Installation Guide for Cisco Unified SIP Proxy Release 10.0

First Published: April 29, 2019

Last Modified: November 25, 2019

This document provides the technical information that you need to install Cisco Unified SIP Proxy Release 10.0 and contains the following topics:

Change History

This table lists all the changes made to this guide, the most recent changes appearing at the top.

Cisco Systems, Inc.
www.cisco.com

Change	See	Date
Published Installation Guide for Cisco Unified SIP Proxy Release 10.0.		April 29, 2019

Overview

Cisco Unified SIP Proxy Release 10.0 mainly addresses the open PSIRTs raised against the Operating System and the third-party components of the earlier versions of Virtual Cisco Unified SIP Proxy versions. Cisco Unified SIP Proxy Release 10.0 supports operating within a VMware ESXi virtualized environment. The software is packaged as an OVA for installation within the ESXi environment (5.1 and above). For more information about the ESXi environment, see:
http://www.vmware.com/products/vsphere/esxi-and-esx/overview.html

Except the High Availability (HA) feature using Hot Standby Router Protocol (HSRP), Cisco Unified SIP Proxy Virtual application supports all the other features that are supported by Cisco Unified SIP Proxy on a SRE Module.

Note For information on PSIRTs addressed in Cisco Unified SIP Proxy Release 10.0, see "Caveats" section in *Release Notes for Cisco Unified SIP Proxy 10.0*.

Server Requirements

Following is the approach to select a server for running Cisco Unified SIP Proxy Software within a VMware ESXi environment.

- Specifications-based Platforms

Specifications-based Platforms

This section provides information about specifications-based server platforms. See Table 1 for information about specifications-based server platforms.

Table 1   Specifications-based Server Platforms

For information on...	See...
Hardware requirements	UC Virtualization Supported Hardware https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-hardware.html
VMware installation and configuration	Implementing Virtualization Deployments https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html

Virtual Machine Requirements for Cisco Unified SIP Proxy

Cisco Unified SIP Proxy Software requires VMware ESXi 5.1 and above. After configuring the server hardware, install VMware vSphere ESXi.

Note Cisco Unified SIP Proxy deployment requires 6 GB RAM and 80 GB disk space.

Table 2 provides the hardware recommendations for the virtualized Cisco UCS platform.

Table 2   Virtual Machine Requirements for Cisco UCS Platform

CPS	60 CPS	100 CPS	200 CPS	300 CPS	400 CPS
vCPU	1	2	4	4	4
RAM	6 GB	6 GB	6 GB	6 GB	6 GB
Disk	80 GB	80 GB	80 GB	80 GB	80 GB

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

Table 3 provides the hardware recommendations for virtualized low speed Cisco UCS and Cisco UCS (E) platforms.

Table 3   Virtual Machine Requirements for Low Speed Cisco UCS and Cisco UCS (E) Platforms

CPS	40 CPS	100 CPS	200 CPS	300 CPS	400 CPS
vCPU	1	2	4	6	6
RAM	6 GB	6 GB	6 GB	6 GB	6 GB
Disk	80 GB	80 GB	80 GB	80 GB	80 GB

Note   CPU speed is less than 2.99 GHz.

Caution   Changing the default log file size impacts the performance of Cisco Unified SIP Proxy.

Caution   Over subscription of hardware by virtual machines running on hypervisor is not supported.

Downloading the Cisco Unified SIP Proxy OVA

To download the Cisco Unified SIP Proxy Server OVA template (virtual machine template), perform the following steps:

Step 1   Open the Cisco Unified SIP Proxy Server site:
http://www.cisco.com/c/en/us/support/unified-communications/unified-sip-proxy-software/tsd-products-support-series-home.html

Step 2   If prompted, log in, using your Cisco.com user name and password.

Step 3   Locate the OVA in "Download Software" section and download the file.

Deploying the Cisco Unified SIP Proxy OVA

After downloading the Cisco Unified SIP Proxy OVA, use the following procedure to deploy the virtual machine template.

Prerequisites

- Cisco Unified SIP Proxy OVA for installation
- Server with VMware ESXi environment installed
- VMware vCenter vSphere Client installed and operating

Procedure

Step 1   In the vCenter vSphere Client GUI, select **File > Deploy OVF Template…**

The **Deploy OVF Template** dialog box appears.

Step 2 Browse to the location where Cisco Unified SIP Proxy Server OVA file is downloaded. Click **Next**.

Step 3 Review and confirm the software image details. Click **Next**.

Step 4 Enter the name of the device in **Name** field. The name provided determines how the device appears in the left pane of the vCenter window.

Step 5 Click **Next**.

The **Deploy OVF Template** dialog box displays disk format options.

> ✎
>
> **Note** If there are multiple server hosts running ESXi, select the host on which you want Cisco Unified SIP Proxy Server to run. Click **Next**.

Step 6 Select any of the following **Thick provisioning format**.

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed

Step 7 Click **Next**.

The **Deploy OVF Template** dialog box displays the available networks.

Step 8 Select the network under **Destination Networks** column. The selected network is used to communicate with the remote sites.

Step 9 Click **Next**.

The **Deploy OVF Template** dialog box displays a summary of the options that you have configured.

Step 10 Click **Finish** to deploy Cisco Unified SIP Proxy Server.

A dialog box indicates when the deployment is complete.

Step 11 Select the VM instance, right click and choose **Edit Settings...**.

Virtual Machine Properties dialog box appears.

Step 12 Click the **Hardware** tab and set the values for memory and vCPU as provided in Table 2.

Step 13 Click the **Resources** Tab and select **CPU**. Adjust the Reservation and Shares to the value provided in Table 2.

> ✎
>
> **Note** Select the **Unlimited** option if the call flow details and the expected call capacity expected are not clear (this option takes care of cases where the call load is more than the planned load and needs additional CPU resources).

Step 14 Select **Memory** and change the reservation value as mentioned in the Table 2.

> ✎
>
> **Note** Select the **Unlimited** option if the call flows details and expected call capacity expected are not clear (this option handles the cases where call load is more than the planned load and needs additional RAM).

Step 15 Save the settings and restart the VM.

Step 16 Select **Resource Allocation** and confirm the resource reservations.

Configuring the CUSP Software

When you open the first session, the system launches the post installation configuration tool, and asks you if you want to start configuration immediately.

Enter the appropriate response, **y** or **n**. If you enter **n**, the system will halt. If you enter **y**, the system will ask you to confirm, then begin the interactive post installation configuration process.

The following is an example:

```
IMPORTANT::
IMPORTANT::    Welcome to Cisco Systems Service Engine
IMPORTANT::     post installation configuration tool.
IMPORTANT::
IMPORTANT:: This is a one time process which will guide
IMPORTANT:: you through initial setup of your Service Engine.
IMPORTANT:: Once run, this process will have configured
IMPORTANT:: the system for your location.
IMPORTANT::
IMPORTANT:: If you do not wish to continue, the system will be halted
IMPORTANT:: so it can be safely removed from the router.
IMPORTANT::

Do you wish to start configuration now (y,n)? y
Are you sure (y,n)? y

***********************************
* Service Engine IP configuration *
***********************************

Please enter the IP address of your Module: 192.0.2.1
Please enter the netmask of your Module: 255.255.0.0
Please enter the default gateway for your Module: 192.0.2.10

The following IP configuration is set:

IP     : 192.0.2.1
NETMASK:255.255.0.0
GATEWAY: 192.0.2.10

Do you wish to use this configuration (y, n) [n]: y

Enter Hostname
(my-hostname, or enter to use se-192-0-2-1): Enter
Using se--192-0-2-1 as default

Enter Domain Name
(mydomain.com, or enter to use local domain): Enter
Using localdoamin as default

IMPORTANT:: DNS Configuration:
IMPORTANT::
IMPORTANT:: This allows the entry of hostnames, for example foo.cisco.com, instead
IMPORTANT:: of IP addresses like 1.100.10.205 for application configuration.  In order
IMPORTANT:: to set up DNS you must know the IP address of at least one of your
IMPORTANT:: DNS Servers.

Would you like to use DNS (y,n)?y

Enter IP Address of the Primary DNS Server
  (IP address): 192.0.2.10
Found server 192.0.2.10
```

```
Enter IP Address of the Secondary DNS Server (other than Primary)
  (IP address, or enter to bypass): Enter

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Primary NTP server
  (FQDN or IP address, or enter for 192.0.2.10): cantor.cisco.com
Found server cantor.cisco.com

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Secondary NTP Server
  (FQDN or IP address, or enter to bypass): Enter

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 2
Please select a country.
 1) Anguilla                29) Honduras
 2) Antigua & Barbuda       30) Jamaica
 3) Argentina               31) Martinique
 4) Aruba                   32) Mexico
 5) Bahamas                 33) Montserrat
 6) Barbados                32) Netherlands Antilles
 7) Belize                  34) Nicaragua
 8) Bolivia                 35) Panama
 9) Brazil                  36) Paraguay
10) Canada                  37) Peru
11) Caribbean NL            38) Puerto Rico
12) Cayman Islands          39) St Barthelemy
13) Chile                   40) St Kitts & Nevis
14) Colombia                41) St Lucia
15) Costa Rica              42) St Maarten (Dutch)
16) Cuba                    43) St Martin (French)
17) Curacao                 44) St Pierre & Miquelon
18) Dominica                45) St Vincent
19) Dominican Republic      46) Suriname
20) Ecuador                 47) Trinidad & Tobago
21) El Salvador             48) Turks & Caicos Is
22) French Guiana           49) United States
23) Greenland               50) Uruguay
24) Grenada                 51) Venezuela
25) Guadeloupe              52) Virgin Islands (UK)
26) Guatemala               53) Virgin Islands (US)
27) Guyana
28) Haiti
#? 49
Please select one of the following time zone regions.
 1) Eastern (most areas)
 2) Eastern - MI (most areas)
 3) Eastern - KY (Louisville area)
 4) Eastern - KY (Wayne)
 5) Eastern - IN (most areas)
 6) Eastern - IN (Da, Du, K, Mn)
 7) Eastern - IN (Pulaski)
 8) Eastern - IN (Crawford)
 9) Eastern - IN (Pike)
10) Eastern - IN (Switzerland)
11) Central (most areas)
12) Central - IN (Perry)
13) Central - IN (Starke)
```

```
14) Central - MI (Wisconsin border)
15) Central - ND (Oliver)
16) Central - ND (Morton rural)
17) Mountain (most areas)
18) Mountain - ID (south); OR (east)
19) Mountain Time - Navajo
20) MMST - Arizona (except navajo)
21) Pacific
22) Alaska (most areas)
23) Alaska - Juneau area
24) Alaska - Sitka area
25) Alaska - Annette Island
26) Alaska - Yakutat
27) Alaska (west)
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now: Wed Nov 11 16:33:23 PDT 2018.
Universal Time is now: Wed Nov 11 20:33:23 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1

You can make this change permanent for yourself by appending the line
TZ='America/Los_Angeles'; export TZ
to the file '.profile' in your home directory; then log out and log in again.

Here is that TZ value again, this time on standard output so that you
can use the /bin/tzselect command in shell scripts:

Would you like to manually adjust the system time (y,n)? n
Removed symlink /etc/systemd/system/multi-user.target.wants/initial-setup.service.
Removed symlink /etc/systemd/system/graphical.target.wants/initial-setup.service.
Removed symlink /etc/systemd/system/multi-user.target.wants/initial-setup-text.service.
Removed symlink /etc/systemd/system/graphical.target.wants/initial-setup-text.service.

Waiting 49....

IMPORTANT::
IMPORTANT:: Administrator Account Creation
IMPORTANT::
IMPORTANT:: Create an administrator account.
IMPORTANT:: With this account, you can log in to the
IMPORTANT:: Cisco Unified SIP Proxy
IMPORTANT:: GUI and run the initialization wizard.
IMPORTANT::

Enter administrator user ID:
    (user ID): test
tesEnter password for test:
    (password):
Confirm password for test by reentering it:
    (password):


SYSTEM ONLINE
```

```
se-192.0.2.1# show software versions
Cisco Unified SIP Proxy version (10.0)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco
Systems, Inc.
```

Note During the configuration of Cisco Unified SIP Proxy software, the post installation configuration tool displays an IP address acquired through DHCP, and asks if you want to use this configuration. Enter the appropriate response, **y** or **n**. If you enter **n**, you can configure your module with the required IP address. If you enter **y**, the IP address acquired through DHCP is set as the IP address of your module. To reset the IP address the of your module, follow the steps mentioned in the section Configuring NTP Servers.

Configuring Cisco Unified SIP Proxy Application

Cisco Unified SIP Proxy can be configured in the following ways:

- Configuring Cisco Unified SIP Proxy using GUI, page 9
- Configuring Cisco Unified SIP Proxy using CLI, page 9
- Configuring Cisco Unified SIP Proxy using SSH, page 9

Configuring Cisco Unified SIP Proxy using GUI

Cisco Unified SIP Proxy can be configured using Graphical User Interface (GUI). The GUI can be accessed by using the IP address provided during installation.

For more information on configuring CUSP using GUI, refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.

Configuring Cisco Unified SIP Proxy using CLI

Cisco Unified SIP Proxy can be configured using Command Line Interface (CLI).

For more information on configuring CUSP using CLI, refer to *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.

Configuring Cisco Unified SIP Proxy using SSH

Cisco Unified SIP Proxy users with administrator group privileges can configure using SSH. The user credentials for SSH are the same as configured in Cisco Unified SIP Proxy.

Cisco Smart Software Licensing

Cisco Smart Software Licensing is a standardized licensing platform that facilitates you to deploy and manage Cisco software licenses easily and quickly. Cisco Smart Software Licensing establishes a pool of software licenses that can be used across your network in a flexible and automated manner. It also provides visibility to your purchased and deployed licenses in your network. Cisco Smart Software Licensing removes the need for Product Activation Keys (PAKs) and reduces your license activation and registration time.

You must have a valid account in Cisco Smart Manager to configure smart licensing for Cisco Unified SIP Proxy. By logging into your account in Cisco Smart Manager, you can generate token ID for Cisco Unified SIP Proxy. The generated token ID is unique to your account and it is mandatory to provide the generated token ID during license registration. The Cisco Unified SIP Proxy (Smart Agent) contacts the Cisco Smart Manager (Cisco Datacentre) using Call Home or HTTP protocol and configures the license. Smart licenses can be configured using either Graphical User Interface (GUI) or Command Line Interface (CLI).

Once the smart licensing is enabled and configured using GUI or CLI, the Cisco Unified SIP Proxy sends the entitlement tag, token ID and other required information to the Smart Agent and registers with the Smart Manager (cloud server). The registration is valid for a period of one year. If the registration fails, then Cisco Unified SIP Proxy moves to evaluation mode. In evaluation mode, all features are supported for 90 days. Cisco Unified SIP Proxy stops working after the evaluation period.

After successful registration, the license count and other necessary details are sent to the Smart Manager for authorization. If the authorization is successful, the Cisco Unified SIP Proxy is in authorized state. If the requested number of licenses is within the purchased license count, Licensing Agent state moves to InCompliance state. If the requested number of licenses is more than the purchased licenses, Licensing Agent state moves to OutofCompliance state.

The authorization is renewed automatically every 30 days without the intervention of the users. In case the authorization renewal fails for 90 days, Cisco Unified SIP Proxy moves to the authorization expiry state. In this state, Cisco Unified SIP Proxy continues to receive all the calls. But, at the same time, the Smart Agent retries to renew the authorization every four hours to establish a new registration period. Also, if you have a valid license, calls are not rejected when the calls-per-second exceeds the purchased license count. Since the Cisco Unified SIP Proxy is successfully authorized once, all calls are processed in the AuthorizedPeriodExpired or EvalExpired mode. In the event where the Smart Agent Client is disabled using GUI or CLI, none of the calls are processed. In this case, Cisco Unified SIP Proxy should have another successful authorization with Cisco Smart Manager to process calls in the AuthorizedPeriodExpired or EvalExpired mode.

For information on configuring smart licenses using GUI and CLI refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* and *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.

Cisco Smart Software Manager satellite

Cisco Smart Software Manager satellite is a component of Cisco Smart Licensing and works with Cisco Smart Software Manager (CSSM). It helps customers intelligently manage product licenses, providing near real-time visibility and reporting of the Cisco licenses they purchase and consume. From release 9.1.5 onwards, Cisco Unified SIP Proxy supports Cisco Smart Software Manager satellite version 3.0.0.

For security-sensitive customers who do not want to manage their installed Cisco Unified SIP Proxy using a direct Internet connection, the Smart Software Manager satellite is installed on the customer premises and provided a subset of CSSM functionality. The satellite needs to synchronize with CSSM

to reflect the latest license entitlements periodically. The satellite registration process is immediate. Cisco Unified SIP Proxy can register to the Smart Software Manager satellite directly as though it were a replicate of the Smart Software Manager in one of the following methods:

- Direct connection to CSSM

- Connection to local satellite using secure connection (https)

- Connection to local satellite using nonsecure connection (http)

Note Customers need to synchronize their local databases with the Cisco portal to make sure that the most recent purchases are reflected in their local copies.

For information on deploying, installing, and managing Smart Software Manager satellite, see Smart Software Manager satellite Installation Guide.

For support on installation of the satellite or other synchronization issues, contact the satellite team at: mailto:cs-cssm-satellite@cisco.com.

Registering Cisco Unified SIP Proxy Instances to satellite

Once the satellite is operational, smart-enabled Cisco Unified SIP Proxy instances can register to the satellite. The Cisco Unified SIP Proxy contacts the Cisco Smart Software Manager satellite using the HTTP or HTTPS protocol and configures the license.

For example,

- License Server URL for registering to direct CSSM: https://tools.cisco.com/its/service/oddce/services/DDCEService

- License Server URL for registering to satellite (10.65.125.254 is a local satellite with version 3.0): https://10.65.125.254:443/Transportgateway/services/DeviceRequestHandler

- License Server URL for registering to satellite in nonsecure mode (10.65.125.254 is a local satellite with version 3.0): http://10.65.125.254:80/Transportgateway/services/DeviceRequestHandler

Smart-enabled Cisco Unified SIP Proxy instances register to satellite via Graphical User Interface (GUI) or Command Line Interface (CLI). Once the smart licensing is enabled and configured using GUI or CLI, the Cisco Unified SIP Proxy sends the entitlement tag, token ID, and other required information to the satellite which in turn registers with the Cisco SSM. The registration is valid for one year. If the registration fails, then Cisco Unified SIP Proxy moves to evaluation mode. In evaluation mode, all features are supported for 90 days. Cisco Unified SIP Proxy stops working after the evaluation period.

After successful registration, the license count and other necessary details are sent to the Smart Manager for authorization. If the authorization is successful, the Cisco Unified SIP Proxy is in authorized state. If the requested number of licenses is within the purchased license count, Licensing Agent state moves to InCompliance state. If the requested number of licenses is more than the purchased licenses, Licensing Agent state moves to OutofCompliance state.

The authorization is renewed automatically every 30 days without the intervention of the users. In case the authorization renewal fails for 90 days, Cisco Unified SIP Proxy moves to the authorization expiry state. In this state, Cisco Unified SIP Proxy continues to receive all the calls. But, at the same time, the Smart Agent retries to renew the authorization every four hours to establish a new registration period. Also, if you have a valid license, calls are not rejected when the calls-per-second exceeds the purchased license count. Since the Cisco Unified SIP Proxy is successfully authorized once, all calls are processed in the AuthorizedPeriodExpired or EvalExpired mode. In the event where the Smart Agent Client is

disabled using GUI or CLI, none of the calls are processed. In this case, Cisco Unified SIP Proxy should have another successful authorization with Cisco Smart Manager to process calls in the AuthorizedPeriodExpired or EvalExpired mode.

For information on configuring smart licenses using GUI and CLI refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* and *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0.*

Migration from Cisco Unified SIP Proxy 8.x to Cisco Unified SIP Proxy 10.0

You can migrate from existing Cisco Unified SIP Proxy 8.x releases to Cisco Unified SIP Proxy Release 10.0. However, the following are the limitations during the migration:

- Cisco Unified SIP Proxy Release 10.0 cannot be installed on SRE Module. You require VMWare ESXi platform to install Cisco Unified SIP Proxy Release 10.0.

- Existing Cisco Unified SIP Proxy 8.x SWIFT licenses cannot be migrated to Cisco Unified SIP Proxy 10.0. Contact your Cisco partner or reseller to enquire about the purchase of current licensing.

- The backup configuration files from Cisco Unified SIP Proxy 8.x release do not have the network-related configuration as the Cisco SRE module gets the relevant information through RBCP protocol from the host router when it powers up. Cisco Unified SIP Proxy 10.0 does not support RBCP communication. So, if a backup configuration from Cisco Unified SIP Proxy 8.5.x release is restored in Cisco Unified SIP Proxy 10.0, you must manually enter and configure the IP address, subnet mask, and default gateway details during the reload as follows:

  a. Ensure that you have console access to the VM of virtual Cisco Unified SIP Proxy 10.0, while you are restoring the configuration of 8.X on 10.0.

  b. After the restore is completed, reload the module as per the instructions on the screen.

  c. Immediately after the reboot is completed, access the console with your username and password.

  d. Configure the IP address, subnet mask, and default gateway as follows:

```
cusp#configure terminal
Enter configuration command, one per line. End with CNTL/Z.
cusp(config)#interface FastEthernet 0
cusp(config-interface)#ip address 10.65.125.187 255.255.255.128
cusp(config-interface)#end interface
cusp(config)#ip default-gateway 10.65.125.129
SYSTEM ONLINE
cusp(config)#exit
cusp#wr mem
```

  e. After the Cisco Unified SIP Proxy is online, re-associate the users to groups with password reset and try to ssh.

```
cusp#configure terminal
cusp#username cisco group Administrators
cusp#username cisco password cisco
cusp#wr mem
```

- Cisco Unified SIP Proxy 8.x release configuration has multiple sub-interfaces. The sub-interface format in Cisco Unified SIP Proxy Release 10.0 is different from that in Cisco Unified SIP Proxy Release 8.x. You must configure these interfaces manually after the reload is complete.

- Listen points are not restored as it requires the IP address of the virtual Cisco Unified SIP Proxy. So, you must manually configure the listen points after restoring the back up from the Cisco Unified SIP Proxy 8.x release.

- SIP Ping configuration is not restored as it requires the IP address of the virtual Cisco Unified SIP Proxy. So, you must manually configure SIP Ping configuration on Cisco Unified SIP Proxy 10.0 release after restoring the backup from the Cisco Unified SIP Proxy 8.x release.

Following are the steps to migrate from any of the existing Cisco Unified SIP Proxy Releases to Cisco Unified SIP Proxy Release 10.0:

1. Take a backup of the existing Cisco Unified SIP Proxy 8.x configuration. For more information, see Cisco Unified SIP Proxy CLI Configuration Guide.

2. Deploy the Cisco Unified SIP Proxy Release 10.0 OVA on a virtual machine. For more information, see Cisco Unified SIP Proxy 10.0 Installation Guide.

3. Configure the Smart licenses. For more information, see GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0 and CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0.

4. Restore the configuration backup of Cisco Unified SIP Proxy 8.x in Cisco Unified SIP Proxy 10.0. For more information, see CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0.

Note Smart licensing details are reset if smart licensing is configured before restore of configuration. It is always recommended to restore the configuration before enabling smart licensing.

Note After configuration restore, you must manually create a user with administrator privileges for accessing SSH.

Note When you migrate from Cisco Unified SIP Proxy Release 8.x to Cisco Unified SIP Proxy Release 10.0, if there are no Sub-Interfaces or VLANs defined on the Virtual Machine, remove the VLAN 0 tag from packets at the ESXi switch side or network side. If not, packets with VLAN 0 tag are dropped.

Upgrading from Cisco Unified SIP Proxy Release 9.1.x to Release 10.0

You can upgrade your system from Cisco Unified SIP Proxy Release 9.1.x to Release 10.0.

A clean install wipes out all configuration and data; therefore, you must back up your configuration first. After you install the new system, you restore the configuration and data. Use the information in this section along with the other configuration sections in this guide.

Note For 10.x versions, the memory requirements have changed. Ensure to increase the RAM size to 6 GB. Refer to Deploying the Cisco Unified SIP Proxy OVA, page 4 for more information.

Note Although a best effort has been made to ensure backward compatibility, we recommend that you thoroughly inspect the backed up configuration to ensure that the data was not compromised.

Summary Steps

1. **commit**
2. **write [erase | memory | terminal]**
3. **offline**
4. **backup {revisions** *number* **| server url** *ftp-url* **username** *ftp-username* **password** *ftp-password***}**
5. **backup category {all | configuration | data}**
6. **continue**
7. Deploy the Cisco Unified SIP Proxy Release 10.0 OVA on a virtual machine and perform the mandatory configurations. For more information, see the "Initial Configuration Tasks" chapter in *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.
8. Configure Smart Licensing. Refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* and *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* for more information.
9. **restore id** *backup-id* **category {all | configuration | data}**
10. **reload**
11. Reset the password for all the restored users (administrators, pfs-privusers, and pfs-readonly). Follow the steps mentioned under the section "Changing your password" in the chapter "Configuring Users" in *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.
12. Re-associate the restored users to the corresponding groups. Follow the steps mentioned under the section "Displaying or Changing Group Subscriptions" in the chapter "Configuring Users" in *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.

Detailed Steps

	Command or Action	Purpose

Step 1	`commit`
	
	Example:
	`se-10-0-0-0(cusp-config)# commit`
		Enables the Cisco Unified SIP Proxy committable configuration changes to take effect.

Step 2	`write [erase	memory	terminal]`  **Example:** `se-10-0-0-0# write memory`	Writes the running configuration to the startup configuration.

Step 3	`offline`
	
	Example:
	`se-10-0-0-0# 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 Cisco Unified SIP Proxy still routes calls in offline mode.

■ **Installation Guide for Cisco Unified SIP Proxy Release 10.0**

14

	Command or Action	Purpose
Step 4	`backup {revisions number	server url ftp-url username ftp-username password ftp-password}`  **Example:** `se-10-0-0-0(offline)# backup server url ftp://192.1.1.1/ username <ftp-username> password <ftp-password>`	Configures the backup server.
Step 5	`backup category {all	configuration	data}`  **Example:** `se-10-0-0-0(offline)# backup category all`	Specifies the type of data to be backed up and stored.

Step 6	`continue`
	
	Example:
	`se-10-0-0-0(offline)# continue`
		Exits offline mode and returns the system to the previous online mode. The system begins processing new calls.

Step 7	Deploy the Cisco Unified SIP Proxy Release 10.0 OVA on a virtual machine and perform the mandatory configurations.	Installs the Cisco Unified SIP Proxy Release 10.0 image onto a system that has a Release 9.1.x image. For more information, see the "Initial Configuration Tasks" chapter in *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.
Step 8	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. Refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* and *CLI Configuration Guide for Cisco Unified SIP Proxy Release 10.0* for more information.
Step 9	`restore id backup-id category {all	configuration	data}`  **Example:** `se-10-0-0-0(offline)# restore id <backup-id> category all`	Specifies the backup ID value and the file type to be restored.

Step 10	`reload`
	
	Example:
	`se-10-0-0-0(offline)# reload`
		Activates the uploaded file information and restarts the Cisco Unified SIP Proxy system.

	Command or Action	Purpose
Step 11	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 under the section "Changing your password" in the chapter "Configuring Users" in *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.
Step 12	Re-associate the restored users to the corresponding groups.	Assign the user to the group after the restore. Follow the steps mentioned under the section "Displaying or Changing Group Subscriptions" in the chapter "Configuring Users" in *GUI Configuration Guide for Cisco Unified SIP Proxy Release 10.0*.