Initial Configuration Tasks

Last updated: October 10, 2019

Configuring SNMP MIB

About SNMP MIB Support

The Cisco Unified SIP Proxy (Unified SIP Proxy) includes SNMP integration for Release 9.1 with support for Cisco-USP-MIB. It is an enhancement from the SNMP MIB basic support introduced in Unified SIP Proxy Release 8.5. The Cisco Unified SIP Proxy Release 9.1 is SNMP version 2 (SNMPv2c) compliant.

Unified SIP Proxy integrates an SNMP agent and SNMP MIBs to monitor the health and to conduct performance monitoring and data collection for Unified SIP Proxy. Cisco-USP-MIB and Cisco-Process-MIB monitor the following data:

- Call Statistics
- Server Group Tables
- License State
- Memory and CPU Utilization
- System State

The SNMP integration sends notifications that helps to effectively monitor and manage performance and all the relevant system-specific data. Cisco-Process-MIB is supported in Cisco Unified SIP Proxy Release 9.1 for generating traps on configured CPU thresholds.

You can configure SNMP to send notifications to one or more monitoring systems. The maximum number of SNMP trap hosts that you can configure is limited to five.

Definitions

Table 1 Definition of SNMP MIB Related Terms

Term	Definition
Simple Network Management Protocol (SNMP)	It is a common network protocol that describes information passed between SNMP-enabled applications.
SNMP Agent	An SNMP Agent acts as a client to an SNMP management application by providing data values for registered OIDs.
Management Information Base (MIB)	MIBs are a defined hierarchy of data values managed by an SNMP Agent application.
SNMP Notification (Trap)/Informs	Information shared by a network entity with the management station to monitor a fault, exception, or an attribute value change. Traps do not need acknowledgment, but Informs request acknowledgment. From SNMPv2, traps are known as notifications.
Object Identifiers (OID)	It is a unique string of digits representing the value defined in an MIB.
SNMP GET	SNMP GET is an SNMP message used to fetch the value for a particular OID.
SNMP SET	SNMP SET is an SNMP request used to modify information on the target agent (controlling agent behavior or configuration of agent).

Prerequisites

CUSP MIB users must ensure that the following prerequisites are met:

- Configure Community Strings.
- Administrators of the Unified SIP Proxy must be familiar with the Cisco Command-line Interface (CLI) or the Graphical User Interface (GUI).
- Use a MIB browser or NMS to interact with the Cisco Unified SIP Proxy Release 9.1.
- Upload the CISCO-USP-MIB to the NMS.
- Ensure that MIB browser or NMS provides SNMP v2c compliance.

Restrictions

SNMP MIB support in Cisco Unity SIP Proxy Release 9.1 is known to have the following limitations or restrictions:

- No Support for SNMP Version 3 (SNMPv3)
- Certain MIB objects in the Cisco Unified SIP Proxy MIB tree are not supported. For a list of MIB objects that are not supported, see MIB Objects (Not Supported).
- If both read-only and read-write community strings are same for SNMP MIBs, then read-only takes preference and SET operations are not allowed.
- If the element table contains nested server group as an element, it does not display the partial state. The element state is shown as either up or down.

Structure

The SNMP MIB structure for Unified SIP Proxy has the following main considerations:

- The Unified SIP Proxy is uniquely identified within the Cisco management (9) group by the number –.1.3.6.1.4.1.9.9.827.
- Use either of the following methods to identify objects in the CISCO-USP-MIB:
  - The object identifier –.1.3.6.1.4.1.9.9.827.<Cisco-USP- MIB-variable>
  - The object name – iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).cisco(9).ciscoMgmt(9).CISCO-USP-MIB(827).<Cisco- USP-MIB-variable>
- Cisco Unified SIP Proxy Release 9.1 supports the following traps in Cisco-Process-MIB for CPU utilization monitoring:
  - cpmCPURisingThreshold (.1.3.6.1.4.1.9.9.109.2.0.1)
  - cpmCPUFallingThreshold (.1.3.6.1.4.1.9.9.109.2.0.2)

The Unified SIP Proxy MIB structure has the following groups and subgroups:

- MIBNotifs
- MIBObjects
  - cuspScalar
  - cuspTable
  - cuspNotifControlInfo
- MIBConform

Cisco Unified SIP Proxy SNMP MIBs

The Cisco Unified SIP Proxy captures the following in a management information base.

- MIB Objects
- MIB Notifications (Traps)

MIB Objects

The supported Cisco Unified SIP Proxy MIB Objects are:

- cuspScalar
  - cuspCallStats
  - cuspMessageStats
  - cuspThresholdValues
- cuspTable
- cuspNotifControlInfo

MIB Objects (Not Supported)

Cisco Unified SIP Proxy Release 9.1 does not support the following MIB objects:

- cuspMemoryThresholdAlert
- cuspDiskSpaceThresholdAlert
- cuspBackupProcessFailAlert
- cuspConnectionExceptionAlert
- cuspThresholdValues
- cuspDiskSpaceThresholdValue
- cuspMemoryThresholdValue
- cuspMessageStats
- cuspStrayMessageCount
- cuspNoOfMessagesRecieved
- cuspMemoryThresholdAlertEnable
- cuspExtensiveLoggingAlertEnable
- cuspDiskSpaceThresholdAlertEnable
- cuspBackupProcessFailAlertEnable
- cuspConnectionExceptionAlertEnable
- cuspDiskSpaceUsed

cuspScalar

This table contains a list of Unified SIP Proxy scalars. An entry in this table represents Unified SIP Proxy information relevant to licenses, system state, and memory.

Table 2 MIB Description for cuspScalar

MIB	OID	Description
cuspLastCounterResetTime	.1.3.6.1.4.1.9.9.827.1.1.1	Gives the timestamps in date and time when the call counter was last reset. All counters related to calls, Calls Per Second (CPS) and messages are reset when the counter is reset.
cuspSystemState	.1.3.6.1.4.1.9.9.827.1.1.2	Gives the Cisco Unified SIP Proxy system state as UP or DOWN.
cuspSystemUpTime	.1.3.6.1.4.1.9.9.827.1.1.3	Gives information on the active time of the Cisco Unified SIP Proxy system.
cuspLicenseLimit	.1.3.6.1.4.1.9.9.827.1.1.4	Gives the license limit information. Calls are rejected if the license limit is exceeded.
cuspLicenseState	.1.3.6.1.4.1.9.9.827.1.1.5	Gives the current license state of Cisco Unified SIP Proxy.
cuspSmartAgentState	.1.3.6.1.4.1.9.9.827.1.1.6	Gives the current license state of the SmartLicense Agent.
cuspConfiguredMemory	.1.3.6.1.4.1.9.9.827.1.1.7	Gives the total memory (RAM) configured on Cisco Unified SIP Proxy in Megabytes.
cuspMemoryUsed	.1.3.6.1.4.1.9.9.827.1.1.8	Gives the Cisco Unified SIP Proxy current memory (RAM) usage information in Megabytes.
cuspDiskSpaceUsed	.1.3.6.1.4.1.9.9.827.1.1.9	Gives the current disk utilization of CUSP in MB (Mega Byte).

cuspCallStats

This Unified SIP Proxy MIB defines data related to calls.

Table 3 MIB Description for cuspCallStats

MIB	OID	Description
cuspTotalCalls	.1.3.6.1.4.1.9.9.827.1.1.10.1	The total number of calls since the last counter reset.
cuspTotalFailedCalls	.1.3.6.1.4.1.9.9.827.1.1.10.2	The total number of failed calls since last counter reset.
cuspCPS	.1.3.6.1.4.1.9.9.827.1.1.10.3	The current running Calls Per Second (CPS) information.
cuspAvgCPSOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.4	The average CPS in the last one minute.
cuspMaxCPSOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.5	The Maximum value of CPS in the last one minute.

MIB	OID	Description
cuspDroppedCalls OneSec	.1.3.6.1.4.1.9.9.827.1.1.10.6	The count on number of calls dropped in the last one second.
cuspAvgDroppedC allsOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.7	The average of 'dropped calls per second' in the last one minute.
cuspMaxDropped CallsOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.8	The Maximum of 'dropped calls per second' in the last one minute.
cuspCallsRoutedO neSec	.1.3.6.1.4.1.9.9.827.1.1.10.9	The number of calls routed through CUSP in one second.
cuspAvgCallsRout edOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.10	The average of 'calls routed per second' in last one minute.
cuspMaxCallsRout edOneMin	.1.3.6.1.4.1.9.9.827.1.1.10.11	The maximum of 'calls routed per second' in the last one minute.
cuspCallsDropped ExceedingLicense	.1.3.6.1.4.1.9.9.827.1.1.10.12	The total calls dropped due to exceeding license limit.

Note There is no CLI and GUI equivalent for the data retrieved through MIB objects related to Calls Per Second (CPS) such as cuspCPS, cuspAvgCPSOneMin, cuspMaxCPSOneMin, cuspDroppedCallsOneSec, cuspAvgDroppedCPSOneMin, cuspMaxDroppedCPSOneMin, cuspCallsRoutedOneSec, cuspAvgCallsRoutedOneMin, and cuspMaxCallsRoutedOneMin. For example, GUI provides data for a five-minute average CPS while the MIB object cuspCPS retrieves CPS data only for the last second.

Note CUSP dropped call MIB objects are not updated if the license is in unidentified state.

Note If call rate limit is set to a value lesser than license limit, cuspCallsDroppedExceedingLicense MIB counts calls dropped due to call rate limit.

cuspThresholdValues

The Unified SIP proxy MIB object cuspThresholdValues (.1.3.6.1.4.1.9.9.827.1.1.12) provides threshold value information (as configured by user) on disk space and memory utilization.

Table 4 MIB Description for cuspThresholdValues

MIB	OID	Description
cuspDiskSpaceThr esholdValue	.1.3.6.1.4.1.9.9.827.1.1.12.1	The percentage threshold value configured by the user. If the percentage disk space utilization exceeds this limit, then cuspDiskSpaceThresholdAlert notification is sent.

MIB	OID	Description
cuspMemoryThresholdValue	.1.3.6.1.4.1.9.9.827.1.1.12.2	The percentage threshold value configured by the user. If the percentage memory utilization exceeds this limit, then cuspMemoryThresholdAlert notification is sent.

cuspTable

The Unified SIP proxy MIB object cuspTable (.1.3.6.1.4.1.9.9.827.1.2) consists of two main subgroups of objects:

- cuspServerGroupTable (OID:.1.3.6.1.4.1.9.9.827.1.2.1)
- cuspElementTable (OID:.1.3.6.1.4.1.9.9.827.1.2.2)

Note If data is retrieved from multiple network elements using cuspTable MIBs, the CPU utilization can spike beyond the optimum levels.

cuspServerGroupTable

The MIB cuspServerGroupTable represents a list of server groups that are part of active configuration. Server groups define the elements with which the Cisco Unified SIP Proxy system interacts for each network.

Table 5 MIB Description for cuspServerGroupTable

MIB	OID	Description
cuspServerGroupEntry	.1.3.6.1.4.1.9.9.827.1.2.1.1	An entry (conceptual row) in the ServerGroup Table.
cuspServerGroupIndex	.1.3.6.1.4.1.9.9.827.1.2.1.1.1	A unique value, greater than zero, for each server group.
cuspServerGroupName	.1.3.6.1.4.1.9.9.827.1.2.1.1.2	The name of the server group.
cuspServerGroupNetwork	.1.3.6.1.4.1.9.9.827.1.2.1.1.3	The network to which the server group belongs.
cuspServerGroupStatus	.1.3.6.1.4.1.9.9.827.1.2.1.1.4	The Server group status is given as up, partial down, and down.
cuspServerGroupPingStatus	.1.3.6.1.4.1.9.9.827.1.2.1.1.5	Server group ping status.
cuspServerGroupLBType	.1.3.6.1.4.1.9.9.827.1.2.1.1.6	The load balancing algorithm for the server group.

Note CuspservergroupPingStatus MIB object retrieves the information of a group irrespective of the global ping status.

cuspElementTable

The MIB cuspElementTable provides a list of elements in a server group table. Also, the table contains information on status (up or down) of the element, its Q-value, weight, and transport type.

Table 6 MIB Description for cuspElementTable

MIB	OID	Description
cuspElementEntry	.1.3.6.1.4.1.9.9.827.1.2.2.1	An entry (conceptual row) in the cuspElementTable.
cuspElementIndex	.1.3.6.1.4.1.9.9.827.1.2.2.1.1	A unique value, greater than zero, for each element.
cuspElementName	.1.3.6.1.4.1.9.9.827.1.2.2.1.2	The Server group element ID.
cuspElementStatus	.1.3.6.1.4.1.9.9.827.1.2.2.1.3	The server group element status as up or down.
cuspElementQValue	.1.3.6.1.4.1.9.9.827.1.2.2.1.4	The Q value of the server group element. Q value range is 0.0 to 1.0.
cuspElementWeight	.1.3.6.1.4.1.9.9.827.1.2.2.1.5	The weight of the server group element. Weight is used for load balancing between server group elements.
cuspElementPort	.1.3.6.1.4.1.9.9.827.1.2.2.1.6	Gives the port number of the server group element.
cuspElementTransport	.1.3.6.1.4.1.9.9.827.1.2.2.1.7	The transport type of the server group element. Transport type can be udp, tcp, or tls.
cuspElementTotalCalls	.1.3.6.1.4.1.9.9.827.1.2.2.1.8	The total routed calls to the server group element.
cuspElementFailedCalls	.1.3.6.1.4.1.9.9.827.1.2.2.1.9	The total failed calls on the server group element.

cuspNotifControlInfo

The MIB cuspNotifControlInfo (OID is.1.3.6.1.4.1.9.9.827.1.3) contains object that manages (enabling and disabling) the traps defined in CiscoUspMIBNotifs.

Table 7 MIB Description for cuspNotifControlInfo

MIB	OID	Description
cuspNotifSeverity	.1.3.6.1.4.1.9.9.827.1.3.1	The classification on the event severity.
cuspNotifDetail	.1.3.6.1.4.1.9.9.827.1.3.2	The detailed information on error encountered.
cuspSystemStateAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.3	Controls generation of cuspSystemStateAlert, cuspConnectionExceptionAlert.

MIB	OID	Description
cuspServerGroupAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.4	Controls the generation of cuspServerGroupElementAlert and cuspServerGroupAlert.
cuspServerGroupElementAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.5	Controls the generation of cuspServerGroupElementAlert.
cuspLicenseExceededAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.6	Controls the generation of cuspLicenseExceededAlert.
cuspLicenseStateAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.7	Controls the generation of cuspLicenseStateAlert.
cuspExtensiveLoggingAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.8	Controls the generation of cuspExtensiveLoggingAlert.
cuspDiskSpaceThresholdAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.9	Controls the generation of cuspDiskSpaceThresholdAlert.
cuspMemoryThresholdAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.10	Controls the generation of cuspMemoryThresholdAlert.
cuspBackupProcessFailAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.11	Controls the generation of cuspBackupProcessFailAlert notification.
cuspConnectionExceptionAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.12	Controls the generation of cuspConnectionExceptionAlert.
cuspSIPMessageQueueOverflowAlertEnable	.1.3.6.1.4.1.9.9.827.1.3.13	Controls the generation of cuspSIPMessageQueueOverflowAlert.

MIB Notifications (Traps)

Unified SIP Proxy generates trap notifications when the Network Management Station (NMS) or the administrator has to be informed about an event. The notification describes the operation state information of a service when a condition occurs. Traps provide information on issues that occur in the network element without polling for SNMP objects.

The administrator can control traps using the Command-line Interface (CLI), the Graphical User Interface (GUI), or through SNMP. By default, the traps are set to disabled state.

Unified SIP Proxy Release 9.1 supports a generic trap and raises SNMP traps on the following events:

- License Limit is exceeded
- System Failure
- Change in Server element state
- Change in Server group element state

Unified SIP Proxy Release 9.1 does not support SNMP traps on the following events:

- Backup Process Failure
- Memory threshold is exceeded
- Disk space threshold is exceeded
- Extensive Debug level logging

- Connection Exception

Table 8 MIB Description for MIB Traps

MIB	OID	Description
cuspSystemStateAlert	.1.3.6.1.4.1.9.9.827.0.1	Generated when the CUSP system goes up or down. This notification can be enabled or disabled by setting cuspSystemStateAlertEnable.
cuspServerGroupElementAlert	.1.3.6.1.4.1.9.9.827.0.2	Generated when the status of server group element changes. This notification can be enabled or disabled by setting cuspServerGroupAlertEnable.
cuspServerGroupAlert	.1.3.6.1.4.1.9.9.827.0.3	Generated when all the elements in the server group go down. Also, it is generated when any one element in the server group comes up after all the elements in the group were down. This notification is enabled or disabled by setting cuspServerGroupAlertEnable.
cuspMemoryThresholdAlert	.1.3.6.1.4.1.9.9.827.0.4	Generated when CUSP memory usage exceeds the cuspMemoryThresholdValue. This notification can be enabled or disabled by setting cuspThresholdAlertEnable.
cuspLicenseExceedAlert	.1.3.6.1.4.1.9.9.827.0.5	Generated when average CPS exceeds cuspLicenseLimit. This notification can be enabled or disabled by setting cuspLicenseExceededAlertEnable.
cuspLicenseStateAlert	.1.3.6.1.4.1.9.9.827.0.6	Generated when CUSP license state changes. This notification is enabled or disabled by setting cuspLicenseStateAlertEnable.
cuspExtensiveLoggingAlert	.1.3.6.1.4.1.9.9.827.0.7	Generated when extensive debug level logging is enabled in CUSP. Extensive logging has an impact on performance and system stability. This notification can be enabled or disabled by setting cuspExtensiveLoggingAlertEnable.

MIB	OID	Description
cuspDiskSpaceThresholdAlert	.1.3.6.1.4.1.9.9.827.0.8	Generated when the CUSP Disk usage exceeds the cuspDiskSpaceThresholdValue. This notification can be enabled or disabled by setting cuspThresholdAlertEnable.
cuspBackupProcessFailAlert	.1.3.6.1.4.1.9.9.827.0.9	Generated when backup process fails. This notification is enabled or disabled by setting cuspBackupProcessFailAlertEnabl.
cuspConnectionExceptionAlert	.1.3.6.1.4.1.9.9.827.0.10	Generated when a connection exception occurs. This notification can be enabled or disabled by setting cuspSystemStateAlertEnable.
cuspSIPMessageQueueOverflowAlert	.1.3.6.1.4.1.9.9.827.0.11	Generated when CUSP system queue is full. Queue full indicates either CUSP is overloaded or encountering network issues. The time interval between two successive notifications is 5 minutes. Notification is not sent within this time frame even if the queue is full. This back-off timer of 5 minutes prevents the CUSP overload. This notification can be enabled or disabled by setting cuspSIPMessageQueueOverflowAlertEnable.
cpmCPURisingThreshold	.1.3.6.1.4.1.9.9.109.2.0.1	Sent when configured rising CPU utilization threshold is reached and CPU utilization remains above the threshold for configured interval, and such a notification is requested.
cpmCPUFallingThreshold	.1.3.6.1.4.1.9.9.109.2.0.2	Sent when the configured falling threshold is reached and CPU utilization remains under threshold for configured interval, and such a notification is requested.

Note cuspLicenseExceededAlert is not generated if the license is in unidentified state.

Configuring Community String

Configure community string to poll data using MIB objects.

Summary Steps

1. **config** *terminal*
2. **snmp-server community** *community string {RO | RW}*
3. **end**
4. **write memory**

Detailed Steps

	Command or Action	Purpose

Step 1	`config`
	Example:
	`se-10-0-0-0# config terminal`
		Enables privileged EXEC mode.

Step 2	`snmp-server community community string {RO| RW}`
	Example:
	`se-10-0-0-0(config)# snmp-server community public RW`
		Configures the community string. The access could be read-only or read-write based on the selected configuration.

Step 3	`end`
	Example:
	`se-10-0-0-0(config)# end`
		Exits the privileged EXEC mode.

Step 4	`write memory`
	Example:
	`se-10-0-0-0# write memory`
		Stores the configuration in the startup configuration file.

Example

The following example configures Community Strings on the Cisco Unified SIP Proxy:

```
se-10-0-0-0# config terminal
se-10-0-0-0(config)# snmp-server community public RW
se-10-0-0-0(config)# end
se-10-0-0-0# write memory
```

Configuring SNMP Traps

Summary Steps

1. **config** *terminal*
2. **snmp-server host** *IP Address*
3. **snmp-server enable traps [All | System-State | Server-Group | SG-Element | CPU-Rising | CPU-Falling |License-Exceeded | Extensive-Logging | SIP-Message-Queue-Overflow]**
4. **snmp-server enable traps**

5. **end**
6. **write memory**

Detailed Steps

	Command or Action	Purpose

Step 1	`config`
	Example:
	`se-10-0-0-0# config terminal`
		Enables privileged EXEC mode.

Step 2	`snmp-server host IP Address community string`
	Example:
	`se-10-0-0-0(config)# snmp-server host 10.104.54.108 public`
		Specifies the host that receives SNMP notifications.

Step 3	`snmp-server enable traps [All | System-State | Server-Group | SG-Element | CPU-Rising | CPU-Falling | License-State | License-Exceeded | Extensive-Logging | SIP-Message-Queue-Overflow]`
	Example:
	`se-10-0-0-0(config)# snmp-server enable traps SG-Element`
		Activates the traps selected. The command **snmp-server enable traps all** activates all traps.
		To activate a specific trap, follow **snmp-server enable traps** with the subcommand specific to that trap.

Step 4	`snmp-server enable traps`
	Example:
	`se-10-0-0-0(config)# snmp-server enable traps`
		Enables trap generation from Cisco Unified SIP Proxy to the configured hosts.
		Traps are sent to the host only when this global command is enabled.

Step 5	`end`
	Example:
	`se-10-0-0-0(config)# end`
		Exits the privileged EXEC mode.

Step 6	`write memory`
	Example:
	`se-10-0-0-0# write memory`
		Stores the configuration in the startup configuration file.

Example

The following example configures SNMP Traps on the Cisco Unified SIP Proxy:

```
se-10-0-0-0# config terminal
se-10-0-0-0(config)# snmp-server host 10.104.54.108 public
se-10-0-0-0(config)# snmp-server enable traps SG-Element
se-10-0-0-0(config)# snmp-server enable traps
se-10-0-0-0(config)# end
se-10-0-0-0# write memory
```

Configuring CPU Threshold Values for Traps

To define rising and falling CPU threshold values for traps, perform these steps:

Summary Steps

1. **config** *terminal*
2. **process cpu threshold type total rising** *percentage* **interval** *seconds* **falling** percentage **interval** *seconds*

Detailed Steps

	Command or Action	Purpose

Step 1	`config`
	Example:
	`se-10-0-0-0# config terminal`
		Enables privileged EXEC mode.

Step 2	`process cpu threshold type {total} rising percentage interval seconds falling percentage interval seconds`
	Example:
	`se-10-0-0-0(config)# process cpu threshold type {total} rising 80 interval 300 falling 5 interval 300`
		Sets the CPU thresholding notifications types and values.
		• In this example, the CPU utilization threshold is set to 80 percent for a rising threshold notification and 5 percent for a falling threshold notification. The polling interval is set as 300 seconds.

Example

The following example configures CPU thresholding values for SNMP traps on the Cisco Unified SIP Proxy:

```
se-10-0-0-0# config terminal
se-10-0-0-0(config)# process cpu threshold type {total} rising 80 interval 300 falling 5
interval 300
```

Configuring Smart Licensing

About Smart 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.

Summary Steps

3. **enable**
4. **license smart destinationAddr** *url*
5. **license smart httpProxyAddr** *url*
6. **license smart activate cusp** *count*
7. **license smart register token_id** *token*

Detailed Steps

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`se-10-0-0-0# enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`license smart destinationAddr`** *`https://tools.cisco.com/its/service/oddce/services/DDCEService`*
	Example:
	`se-10-0-0-0# license smart destinationAddr` *`https://tools.cisco.com/its/service/oddce/services/DDCEService`*
		Connects to the central licensing server.

Step 3	**`license smart httpProxyAddr`** *`10.1.1.1`*
	Example:
	`se-10-0-0-0# license smart httpProxyAddr` *`10.1.1.1`*
		Sets the HTTP(S) proxy server address for smart licensing.

Step 4	**`license smart activate cusp`** *`count`*
	Example:
	`se-10-0-0-0# license smart activate cusp` *`100`*
		Activates the request number of licenses. The count must be multiple of 5.

Step 5	**`license smart register token_id`** *token* **Example:** `se-10-0-0-0# license smart register token_id` *`MjgxZjdkY2RtMWY5Ny00YTk4LOI2N2MtNjcxNmYaMTkzZGFhLHE0MjA3MjY0%0AMjI5N34Z8OVAOdmNzSjdIeG4MMHIzTmZubNFzMHhKOTYyeHlUZWQzQzVIM3Jk%0AHVk3MD0A3D%0N`*	Registers the device instance with the Cisco licensing cloud. This step is performed only once per device instance. The license agent registers the product with Cisco and receives back an identity certificate. This certificate is saved and automatically used for all future communications with Cisco. The license agent automatically renews the registration information with Cisco after one year.

Example

The following example configures Smart License on the Cisco Unified SIP Proxy:

```
se-10-0-0-0# enable
se-10-0-0-0# license smart destinationAddr
https://tools.cisco.com/its/service/oddce/services/DDCEService
se-10-0-0-0# license smart httpProxyAddr 10.1.1.1
se-10-0-0-0# license smart activate cusp 100
se-10-0-0-0# license smart register token_id
MjgxZjdkY2RtMWY5Ny00YTk4LOI2N2MtNjcxNmYaMTkzZGFhLHE0MjA3MjY0%0AMjI5NDZ8OVAOdmNzSjdIeG4MMHI
zTmZubNFzMHhKOTYyeHl67ZWQzQzVIM3Jk%0AHVk3MD0A3D%0N
```

Setting Backup Parameters

About Backup Parameters

Cisco Unified SIP Proxy backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from Cisco Unified SIP Proxy to the FTP server and the restore function copies the files from the FTP server to Cisco Unified SIP Proxy. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

All Cisco Unified SIP Proxy backup files are stored on the specified server. You can copy the backup files to other locations or servers, if necessary.

The backup parameters specify the FTP server to use for storing Cisco Unified SIP Proxy backup files and the number of backups that are stored before the system overwrites the oldest one.

Prerequisites

- Verify that an FTP administrator or other user who can log in to the FTP server has full permission on the FTP server, such as read, write, overwrite, create, and delete permissions for files and directories.
- Gather the FTP server URL and the username and password of the FTP server login.
- Determine the number of revisions to save before the oldest backup is overwritten.

Summary Steps

8. **configure terminal**
9. **backup server url** *backup-ftp-url* **username** *backup-ftp-usrname* **password** *backup-ftp-password*
10. **backup revisions number** *number*
11. **end**
12. **show backup**

Detailed Steps

	Command or Action	Purpose

Step 1	**`configure terminal`**
	`se-10-0-0-0#` **`config terminal`**
		Enters configuration mode.

Step 2	**`backup server url`** *`ftp-url`* **`username`** *`ftp-username`* **`password`** *`ftp-password`*}
	Example:
	`se-10-0-0-0(config)>` **`backup server url ftp://main/backups username “admin” password “wxyz”`**
	`se-10-0-0-0(config)>` **`backup server url ftp://192.0.2.15/backups username “admin” password “wxyz”`**
		Sets the backup parameters.
		Note You must configure the backup server before you can configure the backup revisions.
		• **server url**—The *ftp-url* value is the URL to the network FTP server where the backup files will be stored.
		• The *ftp-username* and *ftp-password* values are the username and password for the network FTP server.
		In the example, **main** is the hostname of the FTP server and **backups** is the directory where backup files are stored.

Step 3	**`backup revisions`** *`number`*
	Example:
	`se-10-0-0-0(config)>` **`backup revisions 5`**
		Sets the number of backup files that will be stored. When the system reaches this number of backups, it deletes the oldest stored file.

Step 4	**`end`**
	Example:
	`se-10-0-0-0(config)>` **`end`**
		Exits configuration mode.

Step 5	**`show backup`**
	Example:
	`se-10-0-0-0>` **`show backup`**
		Displays the backup server configuration information, including the FTP server URL and the maximum number of backup files available.

Example

The following example configures a backup server and displays the **show backup** output:

```
se-10-0-0-0> enable
se-10-0-0-0# configure terminal
se-10-0-0-0(config)> backup revisions 5
se-10-0-0-0(config)> backup server url ftp://10.12.0.1/ftp username “admin” password
“wxyz”
se-10-0-0-0(config)> end
se-10-0-0-0> show backup
Server URL:                         ftp://10.12.0.1/ftp
User Account on Server:
Number of Backups to Retain:        5
se-10-0-0-0>
```

Related Topics

- For information about the CLI commands, see the *CLI Command Reference for Cisco Unified SIP Proxy Release 9.1*.
- For information about backing up and restoring your configuration, see Backing Up and Restoring Data.

Configuring NTP Servers

When you install the Cisco Unified SIP Proxy software, the system gives you the option of adding up to two Network Time Protocol (NTP) servers. You can add additional NTP servers (the system supports up to three NTP servers), remove one or more NTP servers, or display NTP server information using the CLI.

- Adding NTP Servers, page 19
- Removing an NTP Server, page 21
- Displaying NTP Server Information, page 22

Adding NTP Servers

- About Adding NTP Servers, page 19
- Summary Steps, page 19
- Detailed Steps, page 20
- Examples of Adding NTP Servers, page 20

About Adding NTP Servers

You can specify an NTP server using its IP address or its hostname.

Cisco Unified SIP Proxy uses the DNS server to resolve the hostname to an IP address and stores the IP address as an NTP server. If DNS resolves the hostname to more than one IP address, Cisco Unified SIP Proxy randomly chooses one of the IP addresses that is not already designated as an NTP server. If you do not want to go with the random choice, set the **prefer** attribute for one server.

To configure an NTP server with multiple IP addresses for a hostname, repeat the configuration steps using the same hostname. Each iteration assigns the NTP server to its remaining IP addresses.

Summary Steps

1. **configure terminal**
2. **ntp server** {*hostname* | *ip-address*} [**prefer**]
3. **end**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

Detailed Steps

	Command or Action	Purpose

Step 1	`configure terminal`
	Example:
	`se-10-0-0-0# config terminal`
		Enters configuration mode.

Step 2	`ntp server {hostname | ip-address} [ prefer ]`
	Example:
	`se-10-0-0-0(config)> ntp server 192.0.2.14`
	`se-10-0-0-0(config)> ntp server 192.0.2.17 prefer`
		Specifies the hostname or IP address of the NTP server.
		If more than one server is configured, the server with the **prefer** attribute is used before the others.

Step 3	`end`
	Example:
	`se-10-0-0-0(config)> exit`
		Exits configuration mode.

Step 4	`show ntp status`
	Example:
	`se-10-0-0-0> show ntp status`
		Displays statistics about the NTP server.

Step 5	`show ntp configuration`
	Example:
	`se-10-0-0-0> show ntp configuration`
		Displays the configured NTP servers.

Step 6	`copy running-config startup-config`
	Example:
	`se-10-0-0-0> copy running-config startup-config`
		Copies the configuration changes to the startup configuration.

Examples of Adding NTP Servers

The following commands configure the NTP server:

```
se-10-0-0-0# configure terminal
se-10-0-0-0(config)> ntp server 192.0.2.14
se-10-0-0-0(config)> exit
se-10-0-0-0>
```

The output from the **show ntp status** command looks similar to the following:

```
se-10-0-0-0> show ntp status

NTP reference server 1:       192.0.2.14
Status:                       sys.peer
Time difference (secs):       3.268110099434328E8
Time jitter (secs):           0.1719226837158203
```

Removing an NTP Server

You can remove an NTP server using its IP address or hostname.

- Summary Steps, page 21
- Detailed Steps, page 21

Summary Steps

1. **configure terminal**
2. **no ntp server** {*hostname* | *ip-address*}
3. **exit**
4. **show ntp status**
5. **show ntp configuration**
6. **copy running-config startup-config**

Detailed Steps

	Command or Action	Purpose

Step 1	`configure terminal`
	Example:
	`se-10-0-0-0# configure terminal`
		Enters configuration mode.

Step 2	`no ntp server` {*hostname* | *ip-address*}
	Example:
	`se-10-0-0-0(config)> no ntp server 192.0.2.14`
	`se-10-0-0-0(config)> no ntp server myhost`
		Specifies the hostname or IP address of the NTP server to remove.

Step 3	`exit`
	Example:
	`se-10-0-0-0(config)> exit`
		Exits configuration mode.

Step 4	`show ntp status`
	Example:
	`se-10-0-0-0> show ntp status`
		Displays statistics about the NTP server.

Step 5	`show ntp configuration`
	Example:
	`se-10-0-0-0> show ntp status`
		Displays the configured NTP servers.

Step 6	`copy running-config startup-config`
	Example:
	`se-10-0-0-0> copy running-config startup-config`
		Copies the configuration changes to the startup configuration.

Displaying NTP Server Information

- Commands to Display NTP Server Information, page 22
- Examples of Showing NTP Server Information, page 22

Commands to Display NTP Server Information

The following commands are available to display NTP server configuration information and status:

- **show ntp associations**
- **show ntp servers**
- **show ntp source**
- **show ntp status**

Examples of Showing NTP Server Information

The following is sample output for the **show ntp associations** command:

```
se-10-0-0-0> show ntp associations

ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 61253  8000    yes   yes  none    reject
```

The following is sample output for the **show ntp servers** command:

```
se-10-0-0-0> show ntp servers

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 1.100.6.9       0.0.0.0         16 u    - 1024    0    0.000    0.000 4000.00
space reject,       x falsetick,       . excess,          - outlyer
+ candidate,        # selected,        * sys.peer,        o pps.peer
```

The following is sample output for the **show ntp source** command:

```
se-10-0-0-0> show ntp source

127.0.0.1: stratum 16, offset 0.000013, synch distance 8.67201
0.0.0.0:        *Not Synchronized*
```

The following is sample output for the **show ntp status** command:

```
se-10-0-0-0> show ntp status

NTP reference server :        10.100.6.9
Status:                       reject
Time difference (secs):       0.0
Time jitter (secs):           4.0
```

Related Topics

- For information about the CLI commands, see the *CLI Command Reference for Cisco Unified SIP Proxy Release 9.1*.
- For information about the initial installation of the Cisco Unified SIP Proxy system and the post installation configuration tool, see the *Installation Guide for Cisco Unified SIP Proxy Release 9.1*.
- For information about copying the configuration, see Copying Configurations, page 1.

Setting the Time Zone

When you install the Cisco Unified SIP Proxy software, the system prompts you to set the time zone. If you need to change it, use the **clock timezone** command in Cisco Unified SIP Proxy configuration mode.

To display the time zone, use the **show clock detail** command in module EXEC mode.

Example of Setting the Time Zone

```
se-10-0-0-0# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
se-10-0-0-0(config)> clock timezone
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       10) Pacific Ocean
2) Americas         5) Asia             8) Europe
3) Antarctica       6) Atlantic Ocean   9) Indian Ocean
>? 2
Please select a country.
 1) Anguilla              18) Ecuador                35) Paraguay
 2) Antigua & Barbuda     19) El Salvador            36) Peru
 3) Argentina             20) French Guiana          37) Puerto Rico
 4) Aruba                 21) Greenland              38) St Kitts & Nevis
 5) Bahamas               22) Grenada                39) St Lucia
 6) Barbados              23) Guadeloupe             40) St Pierre & Miquelon
 7) Belize                24) Guatemala              41) St Vincent
 8) Bolivia               25) Guyana                 42) Suriname
 9) Brazil                26) Haiti                  43) Trinidad & Tobago
10) Canada                27) Honduras               44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica                45) United States
12) Chile                 29) Martinique             46) Uruguay
13) Colombia              30) Mexico                 47) Venezuela
14) Costa Rica            31) Montserrat             48) Virgin Islands (UK)
15) Cuba                  32) Netherlands Antilles   49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
>? 45
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Standard Time - Indiana - most locations
 6) Eastern Standard Time - Indiana - Crawford County
 7) Eastern Standard Time - Indiana - Starke County
 8) Eastern Standard Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
```

```
>? 16

The following information has been given:

        United States
        Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Aug 27 17:23:54 PDT 2007.
Universal Time is now:  Tue Aug 28 00:23:54 UTC 2007.
Is the above information OK?
1) Yes
2) No
>? 1

Save the change to startup configuration and reload the module for the new time zone to
take effect.
se-10-0-0-0(config)>
```

Configuring HTTPS for Administration Web Interface

You can configure the system to allow HTTPS access to Cisco Unified SIP Proxy GUI.

- Summary Steps, page 24
- Detailed Steps, page 25
- Example of Configuring HTTPS, page 25

Summary Steps

1. **configure**
2. **crypto key generate rsa label** *labelname* **modulus 1024**
3. **web session security keylabel** *labelname*
4. **end**

Detailed Steps

	Command or Action	Purpose

Step 1	**`configure`**
	Example:
	`se-10-0-0-0>` **`configure`**
		Enters Cisco Unified SIP Proxy configuration mode.

Step 2	**`crypto key generate rsa label`** *`labelname`* **`modulus 1024`**
	Example:
	`se-10-0-0-0(cusp-config)>` **`crypto key generate rsa label mykey modulus 1024`**
	`Key generation in progress. Please wait...`
	`The label name for key is mykey`
		Generates a self-signed certificate and an RSA private key.

Step 3	**`web session security keylabel`** *`labelname`*
	Example:
	`se-10-0-0-0(cusp-config)>` **`web session security keylabel mykey`**
		Associates a security key for HTTPS.

Step 4	**`end`**
	Example:
	`se-10-0-0-0(cusp-config)>` **`end`**
		Exits to privileged EXEC mode.

Example of Configuring HTTPS

```
se-10-0-0-0> configure
se-10-0-0-0(cusp)> crypto key generate rsa label mykey modulus 1024
se-10-0-0-0(cusp-config)> web session security keylabel mykey
se-10-0-0-0(cusp-config)> end
```