and alarms on page 44.
- Schedule inventory jobs. For more information, see Schedule inventory job on page 43.
- Schedule warranty retrieval job. For more information, see Schedule warranty retrieval jobs on page 44.

Topics:

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 42.

   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 enables the WBEM service and then disables after retrieving iDRAC IP 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 43.

b. Schedule warranty retrieval job. For more information about scheduling the warranty retrieval job, see Schedule warranty retrieval jobs on page 44.

   If you want to modify the inventory job schedule, go to **Settings** > **vCenter Settings** > **Data Retrieval Schedule** > **Inventory Retrieval** or **Jobs** > **Inventory** > **Hosts Inventory**.

   If you want to modify the warranty retrieval job schedule, go to **Settings** > **vCenter Settings** > **Data Retrieval Schedule** > **Warranty Retrieval** or **Jobs** > **Warranty**.

c. Configure events and alarms. For information about configuring events and alarms, see Configure events and alarms on page 44.

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**.

   It is recommended that you associate 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, 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 **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.
   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 username in the **User Name** box. The username is limited to 16 characters.

          For information about defining username, see the *iDRAC User's Guide* available at **https://www.dell.com/support**.

        - Enter password.

          For more information about the recommended characters in username and passwords, see the *iDRAC User's Guide* available at **https://www.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 Operating System (OS).

        - Enter the username in the **Active Directory User Name** box.

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

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

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

The default username is root.

- To enter the local host credentials, perform the following:
  - Enter password.

    Host password is required only for hosts running ESXi 6.5 U3 and earlier versions.

    To skip this step for ESXi 6.7 and later versions, ensure that the **Use Host Credentials** check box is cleared. If password is entered for host running ESXi 6.7 and later, the password is ignored.

    For hosts running ESXi 6.7 and later versions, it is not required to enter the ESXi credentials. OMIVV can pair the iDRAC with its ESXi host even if incorrect host credentials are entered.
- To enter the credentials for hosts that are already configured and enabled for AD, select the **Use Active Directory** check box.
  - Enter the username in the **Active Directory User Name** box. Enter the username in one of the formats such as `domain\username` or `username@domain`. The username is limited to 256 characters. See the **Microsoft Active Directory Documentation** for username restrictions.
  - Enter password.
- To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.

5. Click **Next**.
   The **Select Hosts** page is displayed.
6. On the **Select Hosts** page, expand the tree view and select the hosts, and then click **OK**.
   - To add or remove hosts from the **Associated Hosts** page, click **ADD HOST**

     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**.

   It is recommended that you test the connection for all configured hosts.

   During test connection, OMIVV enables the WBEM service and then disables after retrieving iDRAC IP for hosts running ESXi 6.5 and later.

   NOTE: After you enter 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.
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. It is recommended that you run 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** > **Inventory 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. To update authorization key, ensure that you have access to index catalog (`https://downloads.dell.com/catalog/CatalogIndex.gz`).
2. To get warranty report, ensure that you have access to `https://apigtwb2c.us.dell.com`.
3. Ensure that the inventory is run successfully on hosts and chassis.
4. 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, it is recommended that you use 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. It is recommended that you select 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. It is recommended that you check 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 operating system deployment is complete.

After the operating system 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 username and password. The default username is **root** and password is **calvin**.
   Ensure that you enter the password based as per iDRAC user password policy set in iDRAC. Also, ensure to use iDRAC supported characters.
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** > **Override Severity for Proactive HA**.
   The data grid displays all the supported Proactive HA events. The data grid columns include columns such as 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**.

A

Accessing documents from the Dell EMC support site

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

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

Using search engines:

- Type the name and version of the document in the search box.

B

Related Documentation

In addition to this guide, you can access the other guides available at **https://www.dell.com/support**. Click **Browse all products**, then click **Software** > **Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 5.2** to access the following documents:

- *OpenManage Integration for VMware vCenter Version 5.2 User's Guide*
- *OpenManage Integration for VMware vCenter Version 5.2 Release Notes*
- *OpenManage Integration for VMware vCenter Version 5.2 Compatibility Matrix*

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

C

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.