Cisco Security Manager 4.7 UCS Server Bundles Quick Start Guide

First Published: December, 2014

Caution Your Cisco Security Manager license is provided in paper format and is packed in your shipping carton along with your new Bundle itself. Please take care that it is not inadvertently discarded or lost.

Caution Recovery media (2 DVDs) are provided with your new Bundle. Please take care that they are not inadvertently discarded or lost.

Contents

Product Description, page 2

Deployment Mode—Standard Only; No HA or DR, page 3

Steps to Get Up and Running with Cisco Security Manager, page 3

BIOS Setup, OS Tuning, and Security Manager Tuning (these were done by Cisco before shipment of the Bundle to you), page 4

Performance Parameters, page 5

Updates and Service Packs for Windows, page 6

Patches and Service Packs for Security Manager, page 6

Usernames and Passwords, page 6

Windows Activation, Product Key, and EULA, page 7

Windows Drivers for the UCS Server, page 7

Updates and Service Packs for the UCS Server, page 7

Cisco Security Manager License, page 7

IP Address and Hostname, page 8

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Recovery Media and Recovery Procedure, page 9

If You Need to Return Your Bundle to Cisco, page 11

Related Documentation, page 11

Product Description

This printed copy of *Cisco Security Manager 4.7 UCS Server Bundles Quick Start Guide* ("Quick Start Guide") is provided with shipments of Cisco Security Manager 4.7 UCS Server Bundles. This "Quick Start Guide" is also available on Cisco.com at the following URL: http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

Cisco Security Manager 4.7 UCS Server Bundles ("Bundle") is a software and hardware bundle that was developed by Cisco Systems, Inc., for users of Cisco Security Manager. Cisco did the following things to develop this Bundle:

1. Selected a server, the Cisco UCS C220 M3, and configured it with appropriate HDDs, RAM, and other components *(this was done by Cisco before shipment of the Bundle to you)*.

   The Cisco UCS C220 M3 is a rack server in a 1RU form factor. You can see an interactive model of it at the following URL:

http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps12369/ucs_c220_kaon_model_preso.html

Note Two hardware configurations are available for this Bundle. However, this "Quick Start Guide" (and all the documentation referred to in it) applies to both of the available hardware configurations. The two hardware configurations are low-end (16 GB RAM, 4 x 500 GB HDD) and high-end (24 GB RAM, 7 x 500 GB HDD).

2. Set up the BIOS on the Cisco UCS server *(this was done by Cisco before shipment of the Bundle to you)*.
3. Installed the operating system, Microsoft Windows Server 2012 R2 Standard Edition ("the OS") *(this was done by Cisco before shipment of the Bundle to you)*.
4. Tuned the OS *(this was done by Cisco before shipment of the Bundle to you)*.
5. Installed Common Services 4.2.2, which provides the framework for installation, user role definitions, and many other functions *(this was done by Cisco before shipment of the Bundle to you)*.
6. Installed Cisco Security Manager 4.7 ("Security Manager") *(this was done by Cisco before shipment of the Bundle to you)*.
7. Tuned Security Manager *(this was done by Cisco before shipment of the Bundle to you)*.

The next steps—unpacking the shipping carton, obtaining an IP address, securing the Security Manager credentials, and all the rest—are to be taken by you as (1) the admin user of Security Manager and (2) the administrator of the Cisco UCS Server.

Cisco recommends that you read this "Quick Start Guide" and the other documentation that you will find packed in your shipping carton along with your new Bundle itself, especially the poster ("Cisco UCS C220 Server Quick Start Guide," Cisco 78-20790-02).

Also, please be sure to refer to the "Related Documentation" section of this "Quick Start Guide."

Please be aware of the following information regarding this product:

- An earlier Cisco product, Cisco Security Manager UCS Server Bundles, used Cisco Security Manager 4.3 and the Cisco UCS C220 M3 server.
  - You must first upgrade the Security Manager database from version 4.3 to version 4.5 and then to version 4.7.
  - However, the Security Manager-UCS Bundle cannot be upgraded because the two bundles use two different hardware platforms.
- SAN storage is not supported by this product. Also, NAS is not supported by this product.

Deployment Mode—Standard Only; No HA or DR

The Bundle is meant for standard deployment only: It does not provide support for high availability (HA) mode or disaster recovery (DR) mode; those modes require the installation of Veritas, which is not part of this bundle.

Steps to Get Up and Running with Cisco Security Manager

Step 1 Obtain and 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.

Step 2 Locate the document “Cisco UCS C220 Server Quick Start Guide” [poster, Cisco 78-20790-02], which is packed in your shipping carton.

Step 3 Verify that your shipping carton contains the following items:

a. the server itself,

b. the driver and utility disc,

c. the AC power cord (optional, up to two),

d. KVM console cable, and

e. Bundle accessory kit.

Step 4 Verify that the Bundle accessory kit in your shipping carton contains the following items:

a. this “Quick Start Guide” (any version)

b. the Cisco Security Manager license in paper format,

c. the Microsoft end-user license agreement in paper format,

d. the recovery media (2 DVDs), and

e. the Microsoft Certificate of Authenticity (COA) label (the COA label is placed on the recovery media).

Step 5 Use the “Cisco UCS C220 Server Quick Start Guide” poster to install the server in a rack.

Step 6 Use the “Cisco UCS C220 Server Quick Start Guide” poster to connect and power-on the server in Standalone Mode.

Step 7 Do not use UCSM mode.

Step 8 Do not update the BIOS; BIOS setup was done by Cisco before shipment of the Bundle to you; see BIOS Setup, OS Tuning, and Security Manager Tuning (these were done by Cisco before shipment of the Bundle to you), page 4.

Step 9 Do not update the CIMC firmware.

Step 10 Use the default username and password to log on to the OS; see Usernames and Passwords, page 6.

Step 11 Activate Windows. For more information, see Windows Activation, Product Key, and EULA, page 7

Step 12 Assign a static IP address to the server; see Assigning an IP Address, page 8.

Step 13 (Optional) Change the hostname; see Changing the Hostname, page 8.

Step 14 Ensure that required ports are enabled and available for use by Security Manager and its associated applications on your server so that the server can communicate with clients and servers running associated applications. For detailed information, refer to "Required Services and Ports" in the "Requirements and Dependencies" chapter of the *Installation Guide for Cisco Security Manager 4.7* at the following URL: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.7/installation/guide/requirem.html#wp1060450.

Step 15 Use the default username and password to log on to Cisco Security Manager; see Usernames and Passwords, page 6.

Step 16 Install the Cisco Security Manager license; see the "Updating Security Manager" section of the "Installing and Upgrading Server Applications" chapter of the *Installation Guide for Cisco Security Manager 4.7* at the following URL: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/installation/guide/IG/inserver.html#pgfId-1053144.

Caution Your Cisco Security Manager license is provided in paper format and is packed in your shipping carton along with your new Bundle itself. Please take care that it is not inadvertently discarded or lost.

Step 17 Refer, as needed, to the Related Documentation section of this "Quick Start Guide."

BIOS Setup, OS Tuning, and Security Manager Tuning *(these were done by Cisco before shipment of the Bundle to you)*

Before your new Bundle was shipped to you, Cisco set up the BIOS on the server, installed and tuned the operating system, and installed and tuned Security Manager.

BIOS settings done in the Cisco UCS server *(these were done by Cisco before shipment of the Bundle to you)*:

- Intel Hyper-Threading Technology enabled.
- Virtualization disabled.
- Mass Storage Controllers Configuration selected.

RAID configuration *(this was done by Cisco before shipment of the Bundle to you)*:

- Hardware RAID controller configured, with RAID 5 set up.

OS tuning and changes done in the Cisco UCS server *(these were done by Cisco before shipment of the Bundle to you)*:

- Disk cache policy configured.

- Virtual memory configured.
- Windows firewall disabled.
- Current Windows updates installed.
- Windows Update settings set to “Check for updates but let me choose whether to download and install them.”

Tip Windows firewall is disabled by default. If you want to enable Windows firewall, follow these steps:

a. Open Server Manager. (To open Server Manager, right-click **Computer** and click **Manage**. Or, select **Start > Programs > Administrative Tools > Server Manager**.)

b. Under “Security Information,” click **Go to Windows Firewall**.

c. Under “Overview,” click **Windows Firewall Properties**.

d. Under “State,” change “Firewall State” to “On.”

Note If you enable Windows firewall, all the required inbound ports for Security Manager are blocked by default. You must ensure that required ports are enabled and available for use by Security Manager and its associated applications on your server so that the server can communicate with clients and servers running associated applications. To find the list of ports that are required to be enabled in Windows firewall, refer to “Required Services and Ports” in the “Requirements and Dependencies” chapter of the *Installation Guide for Cisco Security Manager 4.7* at the following URL: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/installation/guide/IG/requirem.html#24624.

Cisco Security Manager tuning done *(this was done by Cisco before shipment of the Bundle to you)*:

- D:\ProgramFiles\CSCOpx used for installation.
- Default usernames and passwords established.

Performance Parameters

Your new Bundle was tuned for specific performance parameters:

The low-end hardware configuration (16 GB RAM, 4 x 500 GB HDD) provides support for 50 devices. This configuration is suitable for a small enterprise deployment. The maximum number (cumulative) of events per second supported is 5000 events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 4500 syslog + 500 SDEE)].

Note Cisco does not recommend (1) attempting to expand the capabilities of the low-end hardware configuration (16 GB RAM, 4 x 500 GB HDD) by adding licenses or hardware or (2) otherwise attempting to change the license configuration or hardware or both; the Bundle was tested as shipped.

The high-end hardware configuration (24 GB RAM, 7 x 500 GB HDD) provides support for 150 devices. This configuration is suitable for a medium enterprise deployment. The maximum number (cumulative) of events per second supported is 10,000 events per second [this value is a 9:1 ratio of syslogs to IPS SDEE (i.e., 9000 syslog + 1000 SDEE)].

Note Cisco does not recommend (1) attempting to expand the capabilities of the high-end hardware configuration (24 GB RAM, 7 x 500 GB HDD) by adding licenses or hardware or (2) otherwise attempting to change the license configuration or hardware or both; the Bundle was tested as shipped.

Updates and Service Packs for Windows

Your new Bundle was shipped to you with current Windows updates installed.

Also, Windows Update was set to "Check for updates but let me choose whether to download and install them."

Tip To change the Windows Update setting, select **Control Panel > System and Security > Windows Update > Let me Choose My Settings.**

As the administrator of the Cisco UCS Server which forms part of this Bundle, you are responsible for the necessary updates and service packs for Windows. Cisco does not provide Windows updates or service packs.

Patches and Service Packs for Security Manager

Your new Bundle was shipped to you with the Cisco Security Manager version 4.7. No Security Manager patches or service packs were installed.

As the admin user of Security Manager installed on this Bundle, you are responsible for the necessary patches and service packs for Security Manager. Cisco does not install them for you or notify you.

If you have a valid Cisco Service contract, you will be able to upgrade the Cisco Security Manager software from version 4.7 to a future 4.x version.

Usernames and Passwords

Windows:

- Default Windows username/password: Administrator/cisco@123
- To change the Windows username/password: Follow the procedures published by Microsoft for Windows Server 2012.

Security Manager admin:

- Default Security Manager admin username/password: admin/cisco@123
- To change the Security Manager admin username/password: In Security Manager, select **Tools > Security Manager Administration > Server Security**, then click **Local User Setup**.

Security Manager casuser:

- Default casuser username/password: casuser/*[Note: password is generated by Security Manager during installation]*
- To reset the casuser password, follow the procedure for **resetCasuser.exe** in the *Installation Guide for Cisco Security Manager 4.7* at http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

Windows Activation, Product Key, and EULA

Activation of the OS [Microsoft Windows Server 2012 R2 Standard Edition] must be done by you before the activation period expires. To activate the OS, use the Microsoft Certificate of Authenticity (COA) label; the COA label is placed on the recovery media provided with your new Bundle. For more information on activating the OS, refer to "Product Activation," published by Microsoft at the following URL: http://www.microsoft.com

You can view your product key by using normal Microsoft procedures: On the Control Panel, select **System** and refer to the information under "Windows Activation."

To activate the OS, use the Physical Key. Do not use the Virtual Key.

The Windows EULA (end user license agreement) is described in a printed document that you will find packed in your shipping carton.

Windows Drivers for the UCS Server

The required Windows UCS drivers are pre-installed in your new Bundle.

If necessary, you can download these drivers at the following URL:

http://www.cisco.com/cisco/software/type.html?mdfid=284296253&i=rs

Updates and Service Packs for the UCS Server

Cisco periodically releases updates and service packs for its UCS servers. As the administrator of the Cisco UCS Server which forms part of this Bundle, you are responsible for the necessary updates and service packs, which you can obtain by visiting http://www.cisco.com/go/ucs. You can also use the following hyperlink, which is the direct URL:

- Cisco UCS C220 M3 Rack Server Software: http://www.cisco.com/cisco/software/type.html?mdfid=284296253&i=rs

Cisco Security Manager License

Caution Your Cisco Security Manager license is provided in paper format and is packed in your shipping carton along with your new Bundle itself. Please take care that it is not inadvertently discarded or lost.

This Bundle includes the following license support:

- The low-end hardware configuration (16 GB RAM, 4 x 500 GB HDD) provides support for 50 devices.

Note Cisco does not recommend (1) attempting to expand the capabilities of the low-end hardware configuration (16 GB RAM, 4 x 500 GB HDD) by adding licenses or (2) otherwise attempting to change the license configuration; the Bundle was tested as shipped.

- The high-end hardware configuration (24 GB RAM, 7 x 500 GB HDD) provides support for 150 devices.

Note Cisco does not recommend (1) attempting to expand the capabilities of the high-end hardware configuration (24 GB RAM, 7 x 500 GB HDD) by adding licenses or (2) otherwise attempting to change the license configuration; the Bundle was tested as shipped.

Note Evaluation licenses are not available for this Bundle.

IP Address and Hostname

Assigning an IP Address

During deployment of your new Bundle at your site, you must assign the server a static IP address. (Security Manager requires one IP address. It must be a static IP address; dynamic IP addresses are not supported.)

To assign the server a static IP address, first obtain a static IP address from your network administrator and then follow the procedures for IP address assignment published by Microsoft for Windows Server 2012.

Changing the IP Address

To change the IP address of your server, follow the procedures for IP address assignment published by Microsoft for Windows Server 2012, as you did when first assigning an IP address.

After changing the IP address of your server, you must restart the Security Manager Daemon Manager by executing the following commands in a command window:

net stop crmdmgtd

net start crmdmgtd

Changing the Hostname

The default hostname for the low-end hardware configuration (16 GB RAM, 4 x 500 GB HDD) is CSM4-UCS2-50HW. The default hostname for the high-end hardware configuration (24 GB RAM, 7 x 500 GB HDD) is CSM4-UCS2-150HW.

To change the hostname of your new Bundle, take the steps listed in the following procedure.

Caution If the hostname of the machine changes, the stability of the system is not guaranteed and it fails in some cases.

Procedure

Step 1 Change the hostname in the OS:

a. Right-click **Computer** and select **Properties**. Or, open **Control Panel** and select **System**.

b. Under "Computer name, domain, and workgroup settings," click **Change settings**.

c. Click **Change** to change the hostname.

d. Restart the computer.

Step 2 Stop the Security Manager Daemon Manager by executing the following command in a command window:

net stop crmdmgtd

Step 3 Execute the CiscoWorks server hostname change script by executing the following command in a command window:

*NMSROOT***bin\perl** *NMSROOT***bin\hostnamechange.pl**

In this command, *NMSROOT* is the path to the Security Manager installation directory. The default installation directory is D:\ProgramFiles\CSCOpx.

Tip **hostnamechange.pl** is a utility that updates the hostname changes in Common Services-related directories, files, database entries, and registry entries after the hostname is changed in the OS.

Step 4 Restart the computer.

Note In this step, you must restart the computer. Restarting the Security Manager Daemon Manager is not sufficient.

Recovery Media and Recovery Procedure

Caution Recovery media (2 DVDs) are provided with your new Bundle. Please take care that they are not inadvertently discarded or lost.

Note There is no recovery partition.

Caution The purpose of the following procedure is to install Windows and Cisco Security Manager from the start; installing Windows will delete all existing Windows files and data present in the Windows (C:\) partition on the server. Files present in the Security Manager (D:\) partition will not be deleted. If required, back up the files present on the server and ensure that you have the Security Manager database backup stored on another server before proceeding.

If disk corruption or other hardware failure occurs, you can use the recovery media provided with your new Bundle to restore the OS and Security Manager. Take the steps listed in the following procedure.

Procedure

Step 1 From a laptop or other PC, log in to CIMC on the UCS server using Internet Explorer:

https://*<CIMC_IPAddress>/*

Refer to the UCS documentation for setting up the CIMC IP address:

http://www.cisco.com/en/US/partner/products/ps10493/prod_installation_guides_list.html

Step 2 Launch the KVM console from the CIMC web UI.

Step 3 Insert the windows recovery media in the DVD drive of the laptop or other PC.

Step 4 Mount/Map the DVD drive as virtual media from the KVM console.

Step 5 Boot the UCS server into the EFI shell.

Step 6 From the EFI shell execute following command to start Windows installation.

```
fs1:\EFI\BOOT\BOOTX64.EFI
```

Step 7 Under “Select the Operating System you want to install” select option 2 to install “Windows Server 2012 R2 Standard (Server with the GUI)”.

Step 8 At the end of installation, enter the Windows 2K12R2 x64 administrator password.

Step 9 Download and install the UCS C220 M3 windows 2K12R2 x64 drivers for chipset and network devices.

Refer to the UCS documentation for installing the Windows drivers:

http://www.cisco.com/en/US/partner/products/ps10493/products_user_guide_list.html

Step 10 Turn off the Windows firewall.

Step 11 Set the Windows auto update option to “Check for updates but let me choose whether to download and install them.”

Step 12 Configure the static IPv4 IP address for the NIC and enable RDP if needed.

Step 13 Configure the custom virtual memory for C: as specified below:

- For installed RAM = 16 GB, configure Initial = 16384 MB and Max = 24576 MB.
- For installed RAM = 24 GB, configure Initial = 24576 MB and Max = 36864 MB.

Step 14 Activate Windows using the physical key shipped with the product.

Step 15 Format or delete all files present in **D:** drive.

Step 16 Download Security Manager 4.7 installer from www.cisco.com. Launch the command prompt and navigate to the folder where you saved the Security Manager installer. At the command prompt run the following command to start the Security Manager installation.

setup.exe ignoreos

This is done to ignore any Windows installation related warnings that Security Manager generates.

Step 17 Install the Security Manager 4.7 server application on the server in the following path:

`D:\ProgramFiles\CSCOpx`

Refer to the Security Manager installation guide for installing Security Manager:

http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html

Step 18 Download and install the latest service pack for Cisco Security Manager 4.7.

Step 19 Update the Event store size as specified below from the Security Manager client:

a. Navigate to Configuration Manager > Tools > Security Manager Administration > Event Management.

b. For installed RAM = 16 GB, configure "Event data store disk size" = 1000.

c. For installed RAM = 24 GB, configure "Event data store disk size" = 2000.

Step 20 Download and restore the Security Manager database backup created earlier (please refer to the Caution immediately preceding this procedure); doing so also will restore the Security Manager license.

If You Need to Return Your Bundle to Cisco

If you need to return your Bundle to Cisco because of hardware failure or some other reason that requires you to request an RMA, please note the following:

- When returning your Bundle to Cisco, be sure to include everything that was shipped to you. In particular, please be sure to return the recovery media; the Microsoft Certificate of Authenticity (COA) label is placed on the recovery media sleeve and must be returned.

Related Documentation

The following documentation is for the **Software (Cisco Security Manager 4.7)** in this Bundle:

- "Guide to User Documentation for Cisco Security Manager 4.7" (the "documentation roadmap"): http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/roadmap/CSM47Map.html?mdfid=286280114
- Main page for Cisco Security Manager on Cisco.com: http://www.cisco.com/go/csmanager
- Chapter 1 (the "Getting Started" chapter) of *User Guide for Cisco Security Manager 4.7*: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/user/guide/CSMUserGuide/wfplan.html

The following documentation is for the **Hardware (Cisco UCS C-Series Rack-Mount Servers)** in this Bundle:

- "Cisco UCS C220 Server Quick Start Guide" [poster, Cisco 78-20790-02], which is packed in your shipping carton along with your new Bundle itself
- "Cisco UCS C-Series Servers Documentation Roadmap" describes the user documentation available for Cisco Unified Computing System (UCS) rack mount servers: http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html
- "Unified Computing and Servers" main page on Cisco.com: http://www.cisco.com/go/ucs

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.