



Cisco CPAM Deployment on UCS-B and C-series Platforms

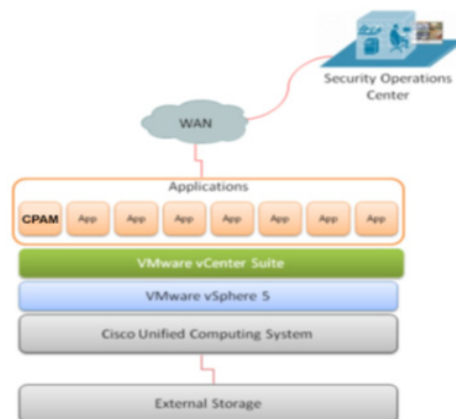
Contents

- [Implementing CPAM on the UCS B- and C-Series Platforms, page 1](#)
- [Deploying the OVF Template, page 3](#)
- [Configuring Ethernet 0 IP Address, page 6](#)
- [Related Documentation, page 7](#)

Implementing CPAM on the UCS B- and C-Series Platforms

This section summarizes the high-level design recommendations and best practices for implementing CPAM on the UCS B- and C-Series platforms. In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support high-quality CPAM. [Figure 1](#) represents a virtualized CPAM application running on a UCS B-Series platform.

Figure 1 Cisco Physical Access Manager on UCS.



Solution Components

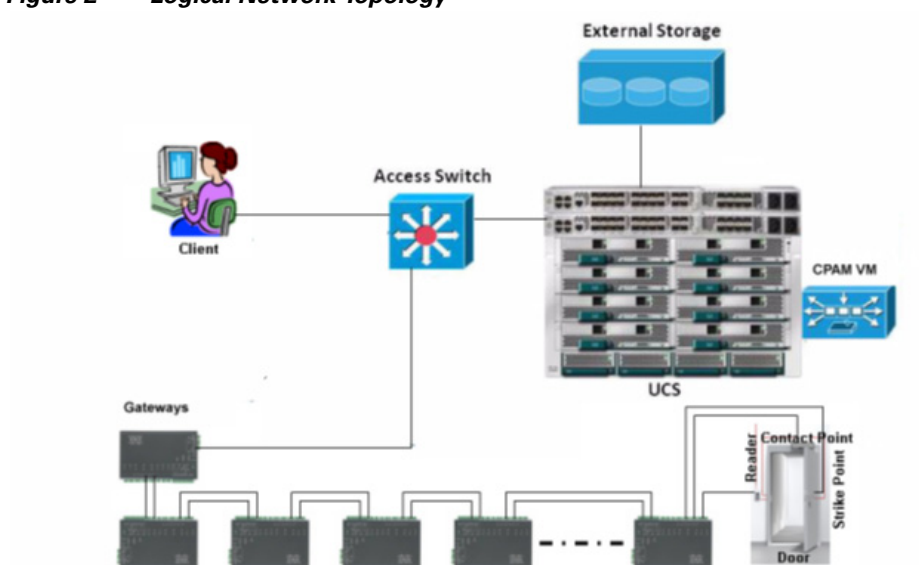
The components required for designing and deploying CPAM on UCS B-and C-Series platforms include:

- **UCS B- and C-Series servers**—The Cisco UCS Servers can be deployed as rack-mount servers (C-Series) or blade servers (B-Series) running the ESXi 5.0 virtualization software. The B-Series servers deliver a scalable and flexible architecture to meet your data center needs while helping to reduce the total cost of ownership. The C-Series servers address fluctuating workload challenges through a varying balance of processing, memory, I/O, and internal storage resources.
- **Cisco Physical Access Manger (CPAM) software**—This software runs on UCS B-or C-Series server in a virtualized environment. The CPAM on UCS software is available for download with purchase of the CPAM on UCS software license R-CIAC-PAME-VM-K9=. This software is an Open Virtual Appliance (OVA) file on Cisco.com. The OVA package is a tar file with the Open Virtualization Format (OVF) directory inside.

Logical Network Topology

Figure 2 illustrates the overall logical topology of the networking and CPAM components, including a UCS B-Series containing the ESXi host running CPAM, gateways, expansion modules, and the operator workstations running the CPAM client.

Figure 2 Logical Network Topology



Note

This guide does not describe the configuration and operation of the Cisco Physical Access Manager (CPAM) products. For more information see, http://www.cisco.com/en/US/products/ps9688/prod_installation_guides_list.html

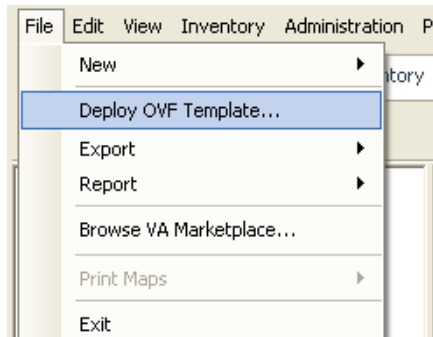
Deploying the OVF Template


Tip

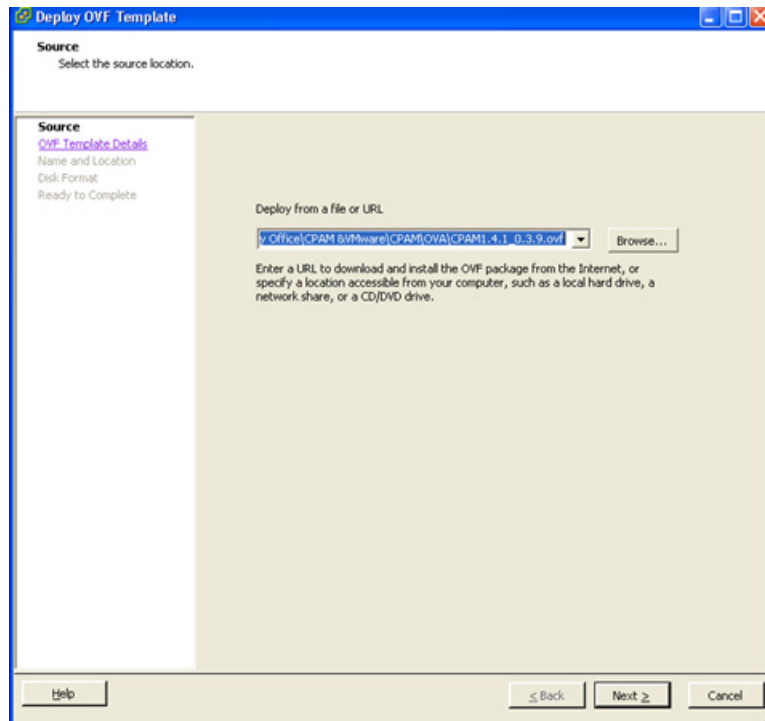
Before performing the following steps, ensure that the ESXi 5.0 Hypervisor is installed on the UCS B- and C-Series platforms.

To deploy the OVF template, complete the following procedure:

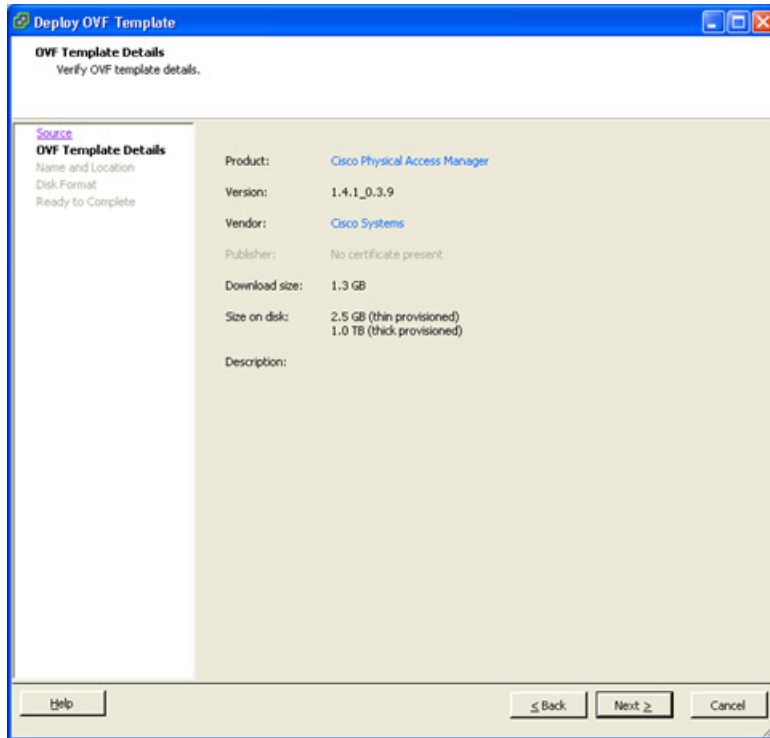
- Step 1** Log in to vSphere Client.
- Step 2** From the File menu, select **Deploy OVF Template**. The Deploy OVF Template page opens.



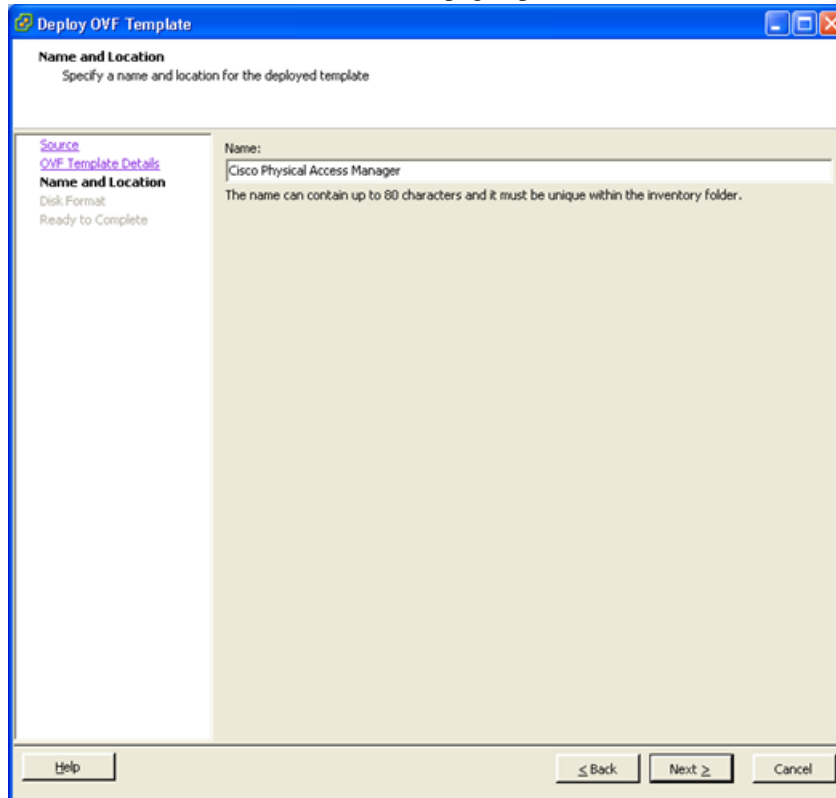
- Step 3** Click **Browse** to select the path of the OVF file from local directory or URL using source window.



Step 4 Click **Next** and the OVF Template Details page appears displaying the CPAM version and disk properties.

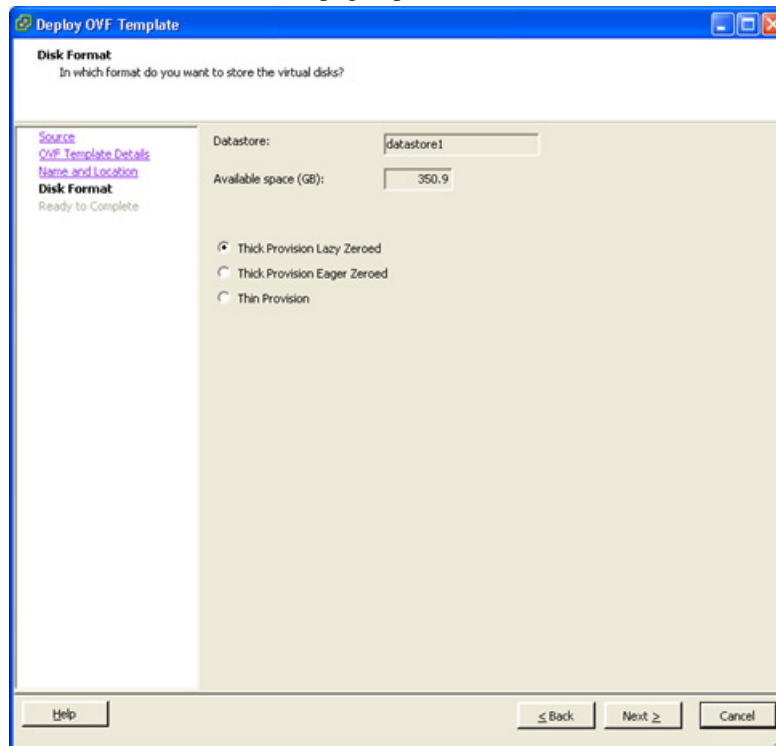


Step 5 Click **Next** and the Name and Location page opens.



Step 6 Enter the CPAM appliance name.

Step 7 Click **Next**, the Disk Format page opens.



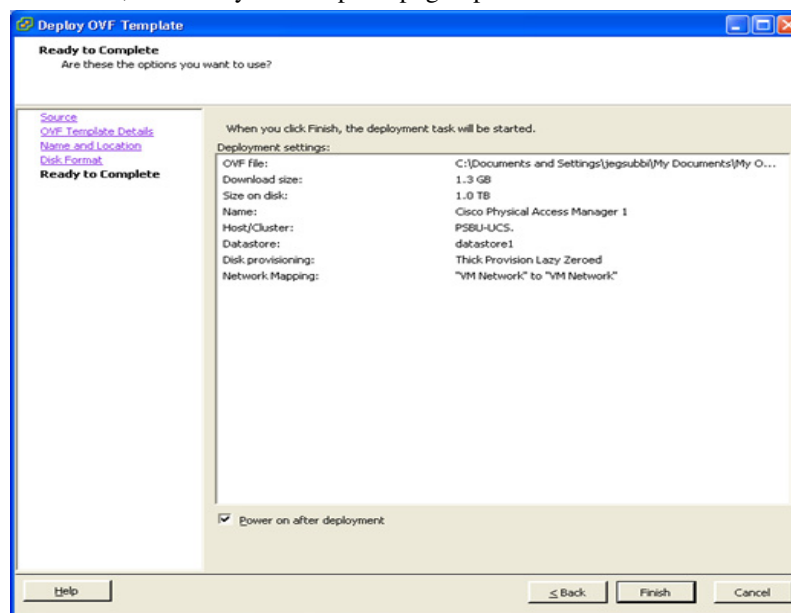
Step 8 Select the desired provisioning policy for the virtual disk file.



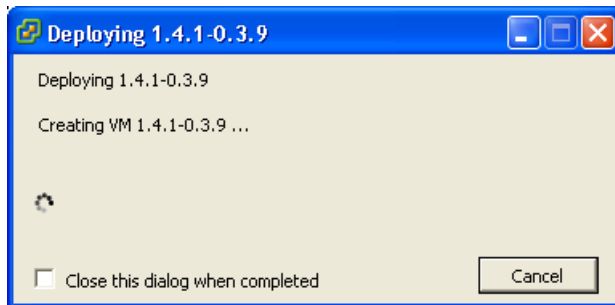
Note

It is advisable to choose either Thick Provision Lazy Zeroed or Thin Provision. It takes a longer time to create a disk with Thick Provision Eager Zeroed format.

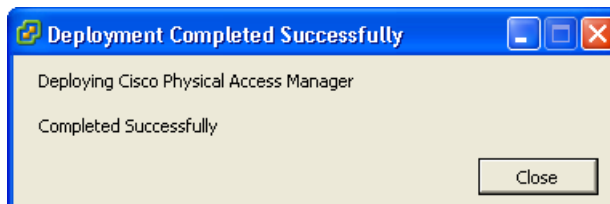
Step 9 Click **Next**, the Ready to Complete page opens.



- Step 10** Check the Power on after deployment checkbox.
- Step 11** Click **Finish** to start the OVF deployment process.
- Step 12** While processing, the following dialog box appears.



- Step 13** When deployment is complete, the following dialog box appears.



Configuring Ethernet 0 IP Address

To configure Ethernet 0(eth0) IP address, complete the following procedure:

- Step 1** Launch console connection for the installed Cisco Physical Access Manager from VSphere Client.
- Step 2** Login with the default user name and password (cpamadmin/cpamadmin).
- Step 3** Change the permission to super user.
- Step 4** Copy **ifcfg-eth0** file in **/home/cpamadmin** to **/etc/sysconfig/network-scripts/** using the following command:
- Step 5** Edit the file using vi and change the default IP ,subnet mask and the default Gateway for **ifcfg-eth0** file in - **/etc/sysconfig/network-scripts/**.

```
cp /home/cpamadmin/ifcfg-eth0 /etc/sysconfig/network-scripts/
```

Sample configuration of ifcfg-eth0:

```
DEVICE=eth0
BOOTPROTO=static
USERCTL=no
PEERDNS=yes
IPADDR=192.168.1.2
NETMASK=255.255.255.0
ONBOOT=yes
TYPE=Ethernet
GATEWAY=192.168.1.1,
```



Note The above network parameters IPADDR, NETMASK, and GATEWAY must be configured based on network.

Step 6 Restart the network services using - **/sbin/service network restart**

Step 7 Check eth0 configuration using - **/sbin/ifconfig**

Step 8 Restart cpadmin service using- **/sbin/service cpadmin restart**

Now the CPAM appliance is ready for the Initial setup.

**Note**

The CPAM VM, gateways, expansion modules, and CPAM client workstations are reachable in the network.

Related Documentation

For more information on Cisco-related products, see the following resources:

Cisco Physical Security product information:

<http://www.cisco.com/go/physec/>

Cisco UCS Manager Configuration Guide:

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco UCS B-Series Blade Servers Data Sheet and Literature:

http://www.cisco.com/en/US/products/ps10280/prod_literature.html

Cisco Physical Access Manager User guide:

http://www.cisco.com/en/US/products/ps9688/products_user_guide_list.html

