CSPC Collection Platform Software
Installation and Configuration Guide

July, 2019

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networks, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CSPC Collection Platform Software Installation and Configuration Guide
Copyright © 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

Introduction 1-1

Introduction to CSPC Collection Platform Software 1-1
Who Should Use This Guide 1-1
Ordering Process 1-1

CHAPTER 2

Installation and Configuration 2-1

OVA Installation 2-1
Pre-requisites 2-1
Deploy CSPC OVA 2-1
  Configure IPv4 address 2-7
  Configure IPv6 Address 2-8
  Configure the IP address directly on shell 2-9
Enable Default Account 2-10
Set GURB Password 2-11
ESXi Patch Installation 2-12
Prerequisites 2-12
Upgrade ESXi 6.0 2-12
CSR1000V NAT OVA Installation 2-12
Prerequisites 2-12
CSR1000v Upgrade 2-19
CIMC Patch Installation 2-21
NOS Configurer 2-22
  Installation Sequence For nos_configurer 2-22
Introduction

Introduction to CSPC Collection Platform Software

The Cisco Common Service Platform Collector (CSPC) is an SNMP-based tool that discovers and collects information from the Cisco devices installed on your network. The CSPC software provides an extensive collection mechanism to gather various aspects of customer device data. Information gathered by the collector is used by several Cisco Service offers, such as Smart Net Total Care, Partner Support Service, and Business Critical Services. The data is used to provide inventory reports, product alerts, configuration best practices, technical service coverage, lifecycle information, and many other detailed reports and analytics for both the hardware and operating system (OS) software.

This guide explains how to use install and configure CSPC Server. Refer to CSPC User Guide to use the application.

For program updates and important notes, refer to CSPC Release Notes and README documentation.

Who Should Use This Guide

This guide is written for Network and Security Administrators and Cisco Network Engineers and also for new users.

The user should have Administrative privileges on the machine to install CSPC.

Ordering Process

To order a M5 hardware you need to do the following:

- **Step 1** Navigate to Cisco Commerce Website CCW and to learn how to using CCW navigate to Cisco_Commerce_User_Guide.pdf
- **Step 2** Enter the chassis part number **UCSC-C220-M5SX** to search as shown below and select the exact part number from the list and then click **Add**.
Step 3  Click **Select Options** link at the bottom of the page to select all the hardware components for the selected UCSC-C220M5SX chassis.

---

**Figure 1-1  Search**

![Image of Search interface]

**Figure 1-2  Options**

![Image of Options interface]
Step 4  After the **Select Options** link is selected, the following screen will be displayed. On LNP, select the **Country** where this M5 hardware will be installed. Although this is optional, it is recommended to select the correct country so that proper cabling that apply to the selected country will be applied.

**Figure 1-3  Country**

<table>
<thead>
<tr>
<th>Configuration Summary</th>
<th>View Full Summary</th>
<th>Global Price List (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DC Persistent Memory Operational Mode</td>
<td>Advanced Memory Settings</td>
<td></td>
</tr>
<tr>
<td>RAID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOCAL STORAGE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SKU</th>
<th>Qty</th>
<th>Estimated Lead Time</th>
<th>Unit List Price (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS-CPU4876</td>
<td>Qty</td>
<td>26 days</td>
<td>25,250.00</td>
</tr>
<tr>
<td>UCS-CPU4878</td>
<td>Qty</td>
<td>26 days</td>
<td>25,150.00</td>
</tr>
<tr>
<td>UCS-CPU4876C</td>
<td>Qty</td>
<td>61 days</td>
<td>19,360.00</td>
</tr>
<tr>
<td>UCS-CPU4842</td>
<td>Qty</td>
<td>26 days</td>
<td>19,060.00</td>
</tr>
<tr>
<td>UCS-CPU4842C</td>
<td>Qty</td>
<td>61 days</td>
<td>8,560.00</td>
</tr>
<tr>
<td>UCS-CPU4842G</td>
<td>Qty</td>
<td>26 days</td>
<td>8,060.00</td>
</tr>
<tr>
<td>UCS-CPU4842G+</td>
<td>Qty</td>
<td>26 days</td>
<td>5,480.00</td>
</tr>
<tr>
<td>UCS-CPU4842G+H</td>
<td>Qty</td>
<td>26 days</td>
<td>4,220.00</td>
</tr>
<tr>
<td>UCS-CPU4842H+</td>
<td>Qty</td>
<td>26 days</td>
<td>3,780.00</td>
</tr>
</tbody>
</table>

Simplified Step 4:

1. After the **Select Options** link is selected, the following screen will be displayed.
2. On LNP, select the **Country** where this M5 hardware will be installed.
3. Although this is optional, it is recommended to select the correct country so that proper cabling that apply to the selected country will be applied.
Step 5  On LNP click **Processor**, then from right side select the **UCS-CPU-4110** processor from the processor list as show below.

**Figure 1-4  Processor**
**Step 6** ON LNP click the **Memory**, then from the right side select the **UCS-MR-X16G1RS-H** from the memory list as shown below.

![Figure 1-5 Memory](image)

- **UCS-MR-X16G1RS-H**
  - Quantity: 1
  - Price: $1,099.80

**Table 1-5**

<table>
<thead>
<tr>
<th>DRAM</th>
<th>Qty</th>
<th>Estimated Lead Time</th>
<th>Unit List Price (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>128GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>28 days</td>
<td>$4,995.00</td>
</tr>
<tr>
<td>64GB DDR4-2933MHz UDIMM</td>
<td>Qty</td>
<td>28 days</td>
<td>$4,896.00</td>
</tr>
<tr>
<td>32GB DDR4-2933MHz UDIMM</td>
<td>Qty</td>
<td>28 days</td>
<td>$2,843.00</td>
</tr>
<tr>
<td>16GB DDR4-2933MHz UDIMM</td>
<td>Qty</td>
<td>28 days</td>
<td>$1,609.00</td>
</tr>
<tr>
<td>32GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>42 days</td>
<td>$40,800.00</td>
</tr>
<tr>
<td>16GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>42 days</td>
<td>$13,800.00</td>
</tr>
<tr>
<td>128GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>14 days</td>
<td>$18,800.00</td>
</tr>
<tr>
<td>64GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>14 days</td>
<td>$5,820.00</td>
</tr>
<tr>
<td>32GB DDR4-2666MHz UDIMM</td>
<td>Qty</td>
<td>14 days</td>
<td>$4,720.00</td>
</tr>
</tbody>
</table>
Step 7  On LNP click the **SAS/SATA HDD**, then from the right side select the **UCS-HD1T7K6GAN** from the SATA HDD list shown below.

### Figure 1-6  SAS/SATA HDD
Step 8  On LNP click **UCS C-Series CIMC Version**, then from the right side select the **CIMC-Latest** from the CIMC version list as shown below.

**Figure 1-7  UCS C-Series CIMC**

Step 9  On LNP click **Power Supply**, then from the right side select **UCSC-PSU1-1050W** as shown below.

**Figure 1-8  Power Supply**

**Note** Once the power supply type is selected, the system automatically adds the correct power cable and in this example the product part number for the corresponding cable is CAB-9K12A-NA
Step 10  On LNP click the Rail Kit Accessories, then from the right side select UCSC-RAILB-M4 from the Rail Kit Accessories list as shown below.

Figure 1-9  Rail Kit Accessories

Step 11  On LNP click Infrastructure Options, then from the right side select UCS-SID-INFR-OI from the Infrastructure Options list as shown below.

Figure 1-10  Infrastructure Options
Step 12  On LNP click **Workload Options**, then from the right side select **UCS-SID-WKL-OW** from the Workload Options list as shown below.

**Figure 1-11  Workload Option**

Step 13  A prompt appears, click **Done**

**Figure 1-12  Prompt**
In the main screen, if you expand the + sign for the USCS-C220-M5SX chassis the entire components will be expanded, and you will see the following configurations for your M5.

**Note**
These remaining items will be automatically added based on the configuration:
- UCS-HS-C220M5
- UCSC-BBLKD-S2
- UCSC-SATAIN-220M5
- UCSC-PSU-M5BLK

**Figure 1-13** M5 Configuration
CHAPTER 2

Installation and Configuration

CSPC Server image comes with a preloaded application that consists of server software, database, and all the necessary tools.

OVA Installation

This section describes detailed installation procedures for different installation stages.

Pre-requisites

For an uninterrupted deployment, installation, and configuration of CSPC software, have these ready:

- \textit{xxx.ova} file form the download center
- CSPC static IP address, default gateway IP address and subnet mask. This is recommended only if DHCP is not enabled.

Deploy CSPC OVA

This section describes the steps to deploy CSPC OVA using VMWare vSphere Client:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Get the xxx.ova file either to a web server or local file system where vSphere client is available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Launch vSphere client and login using credentials with the privilege to deploy an OVA file</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use vSphere client and select the ESXi host or IP address that manages CSPC virtual machine</td>
</tr>
<tr>
<td>Step 4</td>
<td>Use vSphere client and select the File menu and then select the Deploy OVF Template… menu item shown in the file menu.</td>
</tr>
<tr>
<td>Step 5</td>
<td>There are two ways to select the OVF file to deploy:</td>
</tr>
<tr>
<td></td>
<td>• Select the OVF file residing on local or a remote web server using web browser. If this option is selected, type the URL for the file \textit{xxx.ova}, then click Next.</td>
</tr>
<tr>
<td></td>
<td>• Select the OVF file residing locally using the file explorer. If this option is selected, click Browse… and navigate the file explorer to locate the file \textit{xxx.ova}, then click Next.</td>
</tr>
</tbody>
</table>

\textbf{Note} All the screens below are just for illustration and not actual ones
Step 6  Browse to select the URL and click Next to proceed
Step 7  Click **Next** to proceed

*Figure 2-3  Verify OVF Template Details*

Step 8  Click **Accept** to acknowledge the end user agreement.

*Figure 2-4  End User Agreement*
Step 9  Select the appropriate storage to store the virtual machine then click **Next** to proceed.

*Figure 2-5  Name and Location*

Step 10  Select the required configuration and click **Next**

*Figure 2-6  Deployment Configuration*
Step 11   Click Next to proceed

*Figure 2-7    Disk Format*

Step 12   Map the network use and click Next.

*Figure 2-8    Network Mapping*
Step 13  Choose the **Power on after deployment**, then click **Finish**

**Figure 2-9  Ready to Complete**

Deployment progress screen appears. Wait for the deployment to complete.

**Figure 2-10  Deployment progress**

After successful installation of CSPC OVA, you have to configure IP address.

**Step 1**  Click on the new installed CSPC OVA.
You will be prompted to enter your password. First enter the password and confirm the password.

**Note**
Be sure to save this password in a secure, accessible location. The Admin password is needed to access the Admin Shell (CLI).

Once you enter your password, you will be able to configure the IP from the menu or in the command shell prompt.

No matter which method you use to configure the IP address, be sure to connect to the admin shell to initialize the collectorlogin and root users.

**Configure IPv4 address**

**Step 1** Select 1 to configure IPv4 address

- Select the any one option:
  - Select 1 to fetch IP address automatically.
Figure 2-13  DHCP

Select 2 to enter the IP Address manually.

Figure 2-14  IP Address Manually

Select 3 to go back to main menu

**Configure IPv6 Address**

**Step 2**  Select 2 to configure IPv6 address
- Select the any one option:
  - Select 1 to fetch IP address automatically.
Configure the IP address directly on shell

**Step 1** Select 3 to view Command line (Shell)

**Note** Only admin users can configure IP. Before configuring IP switch over as an admin user.
Step 2  Enter the command `conf ip -v4 eth0` or `conf ip -v6 eth0` and enter IP Address, Subnet mask, and gateway as show in the figure.

Figure 2-17  Conf ip command

```
admin> conf ip =

Usage:
admin> conf ip <type> <intf> <ipaddr> <netmask> <gateway>
admin> conf ip -v4 <intf> <ipaddr> <netmask> <gateway>
admin> conf ip -v6 <intf> <ipaddr>/prefix > gateway>
where prefix Should be between 1 and 128
```

Confirm your IP address settings

# show ip

Enable Default Account

To initially set or reset the password use the below command:

---

Step 1  Enable the Linux user login "collectorlogin"

# pwdreset collectorlogin 90

This generates a password for the username "collectorlogin."

Step 2  Enable the Linux root login

# pwdreset root 90

This generates a password for the username "root".

To connect to root first connect to the collectorlogin prompt and then use the command `su root`

$ su root

---

Note

- Be sure to save both the collectorlogin and root passwords in a secure, accessible location!
- You are not allowed to connect directly to root, attempts to connect directly to the user root will cause a lock on that account!
Note

- You can now connect to the server using SSH or through a browser at address https://<IP Address of the Collector>:8001
- There are additional commands on the admin shell. To display them just do the following:

  # ?

Set GURB Password

**Step 1**  Login as a root user.
**Step 2**  Execute the command `grub-crypt > /var/tmp/Gpass`
**Step 3**  Provide the password and make sure you save this password
**Step 4**  Execute the below commands in sequence:

```
fp=$(cat /var/tmp/Gpass)
P="password --encrypted $fp"
```
```
sed -i '/password/d' /boot/grub/grub.conf
sed -i "12i\"$P\"" /boot/grub/grub.conf
sed -i "s/\r//g" /boot/grub/grub.conf
sed -i 's/\password/password/g' /boot/grub/grub.conf
rm -rf /var/tmp/Gpass
```
ESXi Patch Installation

Prerequisites

- Make sure all the virtual machines are powered off before proceeding for Upgrade.
- After upgrade from ESXi 5.x to ESXi 6.x, old 5.x license key will be deleted and you are required to add 6.x license key for VMs in ESXi to work.

Upgrade ESXi 6.0

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Login to collector appliance as admin</td>
</tr>
</tbody>
</table>
| 2    | To check updates for ESXI execute below command:  
      # check update esxi |
| 3    | To download the ESXI patch execute below command:  
      # download jeos-100.0.6-0-lnx64 |
| 4    | To check download status execute below command:  
      # show download |
| 5    | Once the patch is downloaded to /opt/LCM/tmp, unzip the patch and follow the instructions from Read_me_ESXI_6.0U3_and_6.0_patch_build_9313334.docx |

CSR1000V NAT OVA Installation

Prerequisites

You require all these noted below before you start deploying CSRV

- ESXI Login IP and credentials.
- Existing NAT router / Pfense VM login IP and credentials.
- Copy of NAT rules and other customized configuration on old NAT router VM that required to be replaced.
- VSphere client to connect to ESXI.
- CSR1000V CSPC NAT OVA available locally or on network to deploy. Default credentials of the OVA.

This section describes steps to deploy CSR1000V CSPC NAT OVA using VMWare vSphere Client:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Get the xxx.ova file either to a web server or local file system where vSphere client is available</td>
</tr>
<tr>
<td>2</td>
<td>Launch vSphere client and login using credentials with the privilege to deploy an OVA file</td>
</tr>
<tr>
<td>3</td>
<td>Use vSphere client and select the ESXi host or IP address that manages NAT virtual machine</td>
</tr>
</tbody>
</table>
Step 4  Use vSphere client and select the File menu and then select the **Deploy OVF Template...** menu item shown in the file menu.

Step 5  Select the OVA file residing locally using the file explorer. If this option is used, click **Browse...** and navigate the file explorer to locate the file `xxx.ova`, then click **Next**.

*Figure 2-19  Deploy OVF Template*

Step 6  Browse to select the URL and click **Next** to proceed

*Figure 2-20  Source*

Step 7  Click **Next** to proceed
Step 8 Select the appropriate storage to store the virtual machine then click **Next** to proceed.

Step 9 Click **Next** to proceed.
Figure 2-23  Disk Format

Step 10  Map the network use and click Next.

Figure 2-24  Network Mapping

Step 11  Choose the Power on after deployment, then click Finish.
Step 12 Deployment is completed. Click **Close**.

After successful installation of OVA, you have to configure CSR1000V CSPC NAT OVA. To configure CSR1000V CSPC NAT OVA, perform the following:

Step 1 Take Snapshot of old Pfsense and Power OFF old Pfsense VM.
Step 2  Right click on new CSR1000V VM, and select **Open Console**. Once Router up and running, press **Enter** key. It navigates to console mode of router.

Step 3  In router console mode, enter **en** and press **Enter** key and provide default password **XXxxXX** (contact CSPC support for default password).
Step 4 Enter `conf t`, it navigates to router’s configure terminal mode.

Step 5 Enter `int gi1`, it navigates to wan interface configuration mode. (provide IP address and Netmask)

```
ip address <ipaddress> <netmask>
no shutdown
exit
```

Step 6 Provide default gateway and default routing in configuration mode and exit and save the configuration.

```
ip default-gateway <gateway IP>
ip route 0.0.0.0 0.0.0.0 <gateway IP>
exit
wr mem
```

Step 7 To verify the Configuration use the command `sh run`
Step 8  CSR1000V router is configured with IP and accessible from WEB UI. Login to WEB UI by URL http://<IP Address> and username root and password XXxxXX (contact CSPC support for password, CLI and UI will have same password).

Note: This CSR V Nat router OVA can be accessed from ESXI console or by CLI using telnet from private network VMs only. (You need to login to CSPC or other VMs on that host by using CLI and do telnet to CSR1000V IP or 192.168.1.1)

Once configuration is completed on CSRV1000V router you will be able to access CSPC and other VMs from CLI and UI.

**CSR1000v Upgrade**

To upgrade CSR1000V, perform the following:

**Step 1** Get new CSR1000v System Image(xxx.bin) to CSR1000V VM under bootflash: directory.

**Step 2** Run dir bootflash: command to view list of all files and directories in bootflash.
Example: Router# dir bootflash:

Step 3 Run configure terminal command to enter global configuration mode.
Example:
Router# configure terminal
Router(config)#

Step 4 Run no boot system command to delete all entries in the boot-able image list. That specifies the order in which the router attempts to load the system images at the next system reload or power cycle.
Example: Router(config)# no boot system

Step 5 Run boot system bootflash:<system-image-filename>.bin command to load the new system image after the next system reload or power cycle. For example:
Example: Router(config)# boot system bootflash:<system-image-filename>.bin

Step 6 Run exit command to exit global configuration mode
Example:
Router(config)# exit
Router#

Step 7 Run write or write memory command to update the GRUB menu list of images available on the bootflash disk.
Example: Router# write memory

Step 8 Run show version command to display the configuration register setting.
Example:
Router# show version
Cisco IOS XE Software, Version 16.06.04
...
Cisco Internetwork Operating System Software...
...
Configuration register is 0x2102
Router#

Step 9 If the last digit in the above output in Step 8, in configuration register is 0 or 1, proceed to next Step 10. Or if the last digit in the configuration register is between 2 and F, proceed to the Step 13.

Step 10 Run configure terminal command to enter global configuration mode.
Example:
Router# configure terminal
Router(config)#

Step 11 Run config-register 0x2102 command to set the configuration register so that, after the next system reload or power cycle, the router loads system image from the boot system commands in the startup configuration file.
Example: Router(config)# config-register 0x2102

Step 12 Run exit command to exit global configuration mode
Chapter 2  Installation and Configuration

CSPC  Collection Platform Software Installation and Configuration Guide

CIMC Patch Installation

Step 1  Login to collector appliance as admin

Step 2  To check updates for CIMC execute below command:

    #check update cimc

Step 3  To download the CIMC patch execute below command (M3 server):

    #download jeos-101.0.3-0-lnx64

Step 4  To download the CIMC patch execute below command (M4 server):

    #download jeos-101.0.4-0-lnx64

Step 5  To check download status execute below command:

Example:
Router(config)# exit
Router#

Step 13 Run copy running-config startup-config command to copy the running configuration to the startup configuration.
Example: Router# copy running-config startup-config

Step 14 Run write memory command to update the GRUB menu list of images available on the bootflash disk.
Example: Router# write memory

Step 15 Run reload command to reload the operating system.
Example: Router# reload

Step 16 When prompted to save the system configuration, enter no
Example:
System configuration has been modified. Save? [yes/no]: no

Step 17 When prompted to confirm the reload, enter y
Example:
Proceed with reload? [confirm] y

Step 18 Run show version command to verify that the router loaded the proper system image:
Example:
Router# show version
Cisco IOS XE Software, Version 16.09.02
Cisco IOS Software [Fuji],......
...
System returned to ROM by reload
System image file is "bootflash:csr1000v-xxx"
Last reload reason: Reload Command...
#show download

**Step 6** Once the patch is downloaded to `/opt/LCM/tmp`, unzip the patch and follow the instructions from `Read_me_CIMC_3.0(4i).docx`

## NOS Configurer

### Installation Sequence For nos_configurer

**Note** This is only for NOS

This section shows the instructions on how to install nos_configurer_2.8 on CSPC 2.8, and to configure CSPC for NOS specific functionalities.

**Note**
- The NOS Configurer, RI Addons should be installed manually which are present in the $CSPCHOME/installer/manual folder.
- There is no updates on nos_configurer in CSPC 2.8. So, you can follow the same steps below.

**Note** This only for fresh nos installation

It performs the following tasks:

1. Schedule jobs to carry out NOS functionalities
   
   Following jobs are scheduled:
   - Weekly Inventory Job
   - Daily Upload Job
   - Daily DAV Job
   - Daily Health Upload Job

2. Adds dependency rules to maintain data consistency

Follow the steps given below to install nos_configurer_2.8 on CSPC 2.8:

**Step 1** Terminal login to CSPC appliance

**Step 2** Navigate to path `$CSPCHOME/installs/manual`

**Step 3** Unzip the file `nos_configurer_2.8.zip`

**Step 4** On unzipping, a folder named `nos_configurer_2.8` is created

**Step 5** Enter the command:

```
  a. cd nos_configurer_2.8
  b. sh nos_cspc_2.8_patch.sh <username> <pwd> <fullInventoryDay> <hourOfFullInventory> <hourOfUpload>

  Example: sh nos_cspc_2.8_patch.sh <username> <pwd> 1 22 23
```
Note: You can install the installer without giving above three optional arguments. This will install support installer with default values as 1, 23 and 23.

In the above example:
1..7 = Sunday to Saturday
1…23 = hours in a day.

Step 6: On triggering the above command, it will prompt for user confirmations. Provide them accordingly.

a. Do you want to cancel installation and rerun with additional arguments? Enter Y or N: (y/n)? N
b. Do you want to cancel installation and rerun with different scheduling day and hours? Enter Y or N: (y/n)? N
c. Do you want to schedule health job immediately? Enter Y or N: (y/n)? Y
d. Do you want to schedule inventory/DAV/Upload job immediately? Enter Y or N: (y/n)? Y
e. Restarting the server to make sure inventory is not running. Do you want to continue? Enter Y or N: (y/n)? N

Note: You have the option to schedule the job now or later.