Emulex® OneCommand® Manager for VMware vCenter 6.7 and Later

User Guide
Release 12.4

OCM-VM-HTML-UG124-100
August 27, 2019

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Chapter 1: Introduction

Emulex® OneCommand® Manager for VMware vCenter 6.7 and Later is a management utility for Emulex host bus adapters (HBAs) that provides status monitoring and online maintenance capability for Emulex adapters in VMware vCenter 6.7 environments.

Emulex OneCommand Manager for VMware vCenter 6.7 and Later performs the following functions:

- Discovers adapters on ESXi servers registered to a VMware vCenter 6.7 system.
- Displays adapter attributes.
- Displays adapter port attributes.
- Displays adapter port statistics.
- Displays ESXi host information.
- Upgrades adapter firmware.
- Resets ports.
- Generates and captures diagnostic dumps.
- Modifies diagnostic dump settings.

NOTE: OneCommand Manager for VMware vCenter 6.7 and Later does not have full management capability. For full management capability, use the `elxvcpcmd` CLI (plug-in server path: `C:\Program Files\Emulex\OCM for VMware`), or the `esxcli` utility.

1.1 Compatibility

OneCommand Manager for VMware vCenter 6.7 and Later:

- Requires the HTML5 vCenter client.
- Supports the following Windows operating systems:
  - Windows 10
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

For supported versions of operating systems, platforms, and adapters, go to www.broadcom.com.

1.2 Abbreviations

CA	certificate authority
CIM	Common Interface Model
CLI	command line interface
CRC	cyclic redundancy check
CSR	certificate signing request
DNS	domain name system or domain name server
FC	Fibre Channel
GUI	graphical user interface
HBA	host bus adapter
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
IP	Internet Protocol
JEDEC ID	Joint Electron Device Engineering Council identification code
KB	Kilobyte (1024 bytes)
LIP	Loop Initialization Primitive
NOS	network operating system
OS	operating system
Rx	receive
SLI®	Service Level Interface
SSL	Secure Sockets Layer
Tx	transmit
URL	Uniform Resource Locator
vCSA	VMware for vCenter Server Appliance
WWN	World Wide Name

Chapter 2: Installing, Enabling, and Upgrading OneCommand Manager for VMware vCenter 6.7 and Later

OneCommand Manager for VMware vCenter 6.7 and Later provides real-time management as a plug-in through VMware vCenter.

NOTE: System performance is directly influenced by the speed and efficiency of the underlying network infrastructure.

2.1 Hardware Requirements

- Physical or virtual (x86 or x86_64) servers with a minimum RAM of 2 GB and 250 GB of disk space.

2.2 Software Requirements

- Operating system – Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

NOTE: On the system where OneCommand Manager for VMware vCenter 6.7 and Later is installed, make sure that the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter 6.7 Server only. No other service should be listening on this port.

- Emulex CIM Provider Package version 12.x.
- ESXi host (containing the FC HBA cards to be managed) version 12.x.

NOTE: Version 12.x packages are not compatible with the 11.1 or earlier versions of Emulex software.

- Driver and firmware requirements.

  Go to www.broadcom.com for the latest compatible driver and firmware versions.

2.3 Installing OneCommand Manager for VMware vCenter 6.7 and Later

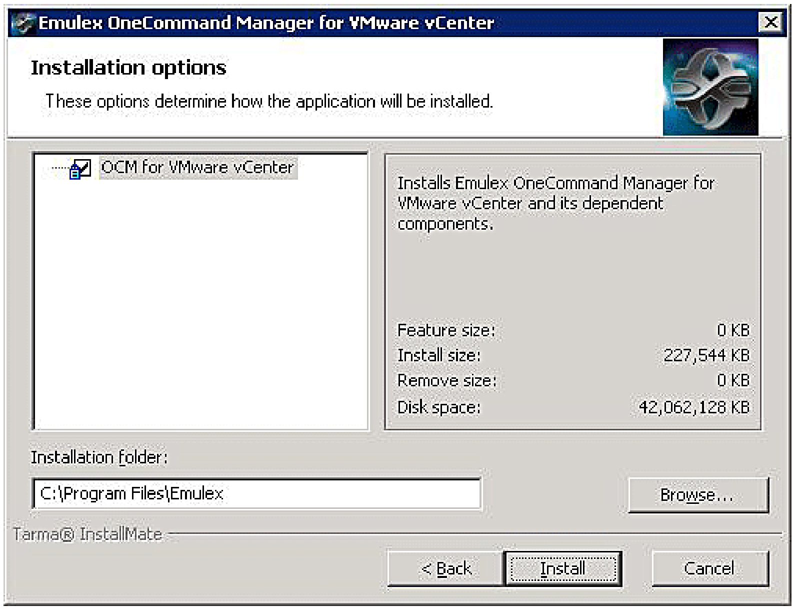
The Emulex CIM Provider must be installed on your ESXi host before installing OneCommand Manager for VMware vCenter 6.7 and Later. For more information on installing the CIM Provider, refer to the *CIM Provider Package Installation Guide* available on www.broadcom.com.

To install OneCommand Manager for VMware vCenter 6.7 and Later in Windows, perform these steps:

1. Go to www.broadcom.com to download the `ELXOCM-VMware-vCenter-<version>-Setup.exe` installation file to your system.
2. Navigate to the system directory to which you downloaded the file.
3. Double-click **ELXOCM-VMware-vCenter-<*version*>-Setup.exe**.

   The **OneCommand Manager for VMware vCenter** window appears.
4. Click **Next**. The **Installation options** window with the default installation folder appears (Figure 1).

Figure 1: Installation options Window



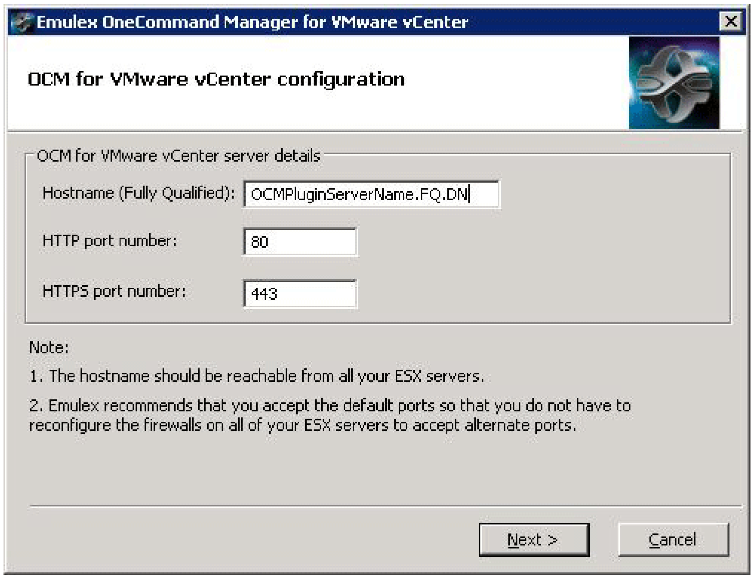
Emulex OneCommand Manager for VMware vCenter
Installation options
These options determine how the application will be installed.
OCM for VMware vCenter
Installs Emulex OneCommand Manager for VMware vCenter and its dependent components.
Feature size: 0 KB
Install size: 227,544 KB
Remove size: 0 KB
Disk space: 42,062,128 KB
Installation folder:
C:\Program Files\Emulex
Browse...
Tarma® InstallMate
< Back
Install
Cancel

5. Ensure that **OCM for VMware vCenter** is selected.

6. Program files install by default to `C:\Program Files\Emulex`. To change this location, click **Browse** and navigate to where you want the program files to reside.

7. Click **Install**. The **Operation in progress** dialog appears. When the process is complete, the **OCM for VMware vCenter configuration** window appears (Figure 2).

Figure 2: OCM for VMware vCenter configuration Window



Emulex OneCommand Manager for VMware vCenter
OCM for VMware vCenter configuration
OCM for VMware vCenter server details
Next >
Cancel

Hostname (Fully Qualified): OCMPluginServerName.FQ.DN

HTTP port number: 80

HTTPS port number: 443

Note:

1. The hostname should be reachable from all your ESX servers.

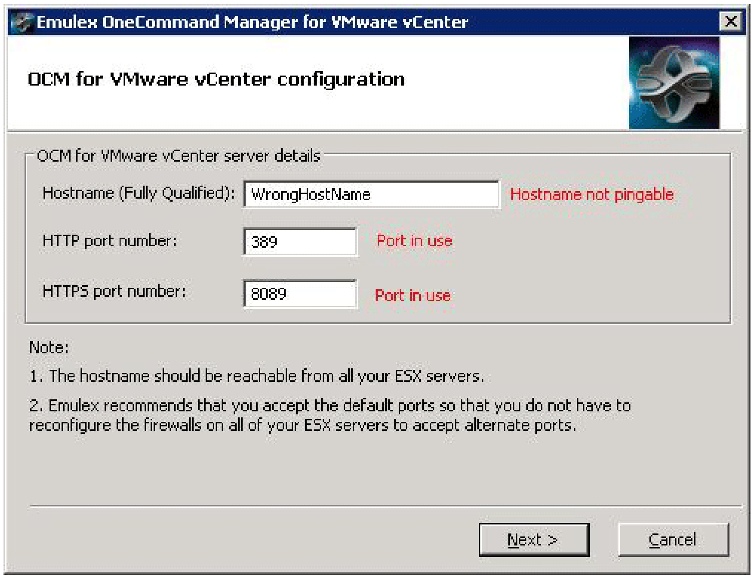
2. Emulex recommends that you accept the default ports so that you do not have to reconfigure the firewalls on all of your ESX servers to accept alternate ports.

Default port numbers for OneCommand Manager for VMware vCenter 6.7 Server are displayed.

NOTE: The Windows firewall setting must allow incoming connections on the HTTP and HTTPS ports that you configure here.

If the port numbers are already in use, a popup appears next to the port number (Figure 3).

Figure 3: OCM for VMware vCenter configuration Window with Port in use Popup



Emulex OneCommand Manager for VMware vCenter

OCM for VMware vCenter configuration

OCM for VMware vCenter server details

Hostname (Fully Qualified): WrongHostName Hostname not pingable

HTTP port number: 389 Port in use

HTTPS port number: 8089 Port in use

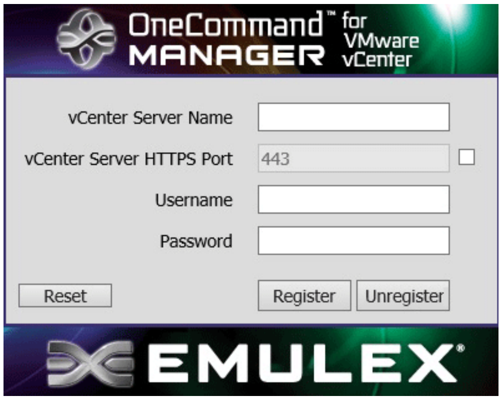
Note:

1. The hostname should be reachable from all your ESX servers.

2. Emulex recommends that you accept the default ports so that you do not have to reconfigure the firewalls on all of your ESX servers to accept alternate ports.

8. Click **Next**. The **Operation in progress** dialog appears. When the installation process is complete, a message prompts you to launch the registration utility.
9. Click **Yes**. A registration dialog appears in a new browser window (Figure 4).

Figure 4: registration Dialog



vCenter Server Name

vCenter Server HTTPS Port 443 □

Username

Password

10. Enter the following details of the vCenter Server:
    - **vCenter Server Name** – The IP address of the vCenter Server.
    - **vCenter Server HTTPS Port** – The HTTPS port number of the vCenter Server.

NOTE: The vCenter Server HTTPS port is 443 by default. You can change this value if you have configured a different HTTPS port while installing the vCenter.

- **Username** – The user name with required privileges.
- **Password** – The user password.

11. Click **Register** to register OneCommand Manager for VMware vCenter 6.7 and Later with a new vCenter Server.

NOTE:

- You can unregister an existing OneCommand Manager for VMware vCenter 6.7 and Later by clicking **Unregister**.
- If you change the host name of the machine that hosts the vCenter Server, you must re-install the vCenter Server and re-register.

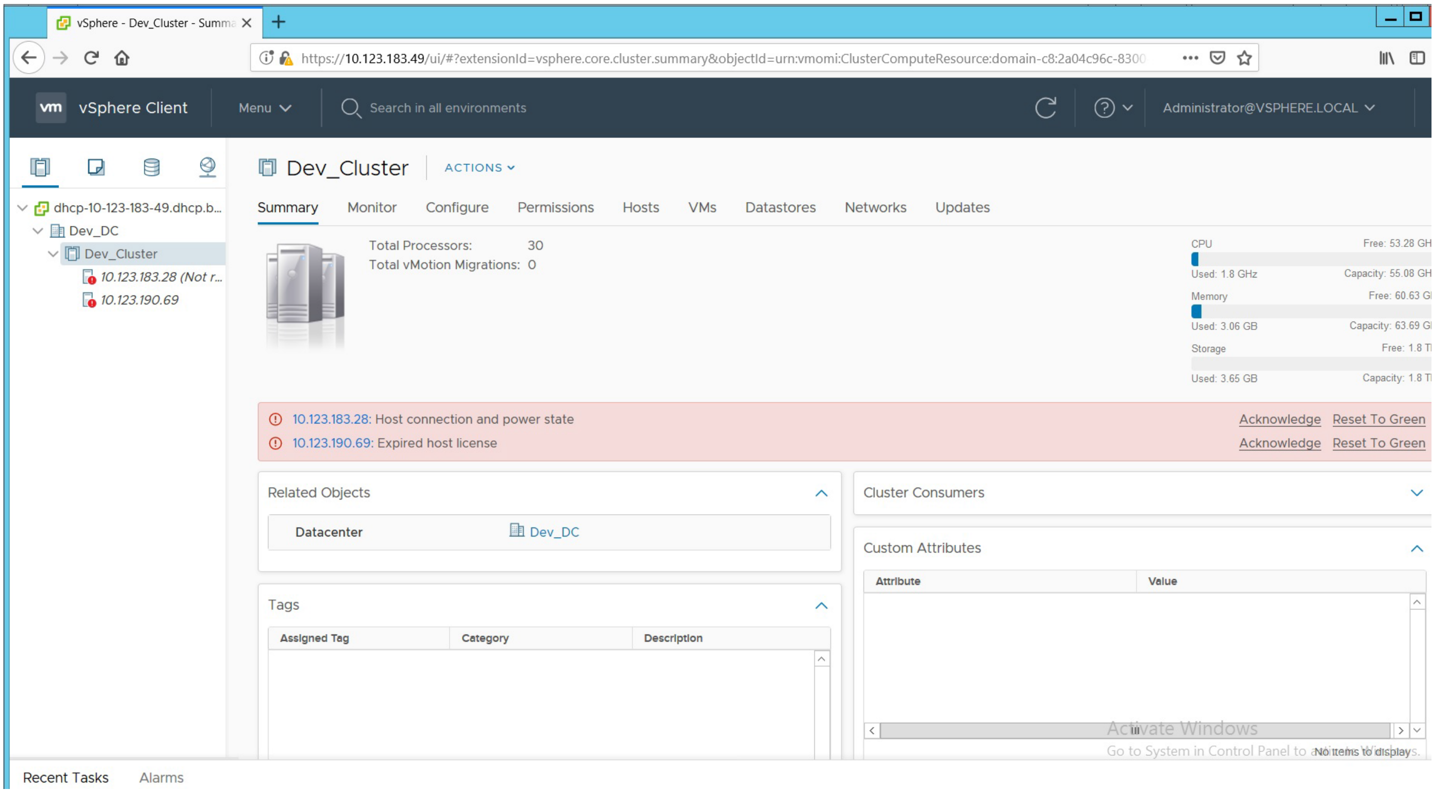
12. When the operation is successful, a message is displayed. Click **OK**.
13. Close the browser window. The **Installation completed** window appears.
14. Click **Finish**. The **OneCommand Manager for VMware vCenter 6.7 and Later Registration** icon is created on the desktop. You do not need to reboot the system.

2.3.1 Verifying the Installation of the OneCommand Manager for VMware vCenter 6.7 and Later

To verify the OneCommand Manager for VMware vCenter 6.7 and Later installation, perform these steps:

1. Launch a Web browser and enter the IP address of the vCSA.
2. Select **vCenter client HTML5**.
3. Enter the credentials for the vCSA. The vCenter client window displays all hosts managed by the vCSA (Figure 5).

Figure 5: VMware vCenter Client Window



https://10.123.183.49/ui/#?extensionId=vsphere.core.cluster.summary&objectId=urn:vmomi:ClusterComputeResource:domain-c8:2a04c96c-8300

Total Processors: 30
Total vMotion Migrations: 0

CPU Free: 53.28 GH
Used: 1.8 GHz Capacity: 55.08 GH
Memory Free: 60.63 GI
Used: 3.06 GB Capacity: 63.69 GI
Storage Free: 1.8 TI
Used: 3.65 GB Capacity: 1.8 TI

10.123.183.28: Host connection and power state
10.123.190.69: Expired host license

Datacenter	Dev_DC

Assigned Tag	Category	Description

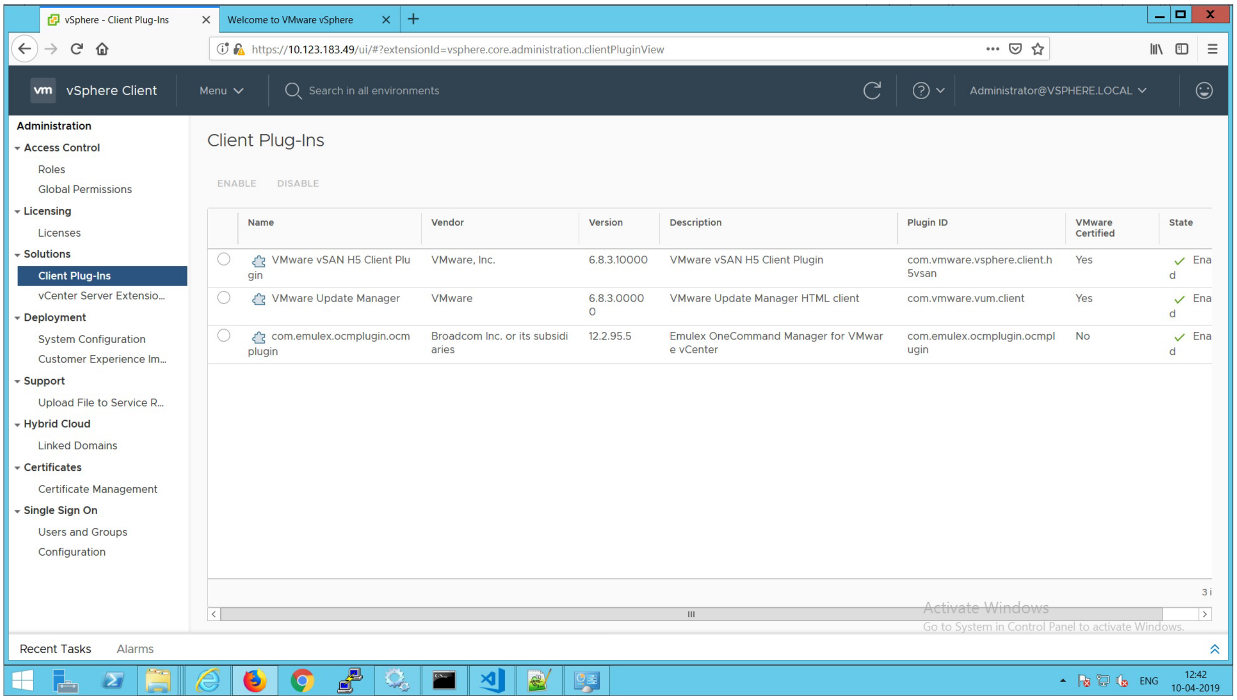
Attribute	Value

No items to display

4. From the vCenter client window **Menu**, select **Administration**.

5. From the window’s left panel, select **Client Plug-ins** (Figure 6).

Figure 6: vCenter Client Plug-In Window



	Name	Vendor	Version	Description	Plugin ID	VMware Certified	State
○	VMware vSAN H5 Client Plugin	VMware, Inc.	6.8.3.10000	VMware vSAN H5 Client Plugin	com.vmware.vsphere.client.h5vsan	Yes	✓ Ena d
○	VMware Update Manager	VMware	6.8.3.00000	VMware Update Manager HTML client	com.vmware.vum.client	Yes	✓ Ena d
○	com.emulex.ocmplugin.ocmplugin	Broadcom Inc. or its subsidiaries	12.2.95.5	Emulex OneCommand Manager for VMware vCenter	com.emulex.ocmplugin.ocmplugin	No	✓ Ena d

6. In the **Plug-in Manager** window, note the status of OneCommand Manager for VMware vCenter 6.7 and Later (Emulex OneCommand). If the OneCommand Manager for VMware vCenter 6.7 and Later installation is complete, the status of Emulex OneCommand is enabled by default.

2.4 Enabling ESXi Management

This section describes enabling OneCommand Manager for VMware vCenter 6.7 and Later.

NOTE: Refer to the VMware vCenter guide on the VMware website for information on creating a user with required privileges and changing access permissions for a user in the Active Directory.

2.4.1 Requirements

Only a user with these specific privileges can read and perform active management in OneCommand Manager for VMware vCenter 6.7 and Later:

- **Extension.Register extension** to register OneCommand Manager for VMware vCenter 6.7 and Later using the registration utility.
- **Extension.Unregister extension** to unregister OneCommand Manager for VMware vCenter 6.7 and Later using the registration utility.
- **Host.CIM.CIM Interaction** to read and manage data through the OneCommand Manager for VMware vCenter 6.7 and Later.

All other users, including the root user, of the ESXi host cannot perform any actions including reading data. If a user without the required privileges attempts to perform an action in OneCommand Manager for VMware vCenter 6.7 and Later, an error message is displayed.

NOTE: To configure user roles and assign privileges, refer to the *VMware vCenter Server Guide* on the VMware website.

2.4.2 Lockdown Mode Feature

Refer to the vCenter guide on the VMware website for information on enabling and disabling lockdown mode.

If lockdown mode is enabled for an ESXi host, only a user with the required privileges can access the ESXi host and manage adapters using OneCommand Manager for VMware vCenter 6.7 and Later. All other users, including the root user, do not have access to the ESXi host.

2.4.3 Enabling or Disabling OneCommand Manager for VMware vCenter 6.7 and Later

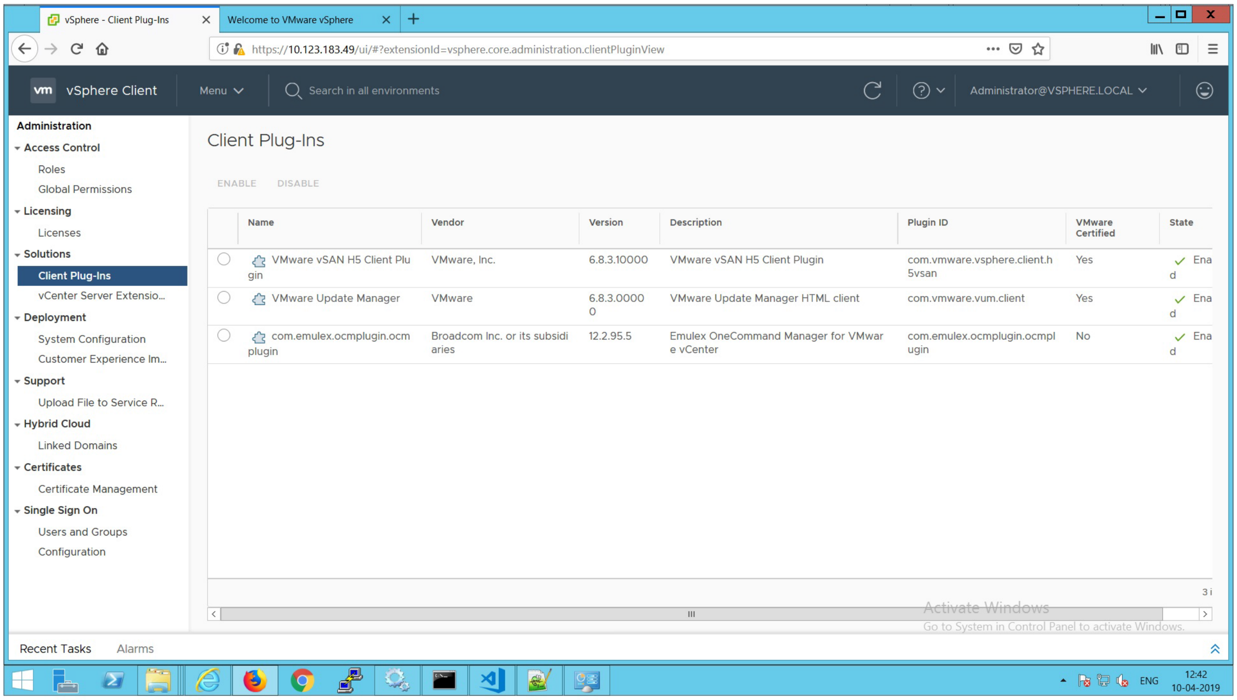
OneCommand Manager for VMware vCenter 6.7 and Later can be enabled or disabled from the Plug-In Management section.

NOTE: You must have sufficient privileges to access the Plug-In Management section. Refer to the VMware documentation for information on configuring users and privileges.

To enable OneCommand Manager for VMware vCenter 6.7 and Later, perform these steps:

1. From the vCenter client window **Menu**, select **Administration**.
2. From the window's left panel, select **Client Plug-ins** (Figure 7).

Figure 7: vCenter Client Plug-Ins Window



Client Plug-Ins

	Name	Vendor	Version	Description	Plugin ID	VMware Certified	State
○	VMware vSAN H5 Client Plugin	VMware, Inc.	6.8.3.10000	VMware vSAN H5 Client Plugin	com.vmware.vsphere.client.h5vsan	Yes	✓ Ena d
○	VMware Update Manager	VMware	6.8.3.00000	VMware Update Manager HTML client	com.vmware.vum.client	Yes	✓ Ena d
○	com.emulex.ocmplugin.ocmplugin	Broadcom Inc. or its subsidiaries	12.2.95.5	Emulex OneCommand Manager for VMware vCenter	com.emulex.ocmplugin.ocmplugin	No	✓ Ena d

3 i

3. Select the **Emulex OneCommand Manager for VMware vCenter** radio button.
4. Select **Enable** or **Disable**.

2.5 Registering and Unregistering OneCommand Manager for VMware vCenter 6.7 and Later

OneCommand Manager for VMware vCenter 6.7 and Later can be registered with more than one vCenter Server.

To register or unregister OneCommand Manager for VMware vCenter 6.7 and Later with a new vCenter Server, perform these steps:

1. Double-click the **OCM for VMware vCenter Registration** icon on the desktop. This icon is created when OneCommand Manager for VMware vCenter 6.7 and Later is successfully installed. The **Register/Unregister** dialog is displayed (Figure 4).
2. Enter the following details of the vCenter Server:
   - **vCenter Server Name** – The IP address of the vCenter Server.
   - **vCenter Server HTTPS Port** – The HTTPS port number of the vCenter Server.

NOTE: The vCenter Server HTTPS port is 443 by default. Change this value if you configured a different HTTPS port when you installed the vCenter Server.

   - **Username** – The user name with required privileges.
   - **Password** – The user password.

3. Do one of the following:
   - Click **Register** to register OneCommand Manager for VMware vCenter 6.7 and Later with a new vCenter Server.

   or

   - Click **Unregister** to unregister an existing OneCommand Manager for VMware vCenter 6.7 and Later with a vCenter Server.

NOTE:

- If you change the host name of the machine hosting the vCenter Server, you must reinstall the vCenter Server and re-register.
- If the vCenter Server is already registered with another instance of OneCommand Manager for VMware server, it is replaced with this server instance.

When the operation is successful, a message is displayed.

4. Click **OK** and close the window.

2.6 Uninstalling OneCommand Manager for VMware vCenter 6.7 and Later

Before you uninstall OneCommand Manager for VMware vCenter 6.7 and Later, you must unregister it from the vCenter Server. For more information, see Section 2.5, Registering and Unregistering OneCommand Manager for VMware vCenter 6.7 and Later.

CAUTION! When you uninstall OneCommand Manager for VMware vCenter 6.7 and Later, ensure that you do not delete the default configuration and log files that are stored in the `%TEMP%\Emulex\OCM for VMware` directory. If these files are deleted, all historical information of active management performed from the host is permanently lost.

To uninstall OneCommand Manager for VMware vCenter 6.7 and Later in a Windows system, perform these steps:

1. Navigate to the system directory to which you downloaded the `ELXOCM-VMware-vCenter-<`*`version`*`>-Setup.exe` file.
2. Double-click the `ELXOCM-VMware-vCenter-<`*`version`*`>-Setup.exe` file. The OneCommand Manager for VMware vCenter window prompts you to reinstall or uninstall the application. Select **Uninstall the application completely** and click **Next**. A progress window is displayed. A window indicating the detection of OneCommand Manager for VMware vCenter 6.7 and Later appears.
3. Click **OK**.

   When uninstallation is complete, the **Uninstallation Completed** window is displayed.
4. Click **Finish**. You do not need to reboot the system.

NOTE: You can also uninstall the OneCommand Manager application from the **Programs and Features** window.

2.7 Upgrading or Reinstalling OneCommand Manager for VMware vCenter 6.7 and Later

To upgrade or reinstall OneCommand Manager for VMware vCenter 6.7 and Later in a Windows system, perform these steps:

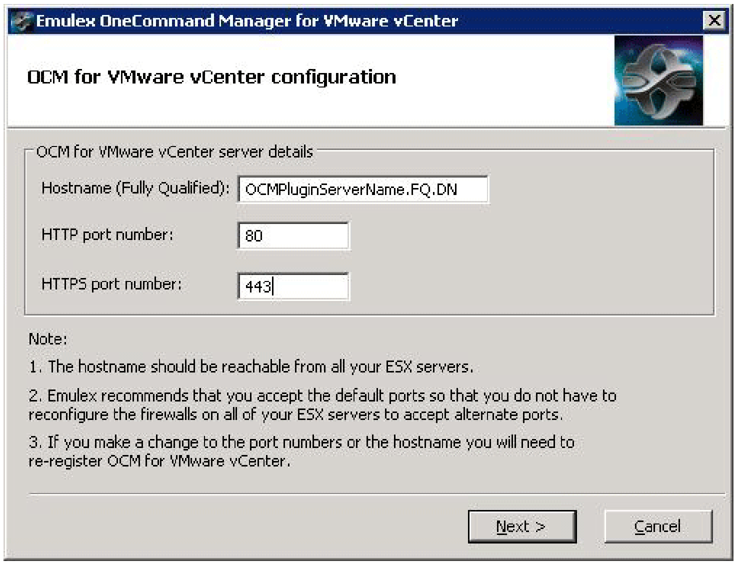
1. Navigate to the system directory to which you downloaded the `ELXOCM-VMware-vCenter-<`*`version`*`>-Setup.exe` file.
2. Double-click `ELXOCM-VMware-vCenter-<`*`version`*`>-Setup.exe`.

   The **OneCommand Manager for VMware vCenter** window prompts you to upgrade\reinstall or uninstall the application.
3. Select **Upgrade\Re-install the application** and click **Next**.

   The **Installation Options** window with the previous installation folder location appears (Figure 1).
4. Ensure that **OCM for VMware vCenter** is selected.
5. To change the installation folder location, click **Browse** and navigate to where you want the program files to reside.
6. Click **Install** on the **Installation Options** window.

   The **operation in progress** window appears. When the installation process is complete, the **OneCommand Manager for VMware vCenter configuration** window appears (Figure 8).

Figure 8: Reinstallation Configuration Dialog



Emulex OneCommand Manager for VMware vCenter

OCM for VMware vCenter configuration

OCM for VMware vCenter server details

Hostname (Fully Qualified): OCMPluginServerName.FQ.DN

HTTP port number: 80

HTTPS port number: 443

Note:

1. The hostname should be reachable from all your ESX servers.

2. Emulex recommends that you accept the default ports so that you do not have to reconfigure the firewalls on all of your ESX servers to accept alternate ports.

3. If you make a change to the port numbers or the hostname you will need to re-register OCM for VMware vCenter.

If OneCommand Manager for VMware vCenter 6.7 and Later was installed earlier with port numbers other than the defaults provided, those configured ports are shown. If the port numbers are already in use, a popup appears next to the port number.

NOTE: The Windows firewall setting must allow incoming connections on the HTTP and HTTPS ports that you configure here.

7. Follow the instructions and complete the installation with steps 8 to 13 of Section 2.3, Installing OneCommand Manager for VMware vCenter 6.7 and Later.

Chapter 3: Using OneCommand Manager for VMware vCenter 6.7 and Later

OneCommand Manager for VMware vCenter 6.7 and Later is available at the host level.

3.1 Viewing the OneCommand Manager for VMware vCenter 6.7 and Later

After you are logged on to the VMware vCenter Server, the OneCommand Manager for VMware vCenter 6.7 and Later is under the **Configure** tab for a particular host that you select in the client.

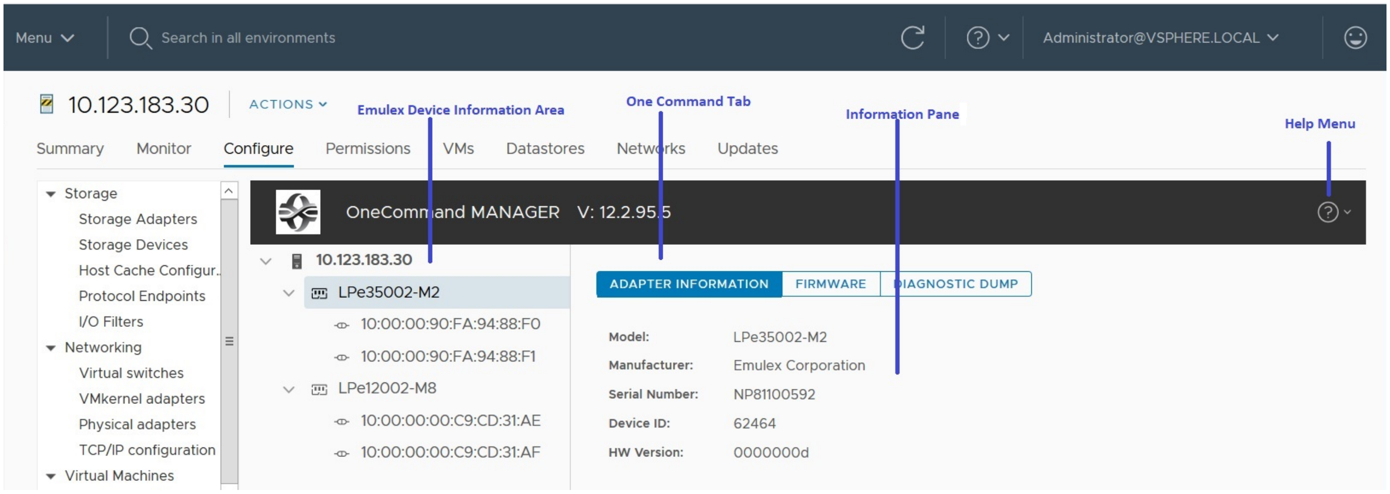
To launch the OneCommand Manager for VMware vCenter 6.7 and Later, perform these steps:

1. Log on to the vCenter Server. The home page is displayed.
2. Navigate to an ESXi host in the **Navigation** pane.
3. From the Host level view, select the host that you want to display.
4. Go to the **Configure** tab to access the OneCommand Manager for VMware vCenter 6.7 and Later.

3.2 Window Elements of OneCommand Manager for VMware vCenter 6.7 and Later

The window for OneCommand Manager for VMware vCenter 6.7 and Later (Figure 9) contains four basic components:

Figure 9: Host View with Callouts



Model: LPe35002-M2
Manufacturer: Emulex Corporation
Serial Number: NP81100592
Device ID: 62464
HW Version: 0000000d

3.2.1 Emulex Device Management Area

The **Emulex Device Management** area is a discovery-tree with icons that represent discovered hosts, adapters, and ports.

3.2.2 OneCommand Tabs

In a host view, the **OneCommand** tabs display configuration, statistical, and status information for network elements.

3.2.3 Information Pane

The information pane displays information based upon the OneCommand tab that is selected.

3.2.4 Help Menu

- **Help** – Click to load the complete indexed online help for OneCommand Manager for VMware vCenter 6.7 and Later. You can search for information for all OneCommand Manager for VMware vCenter 6.7 and Later tabs and functions.
- **About** – Click to display the version of OneCommand Manager for VMware vCenter 6.7 and Later.

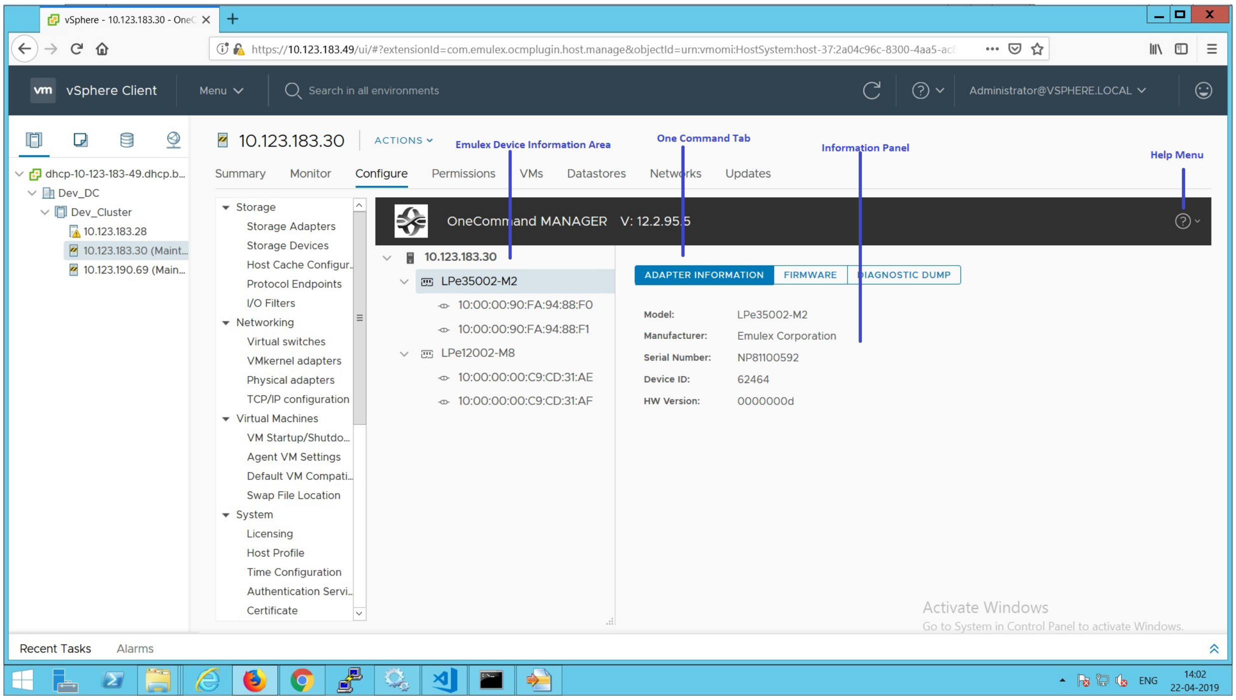
Chapter 4: Viewing Host, Adapter, and Port Information

This chapter explains how to view host, adapter, and port information and how to reset a port.

4.1 Viewing Host Information

To view host information for a single host, select a host in the console tree-view and select the **Emulex OneCommand** tab. The selected host's information appears (Figure 10).

Figure 10: Information for a Single Host



Model: LPe35002-M2
Manufacturer: Emulex Corporation
Serial Number: NP81100592
Device ID: 62464
HW Version: 0000000d

The following host information fields are displayed:

- **Host Name** – The host identifier.
- **Number of Adapters** – The number of adapters installed in the host.
- **Number of Fabrics** – The number of fabrics to which the host is connected.
- **Operating System** – The operating system and version installed on the selected host.
- **Lock Down Mode** – Indicates whether lockdown mode is enabled or disabled.
- **IP Address** – The IP address of the host.
- **Number of Ports** – The number of discovered physical ports that can be managed by this host.
- **Number of Target Ports** – The number of targets discovered across the ports.
- **CIM Provider Version** – The versions of the Emulex CIM Providers that are running on the ESXi host.

4.2 Viewing Adapter and Port Information

This section describes the available adapter and port information, and the procedure for resetting a port.

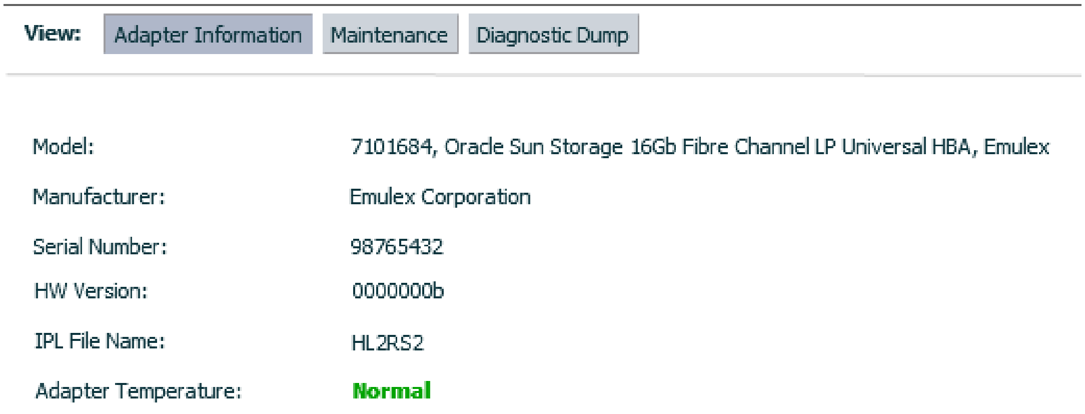
4.2.1 Viewing Adapter Information

When you select an adapter from the Emulex Device Management tree-view, the **Adapter Information** tab displays general attributes associated with the selected adapter.

To view information for an adapter, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select an adapter. The **Adapter Information** tab is displayed (Figure 11).

Figure 11: Adapter Information Tab



Model:	7101684, Oracle Sun Storage 16Gb Fibre Channel LP Universal HBA, Emulex
Manufacturer:	Emulex Corporation
Serial Number:	98765432
HW Version:	0000000b
IPL File Name:	HL2RS2
Adapter Temperature:	Normal

The following **Adapter Information** tab fields are displayed:

- **Model** – The complete model name of the adapter.
- **Manufacturer** – The manufacturer of the adapter.
- **Serial Number** – The manufacturer's serial number for the selected adapter.
- **HW Version** – This field displays the JEDEC ID.
- **IPL File Name** – The name of the IPL file.
- **Adapter Temperature** – This field displays the following adapter temperature information:
  - **Normal**: The adapter’s temperature is within normal operational range.
  - **Exceeded operational range – Critical**: The adapter’s temperature is beyond normal operational range. If the temperature continues to increase, the adapter will shut down. You must determine the cause of the temperature issue and fix it immediately. Check for system cooling issues. Common causes of system cooling issues include clogged air filters, inoperative fans, and air conditioning issues that cause high ambient air temperatures.
  - **Exceeded operational range – Adapter stopped**: The temperature has reached the critical limit, forcing the adapter to shut down. You must determine the cause of the temperature issue and fix it before resuming operation. Check for system cooling issues. Common causes of system cooling issues include clogged air filters, inoperative fans, and air conditioning issues that cause high ambient air temperatures.
  - **Not Supported**: The adapter temperature is not available.

After the system overheating issue is resolved and the adapter has cooled down, reboot the system or, if the system supports hot swapping, cycle the power of the adapter slot.

4.2.2 Viewing Port Details

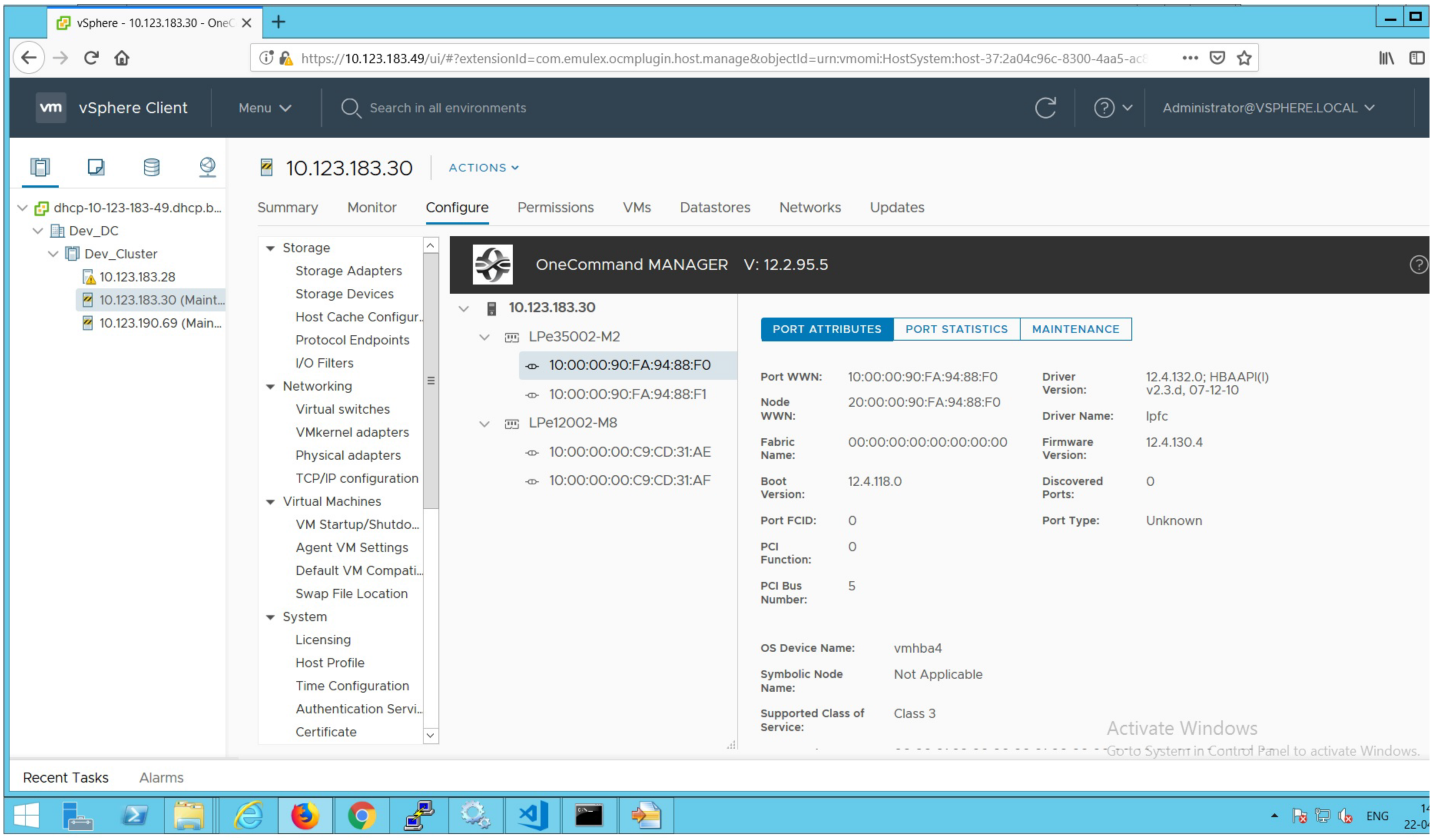
When you select an port from the Emulex Device Management tree-view, the **Port Details** tab contains general attributes associated with the selected port.

To view details for an port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the port whose information you want to view.

   The **Port Details** tab is displayed (Figure 12).

Figure 12: Port Details Tab



Port WWN: 10:00:00:90:FA:94:88:F0
Node WWN: 20:00:00:90:FA:94:88:F0
Fabric Name: 00:00:00:00:00:00:00:00
Boot Version: 12.4.118.0
Port FCID: 0
PCI Function: 0
PCI Bus Number: 5
Driver Version: 12.4.132.0; HBAAPI(I) v2.3.d, 07-12-10
Driver Name: lpfc
Firmware Version: 12.4.130.4
Discovered Ports: 0
Port Type: Unknown
OS Device Name: vmhba4
Symbolic Node Name: Not Applicable
Supported Class of Service: Class 3

The following **Port Details** tab fields are displayed:

- **Port Attributes** area:
  - **Port WWN** – The port World Wide Name of the selected adapter.
  - **Node WWN** – The node World Wide Name of the selected adapter.
  - **Fabric Name** – The 64-bit worldwide unique identifier assigned to the fabric.
  - **Boot Version** – The version of boot code installed on the selected adapter port. If the boot code is disabled, the field displays **Disabled**.

  - **Port FCID** – The FC ID of the selected adapter port.
  - **PCI Function** – The PCI function number of the selected port.
  - **PCI Bus Number** – The PCI bus number.
  - **Driver Version** – The version of the driver installed for the adapter.
  - **Driver Name** – The executable file image name for the driver as it appears in the Emulex driver download package.
  - **Firmware Version** – The version of Emulex firmware currently active on the adapter port.
  - **Discovered Ports** – The number of ports that were discovered.
  - **Port Type** – The type of port that was discovered.
  - **OS Device Name** – The platform-specific name by which the selected adapter is known to the operating system.
  - **Symbolic Node Name** – The FC name used to register the driver with the name server.
  - **Supported Class of Service** – A frame delivery scheme exhibiting a set of delivery characteristics and attributes. There are three classes of service.
    - **Class 1**– Provides a dedicated connection between a pair of ports with confirmed delivery or notification of non-delivery.
    - **Class 2** – Provides a frame switched service with confirmed delivery or notification of non-delivery.
    - **Class 3** – Provides a frame switched service similar to Class 2, but without notification of frame delivery or non-delivery.
- **Supported FC4 Types** – A 256-bit (8-word) map of the FC-4 protocol types supported by the port containing the selected adapter.
- **Port Status** area:
  - **Link Status** – This field indicates the status of the link on the selected adapter port.
- **Port Speed** area:
  - **Port Speed** – The current port speed of the selected adapter port.

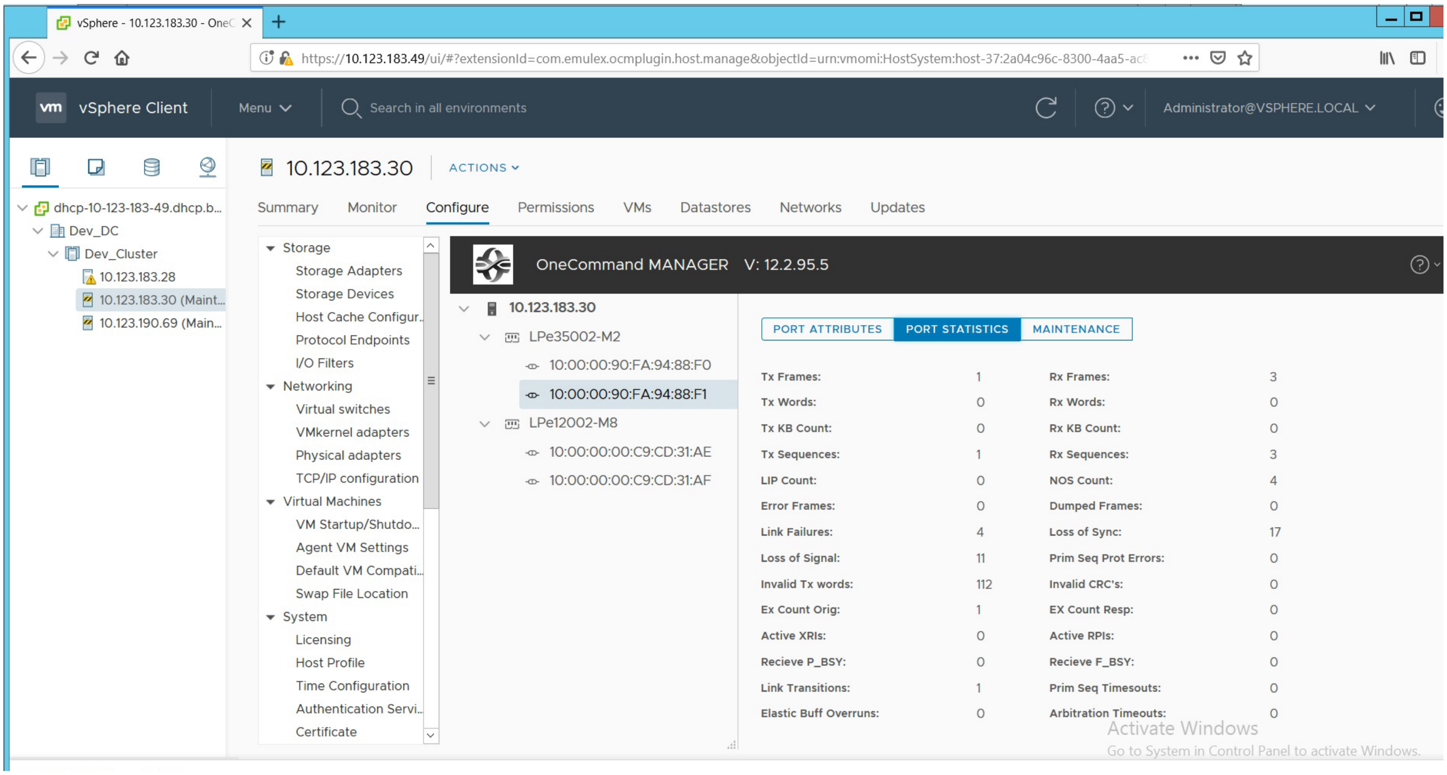
4.2.3 Viewing Port Statistics

When you select a port from the discovery-tree, the **Port Statistics** tab displays cumulative totals for error events and statistics on the port. Some statistics are cleared when the adapter is reset.

To view statistics for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the port whose statistics that you want to view.
3. Select the **Statistics** tab (Figure 13).

Figure 13: Port Statistics Tab



Tx Frames:	1	Rx Frames:	3
Tx Words:	0	Rx Words:	0
Tx KB Count:	0	Rx KB Count:	0
Tx Sequences:	1	Rx Sequences:	3
LIP Count:	0	NOS Count:	4
Error Frames:	0	Dumped Frames:	0
Link Failures:	4	Loss of Sync:	17
Loss of Signal:	11	Prim Seq Prot Errors:	0
Invalid Tx words:	112	Invalid CRC's:	0
Ex Count Orig:	1	EX Count Resp:	0
Active XRIs:	0	Active RPIs:	0
Recieve P_BSY:	0	Recieve F_BSY:	0
Link Transitions:	1	Prim Seq Timeouts:	0
Elastic Buff Overruns:	0	Arbitration Timeouts:	0

The following **Port Statistics** tab fields are displayed:

- **Tx Frames** – The FC frames transmitted by this adapter port.
- **Tx Words** – The FC words transmitted by this adapter port.
- **Tx KB Count** – The FC kilobytes transmitted by this adapter port.
- **Tx Sequences** – The FC sequences transmitted by this adapter port.
- **LIP Count** – The number of LIP events that have occurred for the port. This field is supported only if the topology is arbitrated loop.

  Loop initialization consists of the following:

  - Temporarily suspending loop operations.
  - Determining whether loop capable ports are connected to the loop.
  - Assigning AL_PA IDs.
  - Providing notification of configuration changes and loop failures.
  - Placing loop ports in the monitoring state.
- **Error Frames** – The number of frames received with CRC errors.
- **Link Failures** – The number of times the link has failed. A link failure can cause a timeout.
- **Loss of Signal** – The number of times the signal was lost.
- **Invalid Tx Words** – The total number of invalid words transmitted by this adapter port.
- **Ex Count Orig** – The number of FC exchanges originating on this port.
- **Active XRIs** – The number of active exchange resource indicators.
- **Received P_BSY** – The number of FC port-busy link response frames received.
- **Link Transitions** – The number of times the SLI port sent a link attention condition.
- **Elastic Buff Overruns** – The number of times the link interface has had its elastic buffer overrun.
- **Rx Frames** – The number of FC frames received by this adapter port.

- **Rx Words** – The number of FC words received by this adapter port.
- **Rx KB Count** – The received kilobyte count by this adapter port.
- **Rx Sequences** – The number of FC sequences received by this adapter port.
- **NOS Count** – The number of NOS events that have occurred on the switched fabric (not supported for an arbitrated loop).
- **Dumped Frames** – The number of frames that were lost due to a lack of host buffers available.
- **Loss of Sync** – The number of times loss of synchronization has occurred.
- **Prim Seq Prot Errs** – The primitive sequence protocol error count. This counter is incremented whenever there is any type of protocol error.
- **Invalid CRC's** – The number of frames received that contain CRC failures.
- **Ex Count Resp** – The number of FC exchange responses made by this port.
- **Active RPIs** – The number of remote port indicators.
- **Receive F_BSY** – The number of FC port-busy link response frames received.
- **Primitive Seq Timeouts** – The number of times a primitive sequence event timed out.
- **Arbitration Timeouts** – The number of times the arbitration loop has timed out. Large counts could indicate a malfunction somewhere in the loop or heavy usage of the loop.

4.3 Resetting a Port

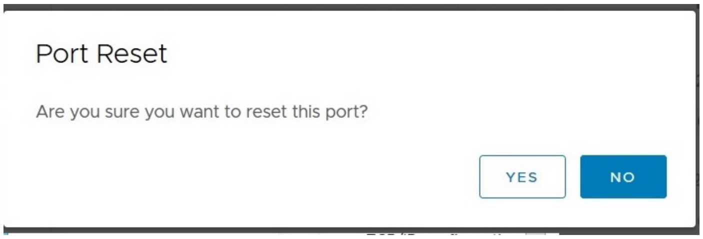
CAUTION! Do not reset an adapter port while copying or writing files. This action could result in data loss or corruption.

NOTE: Do not perform any active management operations on the ESXi host when resetting a port.

To reset a port, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the port that you want to reset.
3. Select the **Maintenance** tab.
4. Click **Reset**. The following popup is displayed (Figure 14).

Figure 14: Port Reset Popup



Port Reset

Are you sure you want to reset this port?

5. Click **Yes**. The adapter port resets. The reset can require several seconds to complete. While the adapter port is resetting, the message `Working` is displayed. When the reset is finished, the message `Reset Port Completed` is displayed.

Chapter 5: Updating Firmware

OneCommand Manager for VMware vCenter 6.7 and Later enables you to update firmware for a single adapter.

NOTE:

- If a secure version of firmware (version 11.0 or later) is installed on an LPe16000-series adapter and you want to update to an earlier unsecured version of firmware, you must remove the secure firmware jumper block before performing the update. Refer to the installation guide for the adapter for more information.
- If you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail.

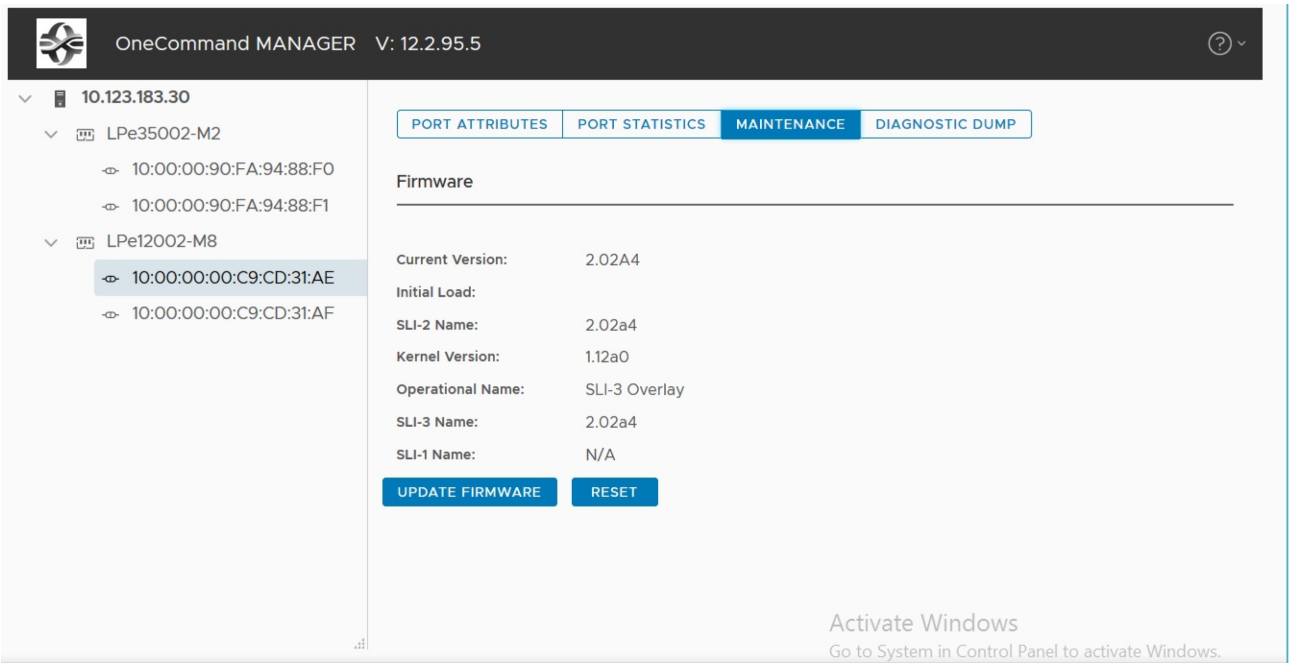
5.1 Updating Adapter Firmware

NOTE: For LPe1200-series adapters, you update firmware on an individual port and not on the entire adapter. For all other adapters, you update firmware on the entire adapter.

To update firmware for a port, or an adapter, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the port (LPe12000-series adapters only), or the adapter, for which you want to update firmware.
3. Select the **Maintenance** tab for LPe12000-series adapter (Figure 15) or the **Firmware** tab for all other adapters (Figure 16).

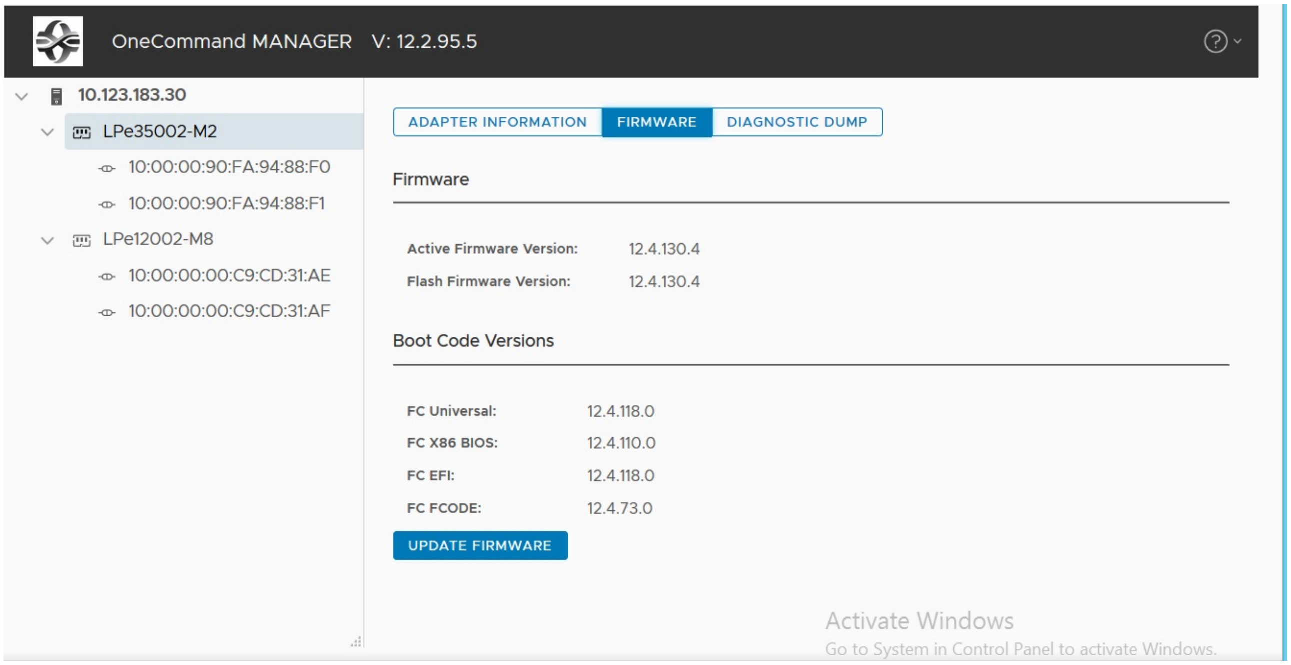
Figure 15: Maintenance Tab (LPe12000-Series Adapters Only)



Firmware

Current Version:	2.02A4
Initial Load:	
SLI-2 Name:	2.02a4
Kernel Version:	1.12a0
Operational Name:	SLI-3 Overlay
SLI-3 Name:	2.02a4
SLI-1 Name:	N/A

Figure 16: Firmware Tab (Non-LPe12000-Series Adapters)



Firmware

Active Firmware Version: 12.4.130.4

Flash Firmware Version: 12.4.130.4

Boot Code Versions

FC Universal: 12.4.118.0

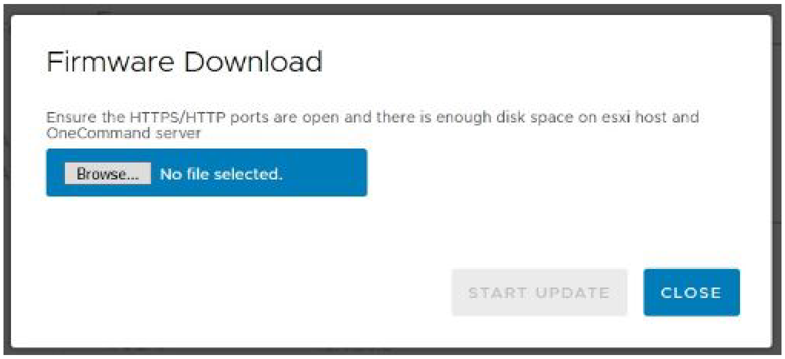
FC X86 BIOS: 12.4.110.0

FC EFI: 12.4.118.0

FC FCODE: 12.4.73.0

4. Click **Update Firmware**. The **Firmware Download** dialog is displayed (Figure 17).

Figure 17: Firmware Download Dialog



Firmware Download

Ensure the HTTPS/HTTP ports are open and there is enough disk space on esxi host and OneCommand server

5. Click **Browse** and navigate to the unzipped, extracted image file that you want to download.
6. On the browse window, select the file and click **OK**.
7. Click **Start Update**. Upon completion, the firmware download status is displayed on the dialog.

Chapter 6: Diagnostic Dumps

This section describes creating and viewing diagnostic dumps for Emulex adapters.

NOTE: Do not perform any active management operations on the ESXi host when creating diagnostic dumps.

6.1 Creating Diagnostic Dumps

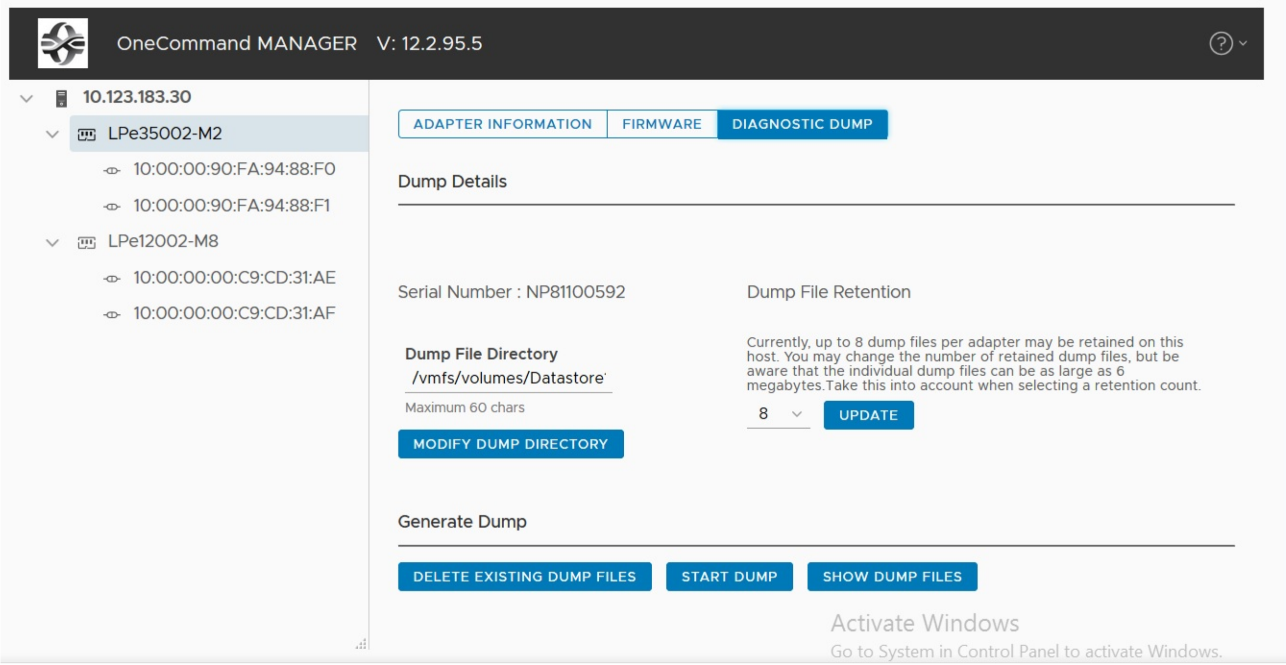
Diagnostic dump enables you to create and manage a diagnostic dump for a selected adapter. Dump files contain information, such as firmware version and driver version, that is particularly useful when troubleshooting an adapter.

You can retrieve user initiated and driver initiated driver dump files, delete the dump files, or repeat the process on all resident dump files. You can also retrieve or delete dump files from remote hosts.

To start a diagnostic dump, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the adapter. (Select the port for LPe12000-series adapters.)
3. Select the **Diagnostic Dump** tab (Figure 18). Diagnostic dump information is displayed.

Figure 18: Diagnostic Dump Tab



Serial Number : NP81100592

Dump File Directory
/vmfs/volumes/Datastore
Maximum 60 chars

Dump File Retention

Currently, up to 8 dump files per adapter may be retained on this host. You may change the number of retained dump files, but be aware that the individual dump files can be as large as 6 megabytes.Take this into account when selecting a retention count.

8

4. Enter a location in the **Dump File Directory** field in the **Dump Details** area to set the dump file directory. The **Delete Existing Dump Files**, **Start Dump**, and **Show Dump Files** buttons are enabled.

NOTE: If the location is not specified, a prefix of `/vmfs/volumes` is added to the location.

5. To specify up to 20 files to retain using the **Dump Files Retention** counter, enter the number of files and click **Update**.
6. Click **Start Dump** to initiate a diagnostic dump on the selected port.

Click **Delete Existing Dump Files** to remove existing dump files for the selected port. Click **Show Dump Files** to display the retained dump files. Click **Modify Dump Directory** to change the dump directory location.

CAUTION! Disruption of service can occur if a diagnostic dump is run during I/O activity.

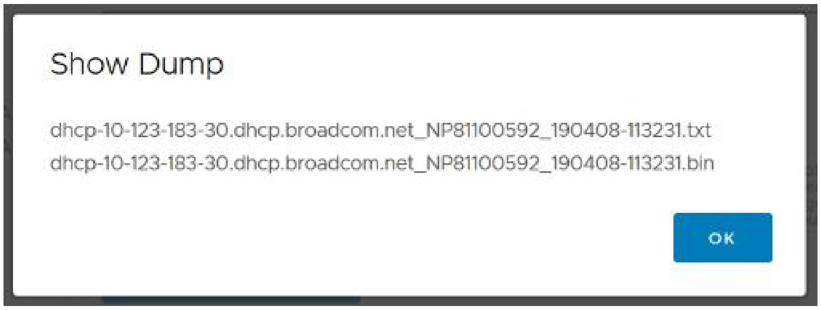
6.2 Viewing Diagnostic Dump Files

You can view diagnostic dump file names using the OneCommand Manager for VMware vCenter 6.7 and Later. The dump files are stored on the host's data store, and the client can be used to download dump files by browsing the host data store.

To view the diagnostic dump, perform these steps:

1. On the **Diagnostic Dump** tab, click **Show Dump Files**. The **Diagnostic Dump Files** window opens showing the diagnostic dump files currently on your system (Figure 19). These files are available in the dump directory configured from the **Diagnostic Dumps** tab. You can extract these files using the client.

Figure 19: Diagnostic Dump Files Window

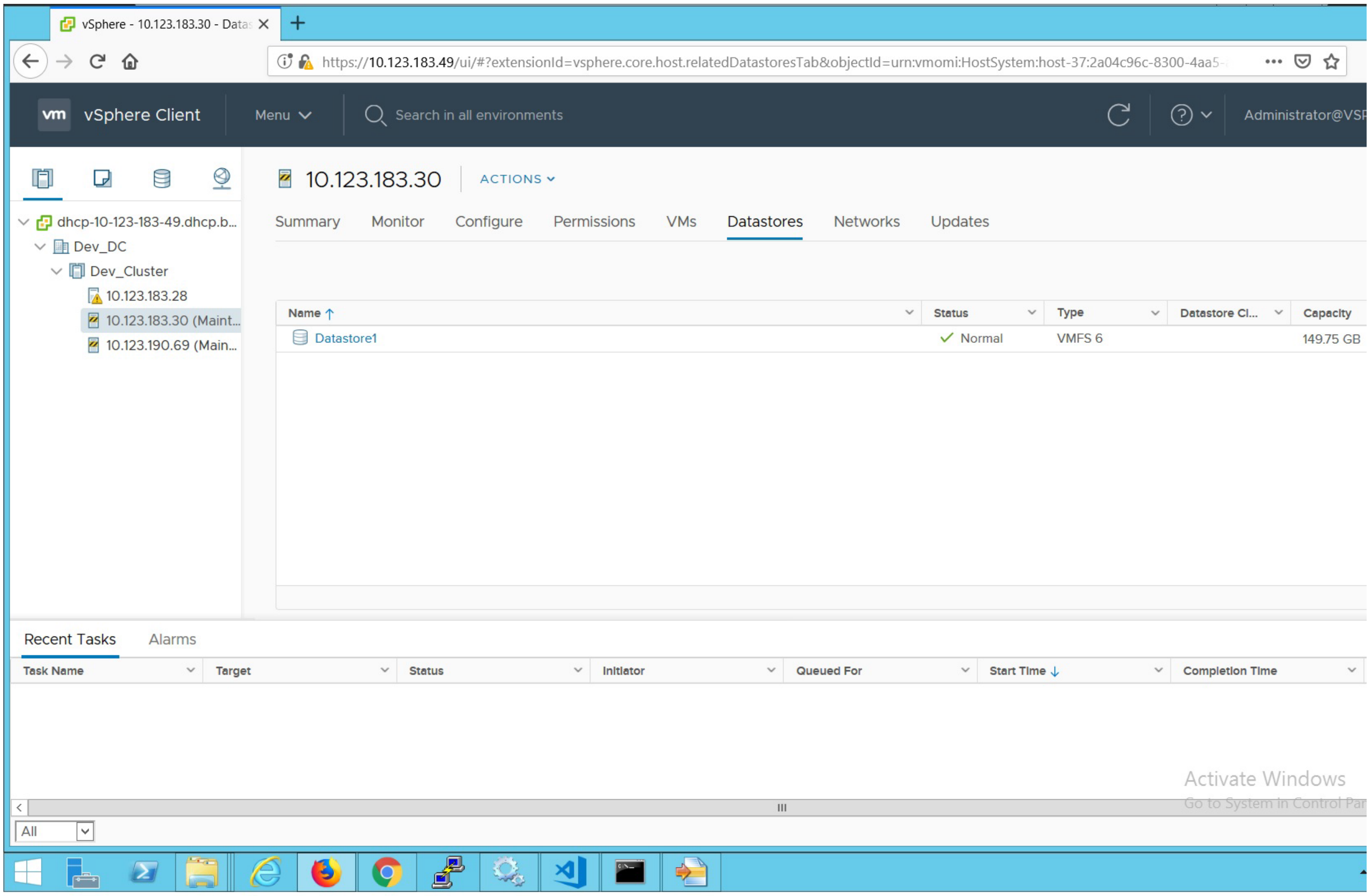


Show Dump

dhcp-10-123-183-30.dhcp.broadcom.net_NP81100592_190408-113231.txt
dhcp-10-123-183-30.dhcp.broadcom.net_NP81100592_190408-113231.bin

2. Extract the dump files by using the client to download the dump files by browsing the data store. Click the **Datastores** tab in the client. The **Datastores** view is displayed (Figure 20).

Figure 20: Datastores View of Client

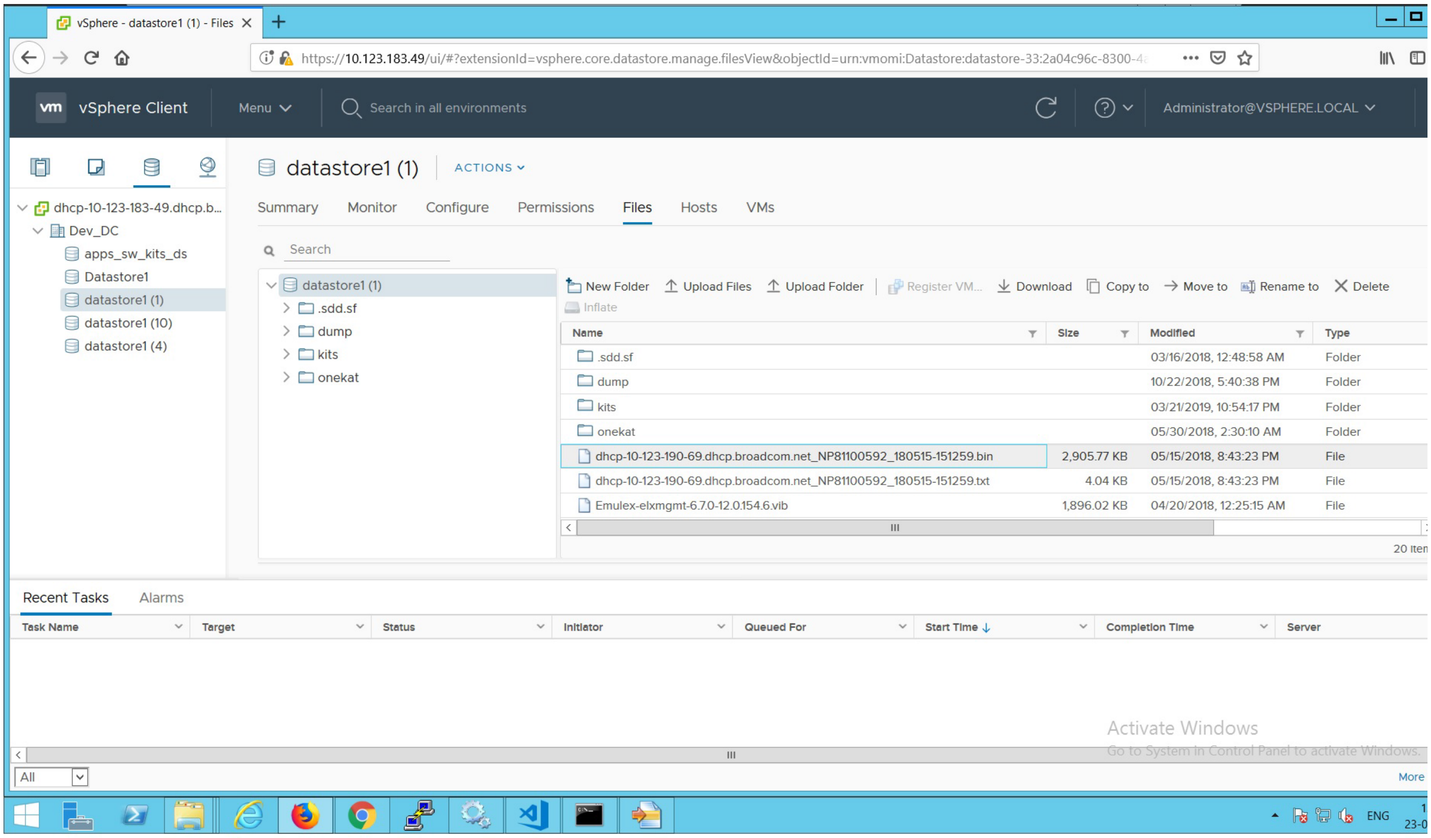

vSphere - 10.123.183.30 - Data
https://10.123.183.49/ui/#?extensionId=vsphere.core.host.relatedDatastoresTab&objectId=urn:vmomi:HostSystem:host-37:2a04c96c-8300-4aa5
vm vSphere Client
Menu
Search in all environments
Administrator@VSP
dhcp-10-123-183-49.dhcp.b...
Dev_DC
Dev_Cluster
10.123.183.28
10.123.183.30 (Maint...
10.123.190.69 (Main...
10.123.183.30
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Updates
Recent Tasks
Alarms
All
Activate Windows
Go to System in Control Par

Name ↑	Status	Type	Datastore Cl...	Capacity
Datastore1	✓ Normal	VMFS 6		149.75 GB

Task Name	Target	Status	Initiator	Queued For	Start Time ↓	Completion Time

3. Double-click the datastore to view its files, select the dump file, and click **Download** (Figure 21).

Figure 21: Datastore Browser



Name	Size	Modified	Type
.sdd.sf		03/16/2018, 12:48:58 AM	Folder
dump		10/22/2018, 5:40:38 PM	Folder
kits		03/21/2019, 10:54:17 PM	Folder
onekat		05/30/2018, 2:30:10 AM	Folder
dhcp-10-123-190-69.dhcp.broadcom.net_NP81100592_180515-151259.bin	2,905.77 KB	05/15/2018, 8:43:23 PM	File
dhcp-10-123-190-69.dhcp.broadcom.net_NP81100592_180515-151259.txt	4.04 KB	05/15/2018, 8:43:23 PM	File
Emulex-elxmgmt-6.7.0-12.0.154.6.vib	1,896.02 KB	04/20/2018, 12:25:15 AM	File

Task Name	Target	Status	Initiator	Queued For	Start Time ↓	Completion Time	Server

The file is downloaded to the location that you select. You can view the dump file in any text editor.

Chapter 7: Generating and Installing Secured Certificates

OCMNG is a Web application, based on a client-server model, that runs on the Apache Tomcat Web Server. Data is exchanged between the client (browser) and the server (on a remote machine), which requires a secure user logon to manage Emulex adapters on different and multiple hosts.

7.1 SSL Certificate

A Secure Sockets Layer (SSL) certificate establishes an encrypted connection between the Web server and the Web browser on a remote machine. This connection allows private information to be transmitted without eavesdropping, data tampering, or message forgery.

An SSL certificate provides security through encryption and authentication. Encryption is ensured by accessing the remote server using the HTTPS protocol and an SSL certificate.

NOTE: If OneCommand Manager for VMware vCenter 6.7 and Later is running, the server must be configured to support HTTPS protocol access and provide a self-signed certificate.

The OneCommand Manager for VMware vCenter 6.7 and Later server is authenticated to the browser by a public key in the self-signed certificate.

7.1.1 Generating an SSL Certificate

To allow secured communication between the client and server, perform these steps:

1. Generate a self-signed certificate with a keystore file for each server providing the server's domain name and company details. See Section 7.1.2, Generating a Self-Signed Certificate, for instructions. For more information, refer to the X.509 attributes list on the International Telecommunications Union website.
2. Use this certificate to create a request to the customer's trusted certificate authority (CA). The request certificate is referred as a Certificate Signing Request (CSR). The CA issues a new SSL certificate. See Section 7.2.1, Generating a CSR for a Server Using the Java Tool, for instructions.
3. Import the new SSL certificate to the application server, and install the SSL certificate on the client's browser. See Section 7.2.4.1, Installing the Certificates to the Keystore of OneCommand Manager for VMware vCenter 6.7 and Later, for instructions.
4. Configure the server to use the keystore file. See Section 7.2.4.2, Configuring a Web Server, for instructions.
5. Access the server's content through the browser using the HTTPS protocol.

   The browsers understand the certificate, and the browsers allow access to and from the remote server.

7.1.2 Generating a Self-Signed Certificate

A self-signed certificate is a certificate that is signed by itself (the server hosting OneCommand Manager for VMware vCenter 6.7 and Later) rather than a trusted CA. This self-signed certificate includes a public or private key that is distributed by the SSL to verify the identity of the server.

A self-signed certificate can also be used as an alternative to SSL certificates if the server is not running in a public domain.

If a self-signed certificate is used in place of an SSL, a warning is shown in the browser before accessing the server content.

For Java-based applications, a self-signed certificate can be generated using the tools provided by Java. This creates a keystore file that must be installed on the Web server. This keystore includes a private key specific to the server used for generating a CSR and authenticating the server.

Because the OneCommand Manager for VMware vCenter 6.7 and Later server is developed using Java, it leverages the keystore tool provided by Java to generate the self-signed certificates at no cost.

NOTE: The self-signed certificate for the OneCommand Manager for VMware vCenter 6.7 and Later server is generated and installed on its server as part of the OneCommand Manager for VMware server installation on a Windows machine. This self-signed certificate is generated with Broadcom® organization details using the RSA algorithm and a private key of size 2048 bits.

To generate a self-signed certificate, perform these steps:

1. In the OCM for VMware installation directory, go to `ApacheTomcat\conf`.
   ```
   >>cd /d  "C:\Program Files\Emulex\OCM for VMware\ApacheTomcat\conf"
   ```
2. Run the following command:
   ```
   >> ..\..\JRE\bin\keytool.exe -genkey -alias <new-alias> -keyalg RSA -keystore emulex.vcplugin.jks
   -keysize 2048
   ```

NOTE: You can change alias, keysize, and keystore name.

Example

```
Enter keystore password: (Enter "emulex" if using the same keystore name)
Re-enter new password:
What is your first and last name?
  [Unknown]:  pluginserver.ad.emulex.com  (Give the complete domain name of the server [FQDN])
What is the name of your organizational unit?
  [Unknown]:  ocm
What is the name of your organization?
  [Unknown]:  elx
What is the name of your City or Locality?
  [Unknown]:  bg
What is the name of your State or Province?
  [Unknown]:  ka
What is the two-letter country code for this unit?
  [Unknown]:  in
Is CN=pluginserver.ad.emulex.com, OU=ocm, O=elx, L=bg, ST=ka, C=in correct?
  [no]:  yes

Enter key password for <elxocm>:
        (RETURN if same as keystore password)
```

7.2 Generating a CSR

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate is used. A CSR contains information to be included in the SSL certificate, such as the organization name, common name (domain name), locality, country, and other X.509 attributes. It also contains the public key that is included in the certificate. The CA uses the CSR to create a new SSL certificate.

7.2.1 Generating a CSR for a Server Using the Java Tool

To generate a CSR for a server, use the Java tool available in the `jre/bin` folder. The syntax using the Java tool follows:

```
keytool -certreq -keyalg <algorithm>  -alias <alias-name>  -file <csr-name> -keystore <keystore-
name>
```

Example

```
keytool -certreq -keyalg RSA -alias selfsigned -file elxocmreq.csr -keystore emulex.vcplugin.jks
```

7.2.2 Generating and Validating a CSR

To generate a CSR, perform these steps:

1. Generate a self-signed certificate (see Section 7.1.2, Generating a Self-Signed Certificate, for instructions).
2. Generate a CSR using the following syntax:

```
>>..\..\JRE\bin\keytool -certreq -v -alias <new-alias> -file elxocmreq.csr -keypass elxocm -
keystore emulex.vcplugin.jks
Enter the keystore password: (Enter "emulex" if using the default keystore name)
Certification request stored in file <elxocmreq.csr>
```

To validate a CSR for its completeness, perform these steps:

You can validate the generated CSR for its completeness before submitting (with the help of the CA). Copy the CSR content from the following link for validation.

```
http://www.sslshopper.com/csr-decoder.html
```

NOTE: The CSR must begin and end with the following tags:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
-----END NEW CERTIFICATE REQUEST-----
```

Example

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC2TCCAcECAQAwZDELMAkGA1UEBhMCaW4xCzAJBgNVBAgTAmthMQswCQYDVQQHEwJiZzEMMAoG
A1UEChMDZWx4MQwwCgYDVQQLEwNvY20xHzAdBgNVBAMTFmJnc3N5ZWQxLmFkLmVtdWxleC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCDhovljXhfjNPM/5eBsX4280AIl3YARn0p
R6Z7eOqs1r5Qh07kT58M6T8fER+NpIN7WhOOF/TbsFsS0gmfYwJQqttvtq1dtxUGpvFe9lywbP+l
kY+w6GOyPTG2qnXgILtX5ArZbC2UBbz+J8WJ3SjPHXiSY35EZWnyZZmIN8v1vOe9e21f8vwRkn/4
fdfFrpoQa3H+GcAJMRSBRTd5H6mXQv6HaA5Z0BbsABisFx4scqSuM/HJKLP6GcSHR61bzHfiO/NH
4qU/s6I2LC5DvGs1hIW3PPbmb1rxBiEFpjPtWhfzPxPMKSU8uey+lE0UIPMS0FMTxo63oYnMeiSX
X5mxAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMB0GA1UdDgQWBBSvpKLBF3lY03Jin9kI4ym94bJi
zjANBgkqhkiG9w0BAQsFAAOCAQEAfs94wzEUlDAMq0jITi6fiD7YxK2KFWJgMBfjxZIGex2zxlHL
mOS14BGSWk5dvSMwqDBC14l4C79rUOlTUwwWs9zFqMHynndQ2Ze2vuJNTWUlnFyFb37/rEvbFufB
QVvFXgycaKRgUpWo2x5sekRJRAPxXI/vLWOFRLLrzcVykgZ/sg3QrO4ezlKFc49put0vKpvI1dY9
l9BN2REuWrlmq5y3L8nx8mKX9dRmP6CKzHBaVrvY+nVju+Vf/ikfTtQIDEXAIW2Q7AObpcOaudnf
Nsaey+u27vGy77gAv7092xBHsDyOrD7COy/83b194igmVBVY4dt0496oXkOHCA0txA==
-----END NEW CERTIFICATE REQUEST----
```

7.2.3 Getting an SSL Certificate

The CSR can be submitted to the trusted CA (as chosen by you). The CA validates the CSR and issues a new SSL certificate.

7.2.4 Installing the SSL into the Web Server

When you receive the SSL certificate from the CA, you must install the SSL certificate on the server to accept the secure connections.

NOTE: The CSR must be generated on the same machine that the server is running on. The SSL certificate must also be installed on this same server.

7.2.4.1 Installing the Certificates to the Keystore of OneCommand Manager for VMware vCenter 6.7 and Later

The Root Certificate file, the Intermediate Certificate file, and the Primary Certificate file must all be installed in the keystore.

To install the certificates to the keystore of OneCommand Manager for VMware vCenter 6.7 and Later, perform these steps:

1. Download the SSL certificate file from the CA. Save the SSL certificate file to the same directory as the keystore (self-signed certificate) that was created for the CSR.

NOTE: The certificate works only with the same keystore that was initially created for the CSR. The certificates must be installed to your keystore in the correct order.

2. Install the Root Certificate file.

   Every time you install a certificate to the keystore, you must enter the keystore password that you chose when you generated it. Enter the following command to install the Root Certificate file:

   ```
   keytool -import -trustcacerts -alias root -file RootCertFileName.crt -keystore keystore.key
   ```

   If the following message is displayed, select `Yes`:

   ```
   Certificate already exists in system-wide CA keystore under alias <...> Do you still want to add
   it to your own keystore?
   ```

   If successful, the following message is displayed:

   ```
   Certificate was added to keystore.
   ```

3. Install the Intermediate Certificate file.

   If the CA provided an Intermediate Certificate file, you must install it here using the following command:

   ```
   keytool -import -trustcacerts -alias intermediate -file IntermediateCertFileName.crt -keystore
   keystore.key
   ```

   If successful, the following message is displayed:

   ```
   Certificate was added to keystore.
   ```

4. Install the Primary Certificate file.

   Use following command to install the Primary Certificate file (for your domain name):

   ```
   keytool -import -trustcacerts -alias tomcat -file PrimaryCertFileName.crt -keystore keystore.key
   ```

   If successful, the following message is displayed:

   ```
   Certificate reply was installed in keystore.
   ```

All the certificates are now installed to the keystore file. You must configure your server to use the keystore file.

7.2.4.2 Configuring a Web Server

NOTE: These configuration changes are not required if the default keystore name and password are used. If they are different, you must change the configuration as needed.

1. Copy the keystore file or SSC to a directory (preferably, the `conf` folder) of the Web server.
2. Open the file `${CATALINA_HOME}/conf/server.xml` in a text editor.
3. Uncomment the SSL Connector Configuration.
4. Make sure that the keystorePass matches the password for the keystore and that the keystoreFile contains the path and file name of the keystore.

   Your connector should be displayed similar to the following:

   ```
   <Connector className="org.apache.catalina.connector.http.HttpConnector" port="8443"
   minProcessors="5" maxProcessors="75" enableLookups="true" acceptCount="10" debug="0"
   scheme="https" secure="true">

   <Factory className="org.apache.catalina.net.SSLServerSocketFactory" clientAuth="false"
   protocol="TLS" keystoreFile="./conf/emulex.vcplugin.jks" keystorePass="emulex"/>
   ```

5. Save the changes to `server.xml`.
6. Restart the Web server.

   If you launch the OneCommand Manager for VMware vCenter 6.7 and Later URL in the browser, the application should start normally.

NOTE: Use the host name with the domain name that you used to generate the CSR.

Chapter 8: Troubleshooting

This section includes information about certificate or insecure-content warnings that might be displayed on the console. This section also describes unexpected circumstances and some proposed solutions.

8.1 Security

OneCommand Manager for VMware vCenter 6.7 and Later can be installed on different machines. As a result, certificate or insecure-content warnings can occur. The two ways to remedy the issue are:

- Accepting the blocked content – temporary solution
- Installing a security certificate – permanent solution

The Microsoft Edge browser does not allow you to accept blocked content. See Section 8.1.3, Installing a Security Certificate in Edge Browsers.

8.1.1 Accepting Blocked Content

Accepting blocked content is not a permanent solution, and you must repeat this procedure every time you use OneCommand Manager for VMware vCenter 6.7 and Later. If you want a permanent solution, you must install the correct security certificate. See Section 8.1.2, Installing a Security Certificate in Internet Explorer 11 or Later Browsers.

To accept blocked content in Internet Explorer 11 or later, Chrome, and Firefox browsers, perform these steps:

1. Load the plug-in URL in a separate tab or window.

   The plug-in URL format is:

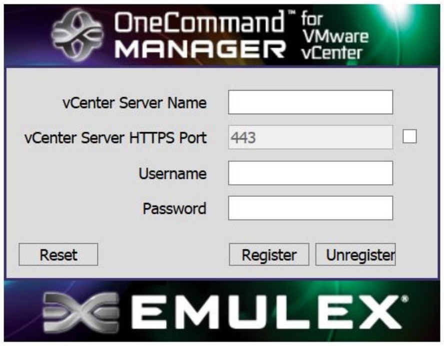
   `https://<plugin-server>:<https-port>/elxvcplugin`

   For example:

   `https://pluginserverhostFQDN:443/elxvcplugin`

2. Confirm or accept the certificate popup (Figure 22).
3. Refresh the **vCenter web client** tab or window.

Figure 22: Blocked Content in the Firefox or Chrome Browser



vCenter Server Name

vCenter Server HTTPS Port 443 □

Username

Password

8.1.2 Installing a Security Certificate in Internet Explorer 11 or Later Browsers

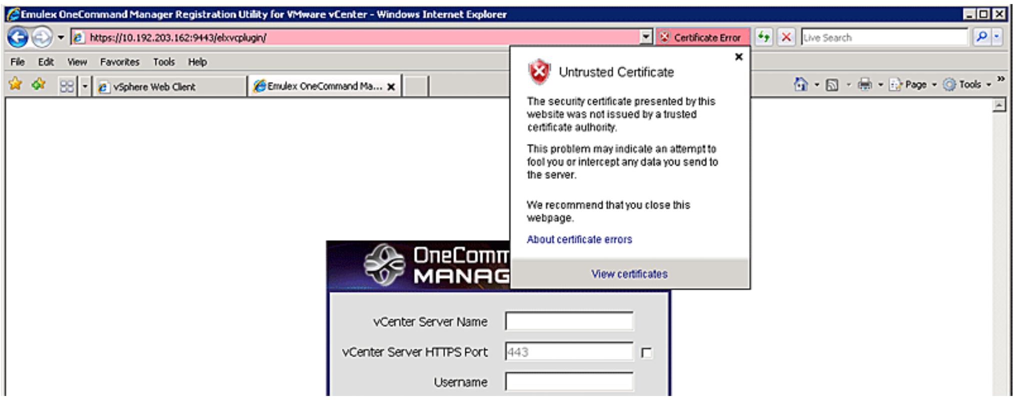
A permanent solution to the security warnings is to install the correct security certificate.

To install a security certificate in Internet Explorer 11 or later browsers, perform these steps:

1. Open Internet Explorer in Administrative mode.
2. Load the plug-in URL, and accept the certificate warning.

   The plug-in URL must have the following format:
   `https://<plugin-server>:<https-port>/elxvcplugin`
   The page loads with a certificate error.
3. Click **Certificate Error**. A list appears showing the untrusted certificate (Figure 23).

Figure 23: Untrusted Certificate



Emulex OneCommand Manager Registration Utility for VMware vCenter - Windows Internet Explorer

https://10.192.203.162:9443/elxvcplugin/

Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

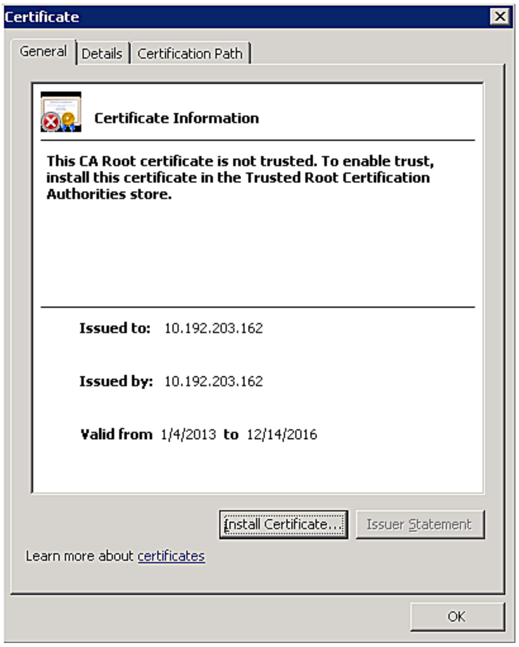
vCenter Server Name

vCenter Server HTTPS Port 443 □

Username

4. Click **View certificates** in the **Certificate Error** list. The **Certificate** dialog is displayed (Figure 24).

Figure 24: Certificate Dialog



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

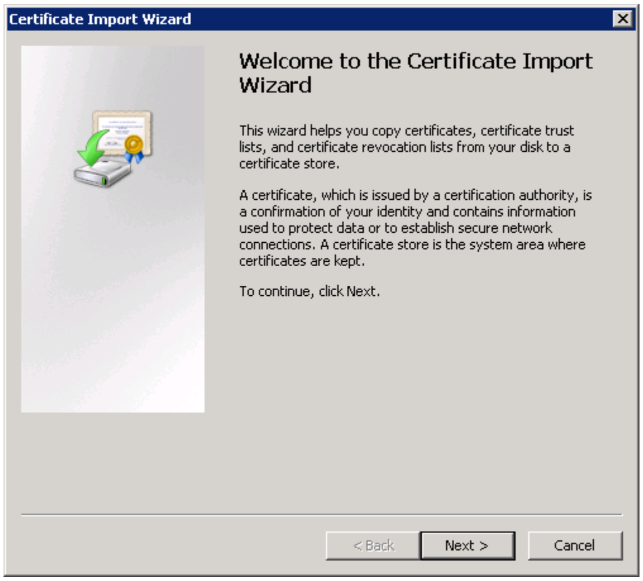
Issued to: 10.192.203.162

Issued by: 10.192.203.162

Valid from 1/4/2013 to 12/14/2016

5. Click **Install Certificate**. The **Certificate Import Wizard** is displayed (Figure 25).

Figure 25: Certificate Import Wizard



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. Follow the wizard instructions and install the certificate to the Trusted Root Certification Authorities location.

8.1.3 Installing a Security Certificate in Edge Browsers

To install a security certificate in Edge browsers, perform these steps:

1. Enter the plug-in url in a new tab in the Edge browser. (This is the IP and port where you installed the plug-in exe.) For example:
   `https://10.123.183.15:443/elxvcplugin`
   You should see a `Certificate error` message in the address bar.
2. Click **Certificate Error** and select **View Certificate**. The **Certificate Information** dialog appears.
3. Click **Export to file** and save the `<`*`filename`*`>.crt` to your system.
4. Open the **Certificate Manager**.
5. Navigate to **Trusted Root Certification Authorities**, and select **Certificates > All tasks > Import**.
6. Add the saved security certificate and relaunch Edge.

8.2 Issues and Resolutions

Your system might operate in an unexpected manner in several circumstances. The following table explains some of these circumstances and offers one or more solutions for each issue.

Table 1: Troubleshooting Issues and Resolutions

Issue	Resolution
The **Emulex OneCommand** tab is not visible in the console.	From the menu, select **Administration**. Under client Plug-Ins, check the status of the Emulex OneCommand Manager for VMware vCenter 6.7 and Later (Emulex OneCommand). The status must be **Enabled**. If it is not enabled, enable it. On the machine where OneCommand Manager for VMware vCenter 6.7 and Later is installed, make sure that the port numbers configured during the installation are open and dedicated to the plug-in server only. No other service should be listening on this port.
When you select the **Emulex OneCommand** tab in the console, the Emulex Device Management tree-view does not display any elements.	Ensure that you have the required privileges to view information in the console.
There is slow response from OneCommand Manager for VMware vCenter 6.7 and Later.	Ensure that the following are on the same network: ■ ESXi servers managed by the OneCommand Manager VMware for vCenter Server ■ Systems hosting the OneCommand Manager for VMware vCenter 6.7 and Later server ■ OneCommand Manager for VMware vCenter 6.7 and Later
Firmware update fails.	On the ESXi host, check the firewall settings and ensure that the HTTP/HTTPS ports are open. Use the following command to disable the firewall: `esxcli network firewall unload`
Firmware update fails with the error message `Error reading resource`.	Check the following: **NOTE:** Make sure that you can run the `ping` command on the host name, on which the OneCommand Manager for VMware vCenter 6.7 and Later is installed, from the ESXi host. If you cannot run the `ping` command on the host name, either reinstall providing the reachable IP or host name (with domain) or add the host name to the DNS. ■ Check the memory space in the ESXi host and clean up the old logs.
When you make any changes to the ESXi host, such as plugging cables, unplugging cables, or storage references, OneCommand Manager for VMware vCenter 6.7 and Later does not reflect the change immediately.	Restart `sfcb` on the ESXi host using the command: `/etc/init.d/sfcbd-watchdog restart`
When OneCommand Manager for VMware vCenter 6.7 and Later loads within the console, it displays a security warning.	See Section 8.1, Security.
Registration of a new host from a non-English system results in a *Host not Pingable* error.	When adding the host, change the locale of the system to English. Once the host is added, the locale can be changed.

Appendix A: License Notices

A.1 VI Java SDK

A.2 @webcomponents/custom-elements

BROADCOM®