

Installation Guide for Cisco Contact Center SIP Proxy (CCCSP)

First Published: 2025-11-26

Last Modified: 2026-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

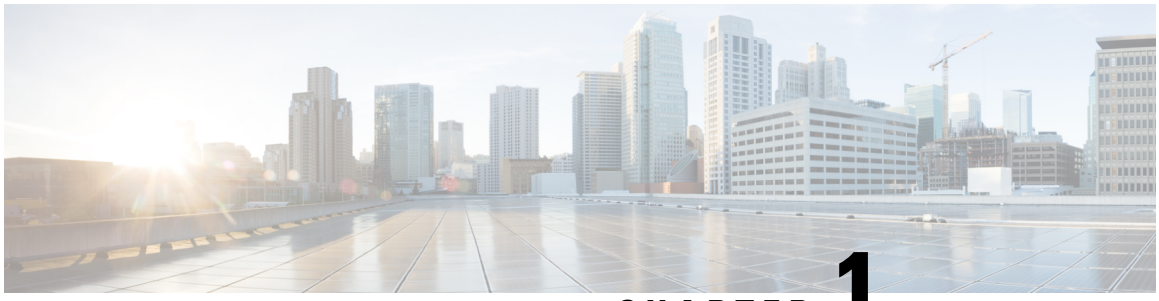
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned 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. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Installation Guide for Cisco Contact Center SIP Proxy (CCCSP)

- Feature History, on page 1
- Overview, on page 1
- System Requirements for Installation, on page 2
- IP Address Requirements, on page 3

Feature History

This table lists all the changes made to Cisco Contact Center SIP Proxy (CCCSP) Installation guide, the most recent changes appearing at the top.

Feature Information	Releases
Support for Nutanix AHV 10.0, AOS 7.0, PC 2024.3 Support for VMware vSphere ESXi 7.0.x and above	CCCSP-15.0(1) SU2
Initial release of Cisco Contact Center SIP Proxy (CCCSP). Support for VMware vSphere ESXi 7.0.x and above	CCCSP-15.0(1)

Overview

Cisco Contact Center SIP Proxy (CCCSP) is supported on both VMware ESXi and Nutanix AHV virtualized environment. The software is packaged as an ISO and is deployed using an OVA template within these environment.

For detailed information regarding your specific environment, please refer to the following resources:

- ESXi environment, see https://www.vmware.com/products/cloud-infrastructure/vsphere-foundation
- Nutanix AHV environment, see https://www.nutanix.com/products/ahv

Cisco Contact Center SIP Proxy (CCCSP) can be deployed in standalone configuration, functioning as a single-server instance. The standard installation method allows you to manually specify the installation information, such as Hostname, IP address, and other system settings using installation wizard.

System Requirements for Installation

VMware vSphere Virtual Machine Requirements for CCCSP

CCCSP software requires VMware ESXi host. After configuring the server hardware, install VMware vSphere ESXi.

Note Make sure that the ESXi version is VMware vSphere ESXi 7.0.x and above.

Table 1: Virtual Machine Requirements for VMware vSphere

CCCSP Options	vCPU	vRAM	vDisk	vNIC
Small - 50cps	1	6 GB	80 GB	Single
Medium – 100cps	2	6 GB	80 GB	Single
Large - 200cps	4	6 GB	80 GB	Single
X-large – 400cps	6	6 GB	80 GB	Single

Note CPU speed is greater than or equal to 2.99 GHz.

Nutanix AHV Virtual Machine Requirements for CCCSP

CCCSP software requires Nutanix Acropolis Hypervisor (AHV) host. After configuring the server hardware, install Nutanix AHV.

Note Make sure that the Nutanix AHV version is 10.0 or later.

Table 2: Virtual Machine Requirements for Nutanix

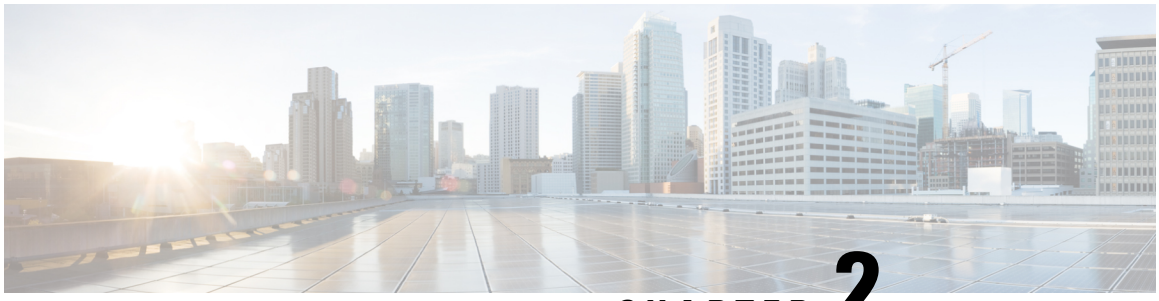
CCCSP Options	vCPU	vRAM	vDisk	vNIC
Small – 50cps	1	6 GB	80 GB	Single
Medium – 100cps	2	6 GB	80 GB	Single
Large – 200cps	4	6 GB	80 GB	Single

CCCSP Options	vCPU	vRAM	vDisk	vNIC
X-large – 400cps	6	6 GB	80 GB	Single

IP Address Requirements

Configure the CCCSP server to use either static IP address or assigned via DHCP server.

We recommend you to configure static IP address to avoid dynamic IP address changes to CCCSP server IP when DHCP is used.



CHAPTER 2

Pre-installation Tasks

- Create a Virtual Machine for VMware, on page 5
- Create a Virtual Machine for Nutanix, on page 5
- Change the Boot Order of the Virtual Machine, on page 6
- Gather Information for Installation, on page 6

Create a Virtual Machine for VMware

Before you begin

- Download the CCCSP OVA (virtual machine template), and the CCCSP ISO software from the Cisco site.

  Contact Center SIP Proxy - 15.0(1) Software Download

- If prompted, log in, using your Cisco.com user name and password.
- Select CCCSP software, and then select the appropriate release number, and download the ISO for the specific version.

Procedure

Step 1 To deploy the OVA template in a supported VMware client, choose **File** > **Deploy OVA Template**.

Step 2 Click to browse and select the OVA template or drag and drop the file saved for the deployment.

Step 3 Follow the on-screen instructions to create the virtual machine.

Create a Virtual Machine for Nutanix

Before you begin

- Download the CCCSP OVA (virtual machine template), and the CCCSP ISO software from the Cisco site.

Contact Center SIP Proxy - 15.0(1) SU2 Software Download

- If prompted, log in, using your Cisco.com user name and password.
- Select CCCSP software, and then select the appropriate release number, and download the ISO for the specific version.

Procedure

Step 1 To deploy the OVA template in a supported Nutanix AHV client, choose **Compute** > **OVAs** > **File** > **Upload OVA**.

Step 2 Click to browse and select the OVA template or drag and drop the file saved for the deployment.

Step 3 Upload CCCSP ISO, **Compute** > **Images** > **File** > **Add Image**.

Step 4 Follow the on-screen instructions to create the virtual machine.

Change the Boot Order of the Virtual Machine

The virtual machine boot into the BIOS menu.

Procedure

Step 1 In VMware client, power off the virtual machine that has the deployed OVA template.

Step 2 In the left pane of VMware client, right-click the name of the virtual machine, and select **Edit Settings**.

Step 3 In the Virtual Machine Properties dialog box, select the **Options** tab.

Step 4 In the Settings column, from the **Advanced** menu, select **Boot Options**.

Step 5 In the Force BIOS Setup, check the **The next time the virtual machine boots, force entry into the BIOS setup** screen check box.

Step 6 Select **OK** to close the **Virtual Machine Properties** dialog box.

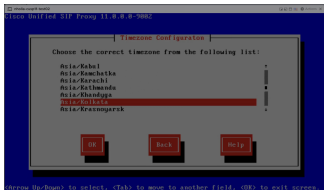
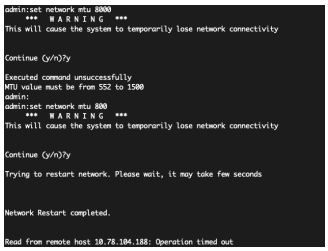
Step 7 Power on the virtual machine.

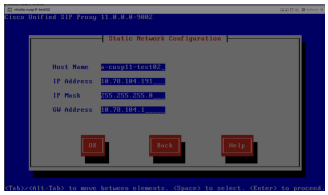
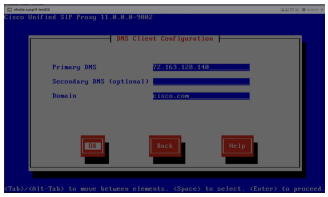
Step 8 Navigate to the Boot menu and change the boot device order so the CD-ROM device is listed first and the Hard Drive device is listed second.

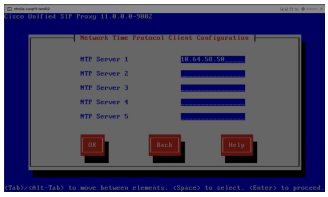
Step 9 **Save** the change and exit BIOS setup.

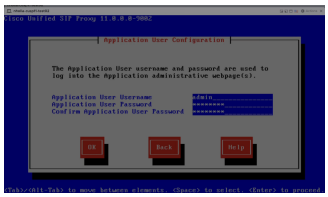
Gather Information for Installation

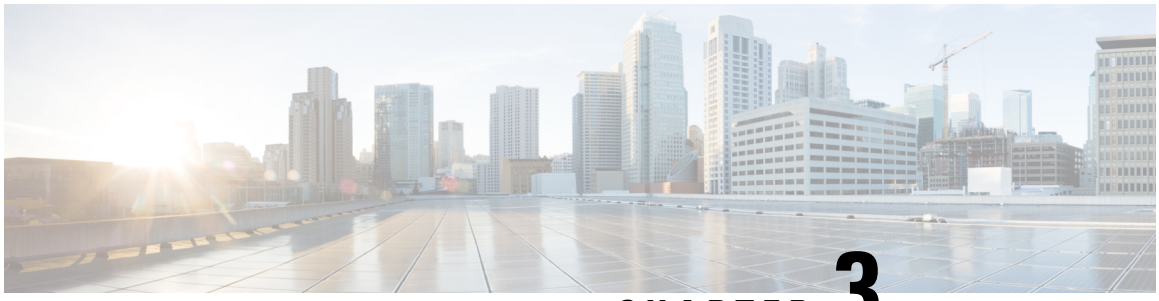
Use the table to record the information about your CCCSP server. The following information are required while configuring the VM after a fresh installation.

Configuration Setting	Description	Can Setting Be Changed After Installation?
Time Zone: 	Sets the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your server.	Yes, using the CLI command CLI > **set timezone**
MTU Size: 	Sets the largest packet, in bytes, that is transmitted by this host on the network. By default, MTU is set to the size defined in the operating system. Selecting a different packet size would be more prevalent where a VPN or IPsec tunnel is used with a custom packet size. Web access over VPN can cause web pages not to load because of an improper MTU configuration. The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network.	Yes, using the CLI command CLI > **set network mtu**

Configuration Setting	Description	Can Setting Be Changed After Installation?
Hostname and IP addresses: DHCP (Yes/No): If DHCP is **No**: Hostname: IP Address: IP Mask: Gateway (GW) Address: 	Sets whether to use DHCP to automatically configure the network settings on your server. If you select **No**, you must enter a hostname, IP address, IP address mask, and the gateway IP address. The hostname can contain up to 50 alphanumeric characters, hyphens, underscores, and period. The first character cannot be a hyphen. We recommend you use static Dynamic Host Control Protocol (DHCP) host configuration to ensure the DHCP server always provides the same IP address settings to the server. **Note** If you do not have a gateway, you must still set this field to 255.255.255.255. Not specifying a gateway may limit you to only being able to communicate with devices on your subnet.	Yes, using the CLI command CLI > **set network dhcp** CLI >**set network gateway** CLI >**set network ip eth0**
Domain Name Server: DNS: (Yes/No): If DNS is **Yes**: Domain: DNS Primary: DNS Secondary: 	Sets whether a DNS server resolves a hostname and IP address **Note** CCCSP enables the use of a domain name server to locate other servers and devices in the network. We recommend you to configure a secondary DNS server to avoid any loss of connectivity or service.	Yes, using the CLI commands CLI > **set network dns** CLI > **set network domain**

Configuration Setting	Description	Can Setting Be Changed After Installation?
Platform Administrator Account Credentials: Login: Password: 	Sets the administrator credentials for secure shell access to the CLI and for logging into CCCSP Operating System. The administrator account should be shared only with installers and engineers who have a thorough understanding and are responsible for the platform administration and upgrades, and backup and restore operations. **Note** If you are restoring from CUSP 10.2 backup, enter the platform administrator username that is different from the CUSP 10.2 version application username. **Note** Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Log in: No. Password: yes, using the CLI command CLI > **set password user admin** **Note** You can create additional administrator accounts after installation.
NTP Servers: NTP Server 1: NTP Server 2: NTP Server 3: NTP Server 4: NTP Server 5: 	Sets the hostname or IP address of one or more network time protocol (NTP) servers that synchronize with your CCCSP server. The NTP service ensures that the time synchronized is accurate for date/timestamps of messages, reports, and various tools, such as logs and traces. All CCCSP servers require an external NTP source that are accessible during installation. The source can be a corporate headend router synchronized with a public NTP time server or it can be the public NTP time server itself. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers should be NTP v4 (version 4).	Yes, using Cisco Unified Operating System Administration: **Settings** > **NTP Servers** Using the CLI command CLI > using the CLI command

Configuration Setting	Description	Can Setting Be Changed After Installation?
Application Account Credentials: Login: Password: 	Sets the CCCSP Administrator credentials. **Note** This administrator account is different from the Platform Administrator account created above. If you try configuring the same administrator id, then the installation will fail.	Yes, using CCCSP Administration and the CLI command: CLI > **user USERNAME password newpassword**



CHAPTER 3

Install Cisco Contact Center SIP Proxy (CCCSP)

- Navigation within Installation Wizard, on page 11
- Install and Configure CCCSP on the Virtual Machine, on page 11

Navigation within Installation Wizard

For instructions on how to navigate within the installation wizard, follow the table:

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Select an option	Space bar or **Enter**
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or **Enter** to select **Back** (when available)
Get help information on a window	Space bar or **Enter** to select **Help** (when available)

Install and Configure CCCSP on the Virtual Machine

Before you begin

While installing CCCSP, you are prompted to enter different configuration information. Refer the table mentioned in the *Gathering Information for Installation* section wherever applicable.

Procedure

Step 1 From the **vCenter** window, open the console of your newly installed virtual machine.

Step 2 Prepare the virtual machine to install CCCSP:

a) You can power off the Virtual Machine (VM) if it is already not powered off.

b) Select **Edit** virtual machine settings to select the ISO image from CD/DVD drive using client device or from data store.
c) Save the VM settings and Power On the VM.
d) Navigate to the **Console** tab. A screen prompting you to check the integrity of the DVD appears.
e) Select **Skip** to skip media test and move to the next step.
f) If the media test was performed, after performing the hardware check, you get a prompt to restart the system. You need to select **Yes** to continue installation. After the system restarts, the Product Deployment Selection window displays.

Step 3 In the **Product Deployment Selection** window, confirm the product name **Cisco Contact Center SIP Proxy** is displayed. Click **OK** to proceed.

Step 4 In the **Proceed with the install** window, verify the version and click **Yes** to proceed.

Note
If you select **Yes** on the **Proceed with Install** window, all existing data on your hard drive gets overwritten and destroyed.

Step 5 In the **Platform Installation Wizard**, click **Proceed** to continue with the install configuration.
a) In the **Apply Patch** wizard, select **No** for the patch upgrade.
b) Click **Continue** to continue with the basic installation.

Step 6 In the **Basic Install** window, select **Continue** to install the software version or configure the pre-installed software.

Step 7 In the **Timezone Configuration** window, select your time zone and click **OK**.

Step 8 In the **Auto Negotiation Configuration** window, select **Continue**.

Step 9 In the **MTU Configuration** window, select the applicable option:
a) Select **No** to accept the default value (1500 bytes).
b) Select **Yes** to change the MTU size, enter the new MTU size, and select **OK**.

Caution
If you configure the MTU size incorrectly, your network performance can be affected.

Step 10 In the **DHCP Configuration** window, select the applicable option:
a) Select **Yes** to use DHCP server that is configured in your network. The network restarts and the Administrator Login Configuration window appears.
b) Select **No** to configure a static IP address for the server and continue with this procedure. The Static Network Configuration window appears.

Step 11 In the **Static Network Configuration** window, enter the following static network configuration values and click **OK**.

- Host Name
- Static IP Address
- Netmask
- Gateway IP address

Step 12 In the **DNS Client Configuration** window, select **Yes** and enable DNS configuration. Configure the following:

- Primary DNS Server IP address
- (Optional) Secondary DNS Server IP address
- Domain Name

The network restarts using the new configuration information, and the **Administrator Login Configuration** screen appears.

Step 13 Enter the **Platform Administrator ID** (OS admin) and set the **Password**. Click **OK** to continue.

Note
If you are restoring from CUSP 10.2 backup, enter the platform administrator username that is different from the CUSP 10.2 version application username.

Step 14 In the **Network Time Protocol Client Configuration** window, enter hostname or IP address of the NTP server(s). Click **OK** to configure the NTP.

Note
Cisco recommends that you use an external NTP server to ensure accurate system time. However, you can configure multiple NTP servers based on your requirements.

Step 15 In the **Application User Configuration** window, create **Application Admin User**:

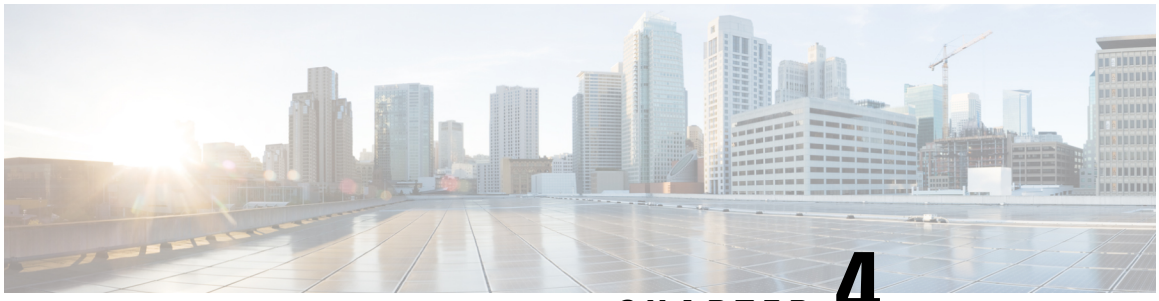
Note
This **Admin user ID** is used for Administrator activities related to CCCSP application configuration and monitoring. This is different from the **Platform Administrator ID** created in *Step 13*.

a) Make sure that the Admin user is different from the platform admin (OS admin), else the installation will fail.
b) Enter a username (for example, admin) and set a password.
c) Click **OK** and continue.

Step 16 In the **Platform Configuration Confirmation** window, verify all configurations and confirm. The system installs and configures the software.
The system will install OS-specific and application-specific RPMs.

Step 17 (Optional) During installation, you may encounter a network connectivity error:
Unable to resolve eth0 IP address into a host name (Reverse DNS lookup failed) - error message. If the hostname is not available in the DNS server, select **Ignore** and proceed.

The installation takes a few minutes to complete. Once complete, the system will display the login screen. Login using the Administrator account and password.



CHAPTER 4

Post Installation Tasks

- Verification of the Installation, on page 15

Verification of the Installation

Procedure

Step 1 Use an external SSH client to log in with the **CCCSP admin user ID** (Application administrator ID).

Enter **SSH** *username@ip-address*. Specify the username and IP address of the CCCSP.

Step 2 Verify that the application is running and the system is online.

After login, if the command prompt is displayed then it indicates that the system is online. You are in system EXEC (#) mode.

Step 3 Verify the deployed software version.

Use the **show software version** command in system EXEC (#) mode to check the software version.

Step 4 Enter the CCCSP management mode.

Use the **cusp** in system EXEC mode and enter in to CCCSP management mode.

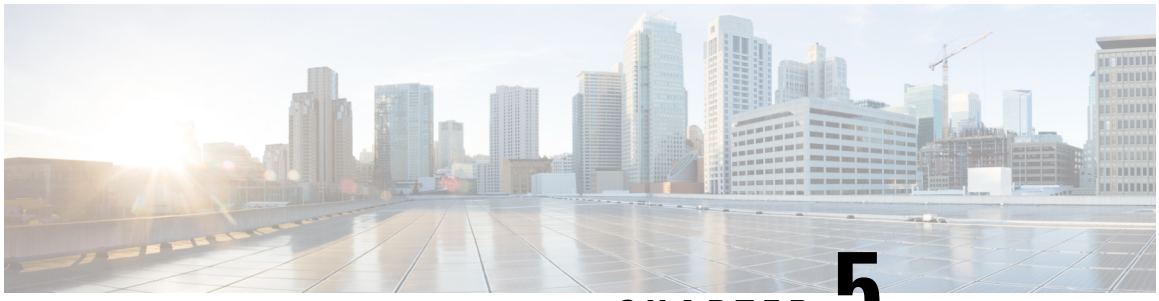
Step 5 Run the show configuration command to check the system configuration.

Use the **show configuration active** command and verify the system configuration.

Step 6 Start configuring specific features of the application.

What to do next

Post CCCSP installation follow the steps mentioned in the *Initial Configuration Task* section in *CLI Configuration Guide for CCCSP*.



CHAPTER 5

Migrate from CUSP Release 10.2(3) to CCCSP Release 15.0(1)

You can migrate your system from CUSP Release 10.2(3) and later versions to CCCSP Release 15.0(1).

CCCSP Release 15.0(1) is deployed as a new VM and backup configuration from CUSP 10.2(3) and later versions is restored on the new VM deployed. Use the information in this section along with the other configuration sections in this guide.

Migration from CUSP Release 10.2(3) and later versions to CCCSP Release 15.0(1) includes the following steps:

- Perform Backup Steps on CUSP 10.2(3) and later versions, on page 17
- Deploy CCCSP Release 15.0(1) on VM, on page 18
- Perform Restore Steps on CCCSP-15.0(1), on page 19

Perform Backup Steps on CUSP 10.2(3) and later versions

SUMMARY STEPS

1. **commit**
2. **write** [**erase** | **memory** | **terminal**]
3. **offline**
4. **backup** { **revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*
5. **backup category** { **all** | **configuration** | **data** }
6. **continue**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**commit** **Example:**	Enables the CUSP committable configuration changes to take effect.

	Command or Action	Purpose
	`Hostname(cusp-config)# commit`	
Step 2	**write** [**erase** | **memory** | **terminal**] **Example:** `Hostname# write memory`	Writes the running configuration to the startup configuration.

Step 3	**offline**
	Example:
	`Hostname# offline`
	`!!!WARNING!!!: Putting the system offline will terminate all active calls.`
	`Do you wish to continue[n]? : y`
		Enters offline mode. All calls are terminated.
		Note
		CUSP still routes calls in offline mode

Step 4	**backup** { **revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password* **Example:** `Hostname(offline)# backup server url sftp://192.1.1.1/ username <sftp-username> password <sftp-password>`	Configures the backup server **Note** You can also backup server using CCCSP GUI options. See GUI Administration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 5	**backup category** { **all** | **configuration** | **data** } **Example:** `Hostname(offline)# backup category all`	Specifies the type of data to be backed up and stored.
Step 6	**continue** **Example:** `Hostname(offline)# continue`	Exits offline mode and returns the system to the previous online mode. The system begins processing new calls.

Deploy CCCSP Release 15.0(1) on VM

Deploy the CCCSP Release 15.0(1) ISO on a virtual machine (VM) and perform the mandatory configurations. Follow the *Initial Configuration Tasks* section in *CLI Configuration Guide for CCCSP* and perform initial CCCSP configurations.

Make sure that the IP address, hostname and the application administrator login credentials remain same as configured in CUSP 10.2(3) and later versions during VM install on CCCSP 15.0(1). Any discrepancies in the user credentials can cause issues when you login to CCCSP User Interface.

Note You need to power down the existing CUSP 10.2(3) and later versions prior to deploying CCCSP 15.0(1) for IP address and hostname to match. See *Install and Configure CCCSP on the Virtual Machine* installation section.

Perform Restore Steps on CCCSP-15.0(1)

Before you begin

Perform initial CCCSP configurations following the *Initial Configuration Tasks* section in CLI Configuration Guide for CCCSP.

Make sure that the SFTP server details are configured as discussed in *Set Backup Parameters* section of CLI Configuration Guide for CCCSP.

SUMMARY STEPS

1. **show backup server**
2. **offline**
3. **restore id** *backup_id* **category** { **all** | **configuration** | **data**}
4. **show restore history**
5. Configure Smart Licensing.
6. Configure certificates manually.
7. **reload**
8. Reset the password for all the restored users (administrators, pfs-privusers, and pfs-readonly)

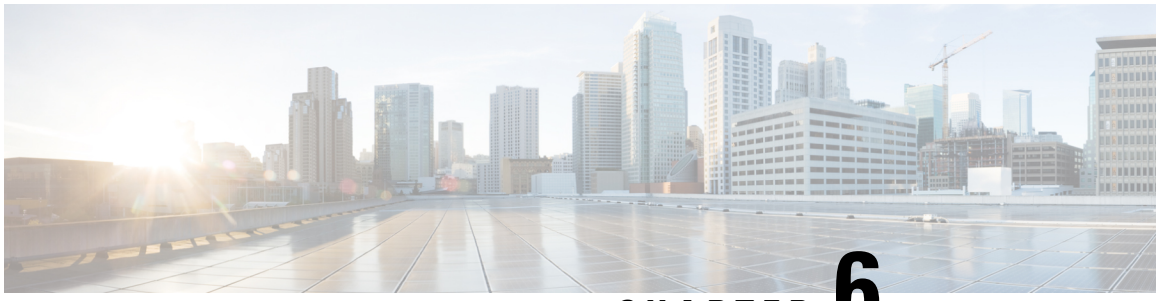
DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show backup server** **Example:** `Hostname# show backup server`	Lists the data and configuration backup files. Look in the backup ID field for the revision number of the file that you want to restore.

Step 2	**offline**
	Example:
	`Hostname# offline`
	`!!!WARNING!!!: Putting the system offline will terminate all active calls.`
	`Do you wish to continue[n]? : y`
		Enters offline mode. Restore is done in offline mode, which terminates all calls. You should therefore consider restoring files when call traffic is least impacted.
		Note
		CCCSP still routes calls in offline mode.

	Command or Action	Purpose
Step 3	**restore id** *backup_id* **category** { **all** | **configuration** | **data**} **Example:** `Hostname(offline)# restore id 22 category all`	Specifies the backup ID value and the file type to be restored. **Note** You can also restore using CCCSP GUI options. See GUI Administration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 4	**show restore history** **Example:** `Hostname# show restore history`	Prints information about previous backup restores.
Step 5	Configure Smart Licensing.	Configure Smart Software Licensing which is a standardized licensing platform that facilitates you to deploy and manage Cisco software licenses easily and quickly. For more information, refer to GUI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP) and CLI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP). **Note** CUSP Smart Licenses are not transferred to CCCSP. New CCCSP Smart Licenses are required.
Step 6	Configure certificates manually.	If TLS was enabled in the previous release (CUSP 10.2(3)) from which the restore is performed, certificates are not backed up or restored by default. Therefore, certificates must be manually configured to ensure TLS functions correctly. For detailed configuration steps, see CLI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 7	**reload** **Example:** `Hostname(offline)# reload`	Activates the uploaded file information and restarts the CCCSP system.
Step 8	Reset the password for all the restored users (administrators, pfs-privusers, and pfs-readonly)	Reset the password of the user after the restore. Follow the steps mentioned *Change your password* section in GUI Admin Guide for Cisco Contact Center SIP Proxy.



CHAPTER 6

Migrate from CUSP Release 10.2(3) to CCCSP Release 15.0(1) SU2

Following are the ways to migrate from CUSP Release 10.2(3) to CCCSP 15.0(1) SU2:

- Migrate from CUSP Release ESXi 10.2(3) to CCCSP ESXi 15.0(1) SU2
- Migrate from CUSP Release ESXi 10.2(3) to CCCSP Nutanix 15.0(1) SU2

Migrate from CUSP Release ESXi 10.2(3) to CCCSP ESXi 15.0(1) SU2

You can migrate your system from any CUSP Release ESXi 10.2(3) to CCCSP ESXi 15.0(1) SU2 using the Backup and Restore followed by Upgrade methods as outlined in the following table:

From deployment	To	Migration Method
CUSP ESXi 10.2(3)	CCCSP ESXi 15.0(1)	Backup and Restore
CCCSP ESXi 15.0(1)	CCCSP ESXi 15.0(1) SU2	Upgrade

Migrate from CUSP Release ESXi 10.2(3) to CCCSP Nutanix 15.0(1) SU2

You can also migrate your system from any ESXi release to CCCSP Nutanix using the backup and restore method. Following a fresh installation, upgrades on CCCSP Nutanix are supported starting from version 15.0(1) SU2.

Note M2 migration on Nutanix is not supported.

The table below outlines the available migration scenarios from ESXi to Nutanix:

From deployment	To	Migration Method
CUSP ESXi 10.2(3)	CCCSP Nutanix 15.0(1) SU2	Backup and Restore
CCCSP ESXi 15.0(1)	CCCSP Nutanix 15.0(1) SU2	Backup and Restore

From deployment	To	Migration Method
CCCSP Nutanix 15.0(1) SU2	Above versions	Backup and Restore Or Upgrade

Migration from CUSP Release 10.2(3) and later versions to CCCSP Nutanix Release 15.0(1) SU2 includes the following steps:

- Perform Backup Steps on CUSP 10.2(3) and later versions, on page 22
- Fresh Installation of CCCSP Release 15.0(1) SU2 VM on Nutanix Server, on page 23
- Perform Restore Steps on CCCSP 15.0(1) SU2 Nutanix, on page 23

Perform Backup Steps on CUSP 10.2(3) and later versions

SUMMARY STEPS

1. **commit**
2. **write** [**erase** | **memory** | **terminal**]
3. **offline**
4. **backup** { **revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*
5. **backup category** { **all** | **configuration** | **data** }
6. **continue**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**commit** **Example:** `Hostname(cusp-config)# commit`	Enables the CUSP committable configuration changes to take effect.
Step 2	**write** [**erase**	**memory**	**terminal**] **Example:** `Hostname# write memory`	Writes the running configuration to the startup configuration.

Step 3	**offline**
	Example:
	`Hostname# offline`
	`!!!WARNING!!!: Putting the system offline will terminate all active calls.`
		Enters offline mode. All calls are terminated.
		Note
		CUSP still routes calls in offline mode

	Command or Action	Purpose
	`Do you wish to continue[n]? : y`	
Step 4	**backup** { **revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password* **Example:** `Hostname(offline)# backup server url sftp://192.1.1.1/ username <sftp-username> password <sftp-password>`	Configures the backup server **Note** You can also backup server using CCCSP GUI options. See GUI Administration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 5	**backup category** { **all** | **configuration** | **data** } **Example:** `Hostname(offline)# backup category all`	Specifies the type of data to be backed up and stored.
Step 6	**continue** **Example:** `Hostname(offline)# continue`	Exits offline mode and returns the system to the previous online mode. The system begins processing new calls.

Fresh Installation of CCCSP Release 15.0(1) SU2 VM on Nutanix Server

Deploy the CCCSP Release 15.0(1) SU2 ISO virtual machine (VM) on Nutanix Server and perform the mandatory configurations. Follow the *Initial Configuration Tasks* section in CLI Configuration Guide for CCCSP and perform initial CCCSP configurations. Make sure that the IP address, hostname and the application administrator login credentials are entered correctly and are noted. Any discrepancies in the user credentials can cause issues when you login to CCCSP User Interface.

Perform Restore Steps on CCCSP 15.0(1) SU2 Nutanix

Before you begin

Perform initial CCCSP configurations following the *Initial Configuration Tasks* section in CLI Configuration Guide for CCCSP.

Make sure that the SFTP server details are configured as discussed in *Set Backup Parameters* section of CLI Configuration Guide for CCCSP.

SUMMARY STEPS

1. **show backup server**
2. **offline**
3. **restore id** *backup_id* **category** { **all | configuration | data**}

4. **show restore history**
5. Configure Smart Licensing.
6. Configure certificates manually.
7. **reload**
8. Reset the password for all the restored users (administrators, pfs-privusers, and pfs-readonly)

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show backup server** **Example:** `Hostname# show backup server`	Lists the data and configuration backup files. Look in the backup ID field for the revision number of the file that you want to restore.

Step 2	**offline**
	Example:
	`Hostname# offline`
	`!!!WARNING!!!: Putting the system offline will terminate all active calls.`
	`Do you wish to continue[n]? : y`
		Enters offline mode. Restore is done in offline mode, which terminates all calls. You should therefore consider restoring files when call traffic is least impacted.
		Note
		CCCSP still routes calls in offline mode.

Step 3	**restore id** *backup_id* **category** {**all** | **configuration** | **data**} **Example:** `Hostname(offline)# restore id 22 category all`	Specifies the backup ID value and the file type to be restored. **Note** You can also restore using CCCSP GUI options. See GUI Administration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 4	**show restore history** **Example:** `Hostname# show restore history`	Prints information about previous backup restores.
Step 5	Configure Smart Licensing.	Configure Smart Software Licensing which is a standardized licensing platform that facilitates you to deploy and manage Cisco software licenses easily and quickly. For more information, refer to GUI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP) and CLI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP). **Note** CUSP Smart Licenses are not transferred to CCCSP. New CCCSP Smart Licenses are required.

	Command or Action	Purpose
Step 6	Configure certificates manually.	If TLS was enabled in the previous release (CUSP 10.2(3)) from which the restore is performed, certificates are not backed up or restored by default. Therefore, certificates must be manually configured to ensure TLS functions correctly. For detailed configuration steps, see CLI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP).
Step 7	**reload** **Example:** `Hostname(offline)# reload`	Activates the uploaded file information and restarts the CCCSP system.
Step 8	Reset the password for all the restored users (administrators, pfs-privusers, and pfs-readonly)	Reset the password of the user after the restore. Follow the steps mentioned *Change your password* section in GUI Admin Guide for Cisco Contact Center SIP Proxy.