Cisco Prime Security Manager UCS Appliance Quick Start Guide

First Published: November 30, 2012
Last Updated: May 2, 2014

Contents

Cisco Systems, Inc.
www.cisco.com

Product Overview

The Cisco Prime Security Manager UCS Server Appliance consists of the following components:

Cisco UCS C220 Server

The Cisco UCS C220 Server is pre-configured with the required hard drives, RAM, and other components.

The server comes with all the parts shipped with a standard UCS server.

VMware

VMware vSphere Hypervisor (ESXi) and its license is already installed on the appliance.

Note You must also install the VMware vSphere Client, which you can download from the appliance to your workstation. Your workstation should have at least 2 GB RAM. You can determine the exact VMware version using the **Help > About VMware** command from this client.

Cisco Prime Security Manager (PRSM)

Cisco Prime Security Manager is a network security management application used to manage multiple ASA and CX devices. (CX devices are also known as Cisco ASA Next-Generation Firewall Services and Cisco ASA CX Context-Aware Security.)

Cisco Prime Security Manager is installed as a virtual machine (VM) running under VMware. Although the software is already installed, you will need to configure its basic settings and install the PRSM license.

Note Your Cisco Prime Security Manager license is provided in paper format as a Cisco Software License Claim Certificate and is packed in your shipping carton along with the appliance.

Before You Begin

Before you start installing the appliance, do the following:

- Please read the document *Regulatory Compliance and Safety Information for the Cisco UCS C-Series Servers* at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/c/regulatory/compliance/cseries_regulatory_compliance_information.html.
- For VMware performance best practices, refer to the following document: http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf. You can search the VMware site for more best practices documents.
- Use the Cisco Software License Claim Certificate to obtain the .lic license file. You will upload this to the PRSM server.

Installing and Configuring the Appliance

Installing and configuring the appliance consists of installing the hardware, configuring the server, setting up VMware, and configuring the PRSM software. The following procedure covers the main points, with details in subsequent sections.

Step 1 Install the server in a rack.

Follow the instructions included in the box and in *Cisco UCS C220 Server Installation and Service Guide*, http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C220/install/install.html.

Step 2 Power on the server in standalone mode and configure a static IP address.

Follow the initial setup instructions in the server installation and service guide carefully. During power-on, you need to enter the BIOS CIMC Configuration Utility to configure various settings, including the IP address.

The default CIMC username/password is **admin/password**. You should change the default password during setup.

Note Power on the server in Standalone mode. Do not use UCSM mode.

Step 3 Open the VMware ESXi home page on the server.

Use a browser to open the VMware ESXi home page, https://*server_IP*, where s*erver_IP* is the IP address of the UCS server.

The home page includes a link to the vSphere client, ESXi documentation, and other important resources for ESXi.

Step 4 Install the vSphere Client.

From the ESXi home page, click the link to install the vSphere Client on your workstation. When the application is installed, open it and log in using the server's IP address and the default ESXi username/password, which is **root/password**.

Step 5 Verify the PRSM virtual machine (VM) characteristics are the desired ones and adjust them if necessary.

You can increase or otherwise change the number of processor cores (virtual CPUs), and the amount of memory and disk space, while the VM is powered off. To view the settings, select the VM, right-click and select **Edit Settings**.

For more information, see Editing the Virtual Machine Settings, page 4.

Step 6 Determine the setup values required to configure the PRSM VM.

PRSM setup will prompt you for management addresses, DNS, NTP, and other information. Determine the correct values before you power on the system.

For more information, see Information Required for PRSM Setup, page 5.

Step 7 Power on the VM and configure the setup.

For detailed information, see Configuring the PRSM Virtual Machine, page 6.

Step 8 Log into the PRSM web interface and respond to the initial prompts. Do not add devices yet.

For best results, use a recent version of Firefox or Chrome to open https://*PRSM_IP*, where *PRSM_IP* is the IP address you configured when setting up the PRSM VM. Log in using the **admin** username and the password you configured during setup.

Note If your web browser cannot open the URL, because it cannot find the server or the server is taking too long to respond, go to the PRSM console, log in as **admin**, and use the **ping** command to ping your workstation IP address. Then, retry the browser connection. Also, verify that you are using https:// instead of http://.

For more information on supported browsers, including supported Internet Explorer versions. see the *Installation Guide for Cisco Prime Security Manager* for your version, available at http://www.cisco.com/en/US/products/ps12521/prod_installation_guides_list.html.

Step 9 Select **Administration > Licenses** and upload the PRSM license file.

Step 10 Check for PRSM updates.

First, select **Administration > About PRSM** and find the exact version number.

Then, go to http://www.cisco.com/go/prsm, find the software downloads page, and look for updates that apply to your version.

If any are available, install them. You can use the web interface or the CLI; for complete instructions, see the online help or the *Installation Guide for Cisco Prime Security Manager* for your version, available at http://www.cisco.com/en/US/products/ps12521/prod_installation_guides_list.html.

Tip Ensure that you install the same version, including build number, on the CX devices you will manage.

Step 11 Now you can add devices and start configuring them. Click the **Help** link in the upper right corner to find information on how to prepare devices for management and to add them to the inventory.

Editing the Virtual Machine Settings

The PRSM virtual machine (VM) has pre-configured VM settings. Keeping in mind that you should not run any other application on the appliance, you might want to adjust the following settings. The recommended values are listed. Your changes must be within the limits of the system hardware, which ships with 8 CPUs, 16 GB memory, and 6 TB hard disk space.

- CPUs (cores)—7.
- Memory (RAM)—14.5 GB.
- Disk Space—As much secondary disk space (hard disk 2) as the system will allow. You might need to add new secondary virtual hard disks to reach the desired allocation, because virtual disks have a maximum disk size. New disks are automatically used for event and report data storage. When creating a new disk, we recommend the following:
  - Disk Provisioning (Create a Disk page)—We recommend that you select the **Support Clustering Features Such As Fault Tolerance** option for the best thick-provisioning performance. However, thin provisioning is supported if you would rather take that approach.
  - Virtual Device Node (Advanced Options page)—Select an open SCSI slot.
  - Mode (Advanced Options page)—Select the **Independent** and **Persistent** options, so that the disk is not included in snapshots.

To change these settings, the VM must be powered off. Then, you can select the VM in the vSphere client, right click, and select **Edit Settings**.

See the VMware online help and documentation for details about using the vSphere client.

In addition, the PRSM installation guide provides more detail about the recommended settings, based on the number of devices you intend to manage, in the section on preparing the server. See the *Installation Guide for Cisco Prime Security Manager* for your version, available at http://www.cisco.com/en/US/products/ps12521/prod_installation_guides_list.html. There is also a detailed discussion of disk space management.

Information Required for PRSM Setup

When you initially start up PRSM, you will be prompted to configure a password for the admin user and then you will be placed in setup mode. During setup, you must be ready to enter the following information that is required to make the PRSM server operational. Before you power up the VM, be sure you determine the correct input for these values:

- **Host name for the system**.

  The hostname must be fewer than 65 characters and can contain characters, numbers, and hyphens only. The first and last character must be a letter or number and the hostname cannot be all numbers.

- **The type of addressing to use for the management IP address**.

  You can configure the following types of address: static IPv4, DHCP for IPv4, static IPv6, IPv6 stateless autoconfiguration. You can configure both IPv4 and IPv6 addressing. Do the following:

  - IPv4 static address—Determine the IPv4 management IP address, subnet mask, and gateway.
  - DHCP—Ensure there is a DHCP server that will respond on the management network.

    Note DHCP is not recommended. The system will stop functioning correctly if DHCP changes the assigned address due to lease expiration or other reasons. We suggest you use static addressing instead.

  - IPv6 static address—Determine the IPv6 management IP address and prefix length and gateway.
  - IPv6 stateless autoconfiguration—IPv6 stateless autoconfiguration will generate a global IPv6 address only if the link on which the device resides has a router configured to provide IPv6 services, including the advertisement of an IPv6 global prefix for use on the link. If IPv6 routing services are not available on the link, you will get a link-local IPv6 address only, which you cannot access outside of the device's immediate network link.

    Note IPv6 stateless autoconfiguration assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly. We suggest you use static addressing instead.

- **DNS information**.

  If you do not use DHCP, you need to specify the IP addresses (IPv4 or IPv6) of the primary and optionally, secondary, DNS servers and the local domain name. If you configure both IPv4 and IPv6 management addresses, you can enter DNS addresses in either or both formats; otherwise, you must match the format of the management address.

You can also enter a comma-separated list of search domains, which are sequentially appended to host names that are not fully qualified in an attempt to resolve the name to an IP address. For example, a search domain list would allow you to ping www instead of a fully-qualified name such as www.example.com.

- **NTP information**.

  You can decide whether to configure Network Time Protocol (NTP) for system time. When using NTP, specify the NTP server names or IPv4 addresses.

Note It is critical that system time be consistent among the CX device, its parent device, and PRSM management server. The best solution is to use NTP servers to maintain consistent time; time zones can be different, but the relative time must be equivalent. If there is a significant time mismatch, PRSM might not be able to add a device to the inventory, for example, if the start time of the CX CA certificate generated during the installation process is later than the current time on the PRSM server. Also, event and dashboard data can be skewed.

Configuring the PRSM Virtual Machine

When you are satisfied with the VM settings, and you have determined the setup information, it is time to power on the PRSM VM and complete its configuration.

Step 1 Open the vSphere Client and log into the appliance.

Step 2 Select the PRSM VM from the list of VMs on the server, and open the VM Console, either in the right pane or as a separate window (by clicking the **Launch Virtual Machine Console** button in the toolbar or selecting **Inventory > Virtual Machine > Open Console**).

Step 3 Power on the VM by clicking the **Power On** (Play) button in the main or Console window, or by selecting **Inventory > Virtual Machine > Power On**.

You will see the boot messages for PRSM in the Console window. Because the time required for disk initialization during initial boot is proportional to the amount of space you have allocated, the initial PRSM boot can take a long time. For example, initialization of a 5 TB disk can take 1-2 hours. Wait until you see the following message about configuring the admin password:

```
Press Enter to configure the password for 'admin' user ...
```

Step 4 Press Enter and specify the password for the **admin** user; your typing is not displayed.

```
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).

Enter password: (type password)
Confirm password: (retype password)
SUCCESS: Password changed for user admin


          Welcome to Cisco Prime Security Manager Setup
                    [hit Ctrl-C to abort]
                Default values are inside [ ]

Enter a hostname [prsm-vm]:
```

Step 5 You are now at the first prompt for the system setup wizard, which will guide you through the initial setup. You can rerun this wizard later using the **setup** command.

The following example shows the configuration of both IPv4 and IPv6 static addresses.

```
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management
interface? (y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
Please review the final configuration:
Hostname:               prsm-vm
Management Interface Configuration

IPv4 Configuration:     static
        IP Address:     10.89.31.65
        Netmask:        255.255.255.0
        Gateway:        10.89.31.1

IPv6 Configuration:     static
        IP Address:     2001:DB8:0:CD30::1234/64
        Gateway:        2001:DB8:0:CD30::1


DNS Configuration:
        Domain:         example.com
        Search:
                        example.com
        DNS Server:
                        10.89.47.11

NTP servers:
        1.ntp.example.com    2.ntp.example.com

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
 ...
Done.
Press ENTER to continue...
```

Step 6 Press Enter to continue.

The system places you at the login prompt and displays the URL you can use to open the web interface.

Step 7 Log back into the CLI using the admin username to check the time settings.

Step 8 If necessary, configure the time settings.

Use the **show time** command to determine the current date, time, and time zone for the system. The default is to use the UTC time zone.

If you are using NTP, you can configure the local time zone using the **config timezone** command. If you are not using NTP, also configure the local time using the **config time** command.

Maintaining the System

You should apply any applicable updates to the system. Look for updates to the following features:

- **Cisco Prime Security Manager**. Go to the software downloads page and look for maintenance releases or system software upgrades that apply to your system. You can get to the software downloads page from the main product page, http://www.cisco.com/go/prsm.

  Before upgrading to a new release, carefully read the compatibility matrix to ensure that the upgrade is allowed, and what effect the upgrade will have on the required ASA Software versions. Upgrading PRSM might require upgrades on all CX devices and even on ASA devices. See *Cisco CX and Cisco Prime Security Manager Compatibility*, http://www.cisco.com/en/US/docs/security/asacx/compatibility/cx_prsm_comp.html.
- **Cisco UCS server**. Go to the software downloads page for Cisco UCS C-Series Rack-Mount UCS-Managed Server Software and look for applicable updates. The direct link is http://www.cisco.com/cisco/software/type.html?mdfid=283862063&flowid=25886, or you can get to the page through the main product page, http://www.cisco.com/go/ucs.
- **VMware vSphere Hypervisor (ESXi)**. Look for updates on the VMware web site. The Help menu in the vSphere Client includes a link to check for updates.

Related Documentation

Use the following documentation road maps to find more information about these products:

- *Finding ASA CX and Cisco Prime Security Manager Documentation*, http://www.cisco.com/en/US/docs/security/asacx/roadmap/asacxprsmroadmap.html
- *Cisco UCS C-Series Servers Documentation Roadmap*, http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html

China RoHS Hazardous Substance Table

产品中有毒有害物质或元素的名称及含量

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价鉻	多溴联苯	多溴二苯醚
金属部件（包括紧固件）	×	○	○	○	○	○
印刷电路板组件和元件	×	○	○	○	○	○
缆线和缆线组件	×	○	○	○	○	○
塑料和聚合物部件	○	○	○	○	○	○
显示器，包含灯泡	×	×	○	○	○	○
除印刷版电路板外的其他电子组件	×	○	○	○	○	○
光学玻璃材料	×	○	×	○	○	○
干电池	○	○	○	○	○	○

○：代表此种部件的所有均质材料中所含的该种有毒有害物质均低于中华人民共和国信息产业部所颁布的《电子信息产品中有毒有害物质的限量要求》（SJ/T 11363–2006）规定的限量。

×：代表此种部件所用的均质材料中，至少有一类材料其所含的有毒有害物质高于中华人民共和国信息产业部所颁布的《电子信息产品中有毒有害物质的限量要求》（SJ/T 11363–2006）规定的限量。

以销售日期为准，此表显示在“思科系统公司”的电子信息产品部件中何处存在这些有毒有害物质。请注意，并非上列所有部件都包有含在内装产品中。

除非产品上另有标记，所有内附产品及其部件的‘环保使用期限’均由此显示的符号表示。此环保使用期限只适用于产品手册中所规定的使用条件。

Note This Table is a regulatory document required for products shipped to the People’s Republic of China.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What’s New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.