Release Notes for Cisco Unified SIP Proxy Release 9.1.x

First Published: September 21, 2015

Last Revised: December 14, 2020

This document describes the new features, system requirements, licensing information, and caveats for Cisco Unified SIP Proxy Release 9.1.x. Use this document in conjunction with the caveats listed in Caveats, page 6 for the respective releases.

Contents

Introduction

Cisco Unified SIP Proxy is a high-performance, highly available Session Initiation Protocol (SIP) server for centralized routing and SIP signaling normalization. By forwarding requests to call-control domains, Cisco Unified SIP Proxy provides the means for routing sessions within enterprise and service provider networks. Cisco Unified SIP Proxy provides multiple features, including SIP trunk aggregation, name resolution, routing, load balancing, scalability, and high availability.

Cisco Systems, Inc.
www.cisco.com

Cisco Unified SIP Proxy 9.1.x is delivered as an Open Virtual Appliance (OVA) and can be installed as a virtual machine on Cisco UCS platform. Cisco Unified SIP Proxy Release 9.1.x supports CISCO-USP-MIB through SNMP.

System Requirements

Determining the Software Version

To determine the software version and the license used, perform the following steps.

Step 1 Enter the following command to display the Cisco Unified SIP Proxy software version:

```
show software versions
```

Step 2 Enter the following command to display the Cisco Unified SIP Proxy software license:

```
show license smart summary
```

File Packages

Release 9.1.1

The following package is available for Cisco Unified SIP Proxy Release 9.1.1:

- cusp-k9.vmw.9.1.1.ova

The CISCO-USP-MIB and CISCO-PROCESS-MIB is available for download at the Cisco site:

- Cisco SNMP Object Navigator

Release 9.1.2

The following package is available for Cisco Unified SIP Proxy Release 9.1.2:

- cusp-k9.vmw.9.1.2.ova

Release 9.1.3

The following package is available for Cisco Unified SIP Proxy Release 9.1.3:

- cusp-k9.vmw.9.1.3.ova

Release 9.1.4

The following package is available for Cisco Unified SIP Proxy Release 9.1.4:

- cusp-k9.vmw.9.1.4.ova

Release 9.1.5

The following package is available for Cisco Unified SIP Proxy Release 9.1.5:

- cusp-k9.vmw.9.1.5.ova

Release 9.1.6

The following package is available for Cisco Unified SIP Proxy Release 9.1.6:

- cusp-k9.vmw.9.1.6.ova

Release 9.1.7

The following package is available for Cisco Unified SIP Proxy Release 9.1.7:

- cusp-k9.vmw.9.1.7.ova

Release 9.1.8

The following package is available for Cisco Unified SIP Proxy Release 9.1.8:

- cusp-k9.vmw.9.1.8.ova

Release 9.1.9

The following package is available for Cisco Unified SIP Proxy Release 9.1.9:

- cusp-k9.vmw.9.1.9.ova

New Features and Enhancements

Release 9.1.1

• Cisco Unified SIP Proxy Release 9.1 supports SNMP MIBs and traps for monitoring its status using the Cisco-USP-MIB and CISCO-PROCESS-MIB.

Release 9.1.2

• Added an inactivity timer configuration that provides a GUI option to configure activity timeout in the range of 10 minutes to 24 hours.

Release 9.1.3

• Introduced **fd count** command that provides an option to change the default file descriptor count value from 1024 to 2048.

Release 9.1.4

• The default value of the file descriptor count was enhanced from 1024 to 25000.

• Introduced **show fd statistics** command that provides information on the maximum file descriptor count and the current open file descriptor count. See show fd statistics.

• Added tcp and tls options to the **show sip** command that displays the active Transmission Control Protocol (TCP) and Transport Layer Security (TLS) connections at the Cisco Unified SIP Proxy application level. See show sip.

• Introduced **show tcp connections** command that displays the status of Transmission Control Protocol (TCP) connections at the operating system level. See show tcp connections.

✎

Note   *CLI Command Reference* for Cisco Unified SIP Proxy Release 9.1.x is not updated with the CLI updates for Cisco Unified SIP Proxy Release 9.1.4.

Release 9.1.5

• Introduced **server-group sip ping-503** command that checks whether the SIP application service in the remote server element is up or down by monitoring the response. Cisco Unified SIP Proxy GUI is also enhanced to include the "Ping 503" parameter in the Server Groups settings.

- Introduced **Packet Capture** check box in the Cisco Unified SIP Proxy GUI to capture the network traffic on Cisco Unified SIP Proxy interfaces. Each packet capture request is limited to 40 MB.
- Cisco Unified SIP Proxy Release 9.1.5 adds support for Cisco Smart Software Manager satellite version 3.0.0.
- In Smart Licensing, if the Smart Agent Client is disabled via GUI or CLI, none of the calls are processed. Cisco Unified SIP Proxy should have another successful authorization with Cisco Smart Manager to process calls in the AuthorizedPeriodExpired or EvalExpired mode.

Release 9.1.6

- Introduced **show license smart agent-version** command that displays the smart agent version.

Release 9.1.7

- Introduced additional traps in this release. Now vCUSP sends TRAP alert when SIP queue is full or when CPU intensive debug is enabled.

Release 9.1.9

- The Cisco Unified SIP Proxy Smart Licensing agent is enhanced to support TLS 1.2.

Limitations and Restrictions

Note Cisco Unified SIP Proxy Release 9.1.x does not support installation of VMware Tools or any third-party tools in a Linux environment.

In a rare scenario, the configuration file may become read only and prevent you from saving the configuration changes using Command Line Interface (CLI) and Graphical User Interface (GUI). The impact is momentary and the file system tries to recover itself in most of such cases. In more persistent scenarios, reload the Cisco Unified SIP Proxy to recover the configuration file, edit, and save the configuration.

Release 9.1.1

Cisco Unified SIP Proxy Release 9.1.1 has the following restrictions:

- No Support for SNMP Version 3 (SNMPv3).
- Certain MIB objects in the Cisco Unified SIP Proxy MIB tree are not supported. For list of MIB objects that are not supported, see CLI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.

Release 9.1.2

There are no limitations in Cisco Unified SIP Proxy Release 9.1.2.

Release 9.1.3

There are no limitations in Cisco Unified SIP Proxy Release 9.1.3.

Release 9.1.4

- The **show sip tcp connections detail** and **show sip tls connections detail** commands will not have the filter options available for the Cisco Unified SIP Proxy Release 9.1.4. For example, you cannot use "pipe - |" to filter the various connection details.

Release 9.1.5

There are no limitations in Cisco Unified SIP Proxy Release 9.1.5.

Release 9.1.6

There are no limitations in Cisco Unified SIP Proxy Release 9.1.6.

Release 9.1.7

There are no limitations in Cisco Unified SIP Proxy Release 9.1.7.

Release 9.1.8

There are no limitations in Cisco Unified SIP Proxy Release 9.1.8.

Release 9.1.9

There are no limitations in Cisco Unified SIP Proxy Release 9.1.9.

Caveats

Caveats describe unexpected behavior in Cisco Unified SIP Proxy Release 9.1.x. To see the caveats associated with Cisco Unified SIP Proxy Release 9.1.x, use the Bug Search Tool at: https://tools.cisco.com/bugsearch/search.

Caveats Resolved in Release 9.1.1

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.1.

Caveat	Description
CSCup46140	CUSP 9.0 SNMP feature request
CSCut49136	Warning message should be associated with CPU intensive debugs
CSCut91199	Thread dump generation support for Cisco Unified SIP Proxy

Caveats Resolved in Release 9.1.2

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.2.

Caveat	Description
CSCuu24490	CUSP routing trigger sequences lost after reload
CSCuv79485	3xx response support and correct response for 380
CSCuv79510	JVM caching issue for domain name lookup
CSCuv89105	False element down notifications and thread leak
CSCuq30071	Thread leak with proactive options ping for TCP and UDP elements
CSCuw28772	CUSP retransmissions for 15 times (10 min) on a dead socket to VXML Gateway
CSCut68569	Network create using GUI not loading defaults for TCP connection setup timeout
CSCup13062	sip-wire-log is not capturing SIP messages on using TCP
CSCup98118	Normalization of user portion using URI manipulation truncates SIP
CSCux93716	Route table missing after reload
CSCus91366	Web GUI - Inactivity timer configuration
CSCux88153	CUSP 9.1 device does not provide the sysObjectID on snmpwalk

Note Though JVM level caching is removed as part of the caveat CSCuv79510, a non-configurable DNS look up caching of approximately 15 minutes is maintained at the OS level. For DNS cache look up at OS level, you can clear the cache using the command **clear ip dns cache**.

Caveats Resolved in Release 9.1.3

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.3.

Caveat	Description
CSCux67777	CUSP does not retain Lite-Mode cps after reboot
CSCva29771	CUSP shows trace size CLI defect
CSCuz93331	Evaluation period to be cleared when using SMART license in vCUSP 9.1.0
CSCuy68926	New CLI introduced to change file descriptor count
CSCuz93300	vCUSP 9.1.0 drops into evaluation mode even if SMART licensing is registered

Caveats Resolved in Release 9.1.4

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.4.

Caveat	Description
CSCva90553	Serviceability changes for TCP/TLS connections
CSCva61035	CUSP is silently discarding SIP messages on established TCP connections
CSCvb23682	Preemption of CLI "show sip tcp connection detail"

Caveats Resolved in Release 9.1.5

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.5.

Caveat	Description
CSCus98962	Ping - 503 handling
CSCvc20099	Logging header
CSCvc88996	Add support for Smart Software Manager Satellite for Smart Licensing
CSCvc96658	Packet capture
CSCvd49788	Evaluation of unified-sip-proxy for struts2-jakarta rce vulnerability
CSCve01766	Remove hard enforcement
CSCve25038	Cisco Unified SIP Proxy Smart License override + CLI reboot
CSCve35371	Multiple SmartAgent instances

Caveats Resolved in Release 9.1.6

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.6.

Caveat	Description
CSCvf02276	Can't commit any time policy configuration
CSCve97684	Unable to add or modify the q-value of elements in server group / route group

Caveat	Description
CSCvc91646	Add show command to display the smart agent version
CSCvf14108	Show fd statistics shows active fd count always as zero

Caveats Resolved in Release 9.1.7

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.7.

Caveat	Description
CSCvj44664	CUSP CLI can become inaccessible under low memory conditions
CSCve84547	Disable public key exchange over SSHv1
CSCvg74537	CLI command "show processes memory" does not work on CUSP 9.1.5
CSCvh69987	Smart Lic Command Injection Evaluation for unified-sip-proxy
CSCvh55130	Evaluate [Smart Licensing] Java CVE-2014-0107 & CVE-2015-6420 to be rebuilt in this product
CSCvh92829	SNMP Alert when either trace is enabled or message queue overflow observed

Caveats Resolved in Release 9.1.8

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.8.

Caveat	Description
CSCvm13980	Evaluation of unified-sip-proxy for Struts remote code execution vulnerability August 2018

Caveats Resolved in Release 9.1.9

The following issues were resolved in Cisco Unified SIP Proxy Release 9.1.9.

Caveat	Description
CSCvw64794	Adding the TLS version that is supported by CSSM for registration in 9.x CUSP

Commands and Notes: Release 9.1.4

To see the new and modified commands associated with Cisco Unified SIP Proxy Release 9.1.4, see:

- show fd statistics
- show sip
- show tcp connections

show fd statistics

To display the maximum number of file descriptor counts and current open file descriptor counts, use the **show fd statistics** command in Cisco Unified SIP Proxy EXEC mode.

show fd statistics

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
9.1.4	This command was introduced.

Usage Guidelines Use the **show fd statistics** command to display the maximum number of file descriptor counts and open file descriptor counts.

Examples The following is sample output from the **show fd statistics** command:

```
se-10-0-0-0(cusp)# show fd statistics
MaxOpenFileDescriptorCount: 25000
OpenFileDescriptorCount: 35
se-10-0-0-0(cusp)#
```

show sip

To display SIP log files, use the **show sip** command in Cisco Unified SIP Proxy EXEC mode.

show sip {**message** | **peg-counting log** [**tail** | *options*] | **tcp** | **tls** [**connections** {**summary** | **detail** [**dumptofile**] }]}

Syntax Description

message	Displays the SIP message log.
peg-counting	Displays the SIP peg-counting log.

options	Options for displaying the log file:
	• Display a given number of lines from the end of the log.
	• Send the output to another command.
	• Display the most recent entries in the log and keep updating them.
tcp	Displays the SIP TCP connections at the application level.
tls	Displays the SIP TLS connections at the application level.
summary	Displays the SIP TCP or TLS connections summary at the application level.
detail	Displays the SIP TCP or TLS connections details at the application level.
	Note **Detail** option has impact on the CPU usage. Hence, it is recommended not to use this option during peak loads. **Dumptofile** is the recommended option.
dumptofile	Dumps all SIP TCP or TLS connection table logs to the **trace.log** file at *"pfs://cusp/log/trace/"* directory at the application level.

Command Modes   Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.
9.1.4	This command was modified to include keywords: **tls** and **tcp**.

Usage Guidelines   The SIP message log file rotates every 10 MB or every night and is located at pfs://cusp/log/sipmsg. The SIP peg-counting log file rotates every 10 MB or every night also and is located at pfs://cusp/log/pegcount.

You can use the **dumptofile** option to get details on the production systems. However, use the **summary** option to get the current information of the SIP TCP or TLS connections.

Note   The **show sip tcp connections detail** and **show sip tls connections detail** commands will not have the filter options available for the Cisco Unified SIP Proxy Release 9.1.4. For example, you cannot use "pipe - |" to filter the various connection details.

Examples   The following example shows sample output from the **show sip message log** command:

```
se-10.0.0.0(cusp)# show sip message log

Request received at Wed, 19 Nov 2008 21:01:25,081 GMT on 192.168.20.101 on port 6060 from
the Remote IP 192.168.20.25 on port 6080

INVITE sip:735551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
```

```
Max-Forwards: 70
To: sut <sip:735551212@192.1.1.75:6061>
From: sipp <sip:sipp@192.168.20.5:6080>;user=phone;vnd.pimg.port=1;tag=1
Contact: sip:sipp@192.168.20.5:6080
Call-ID:1-7675@192.168.20.5
CSeq: 1 INVITE
Content-Length:135
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp

v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000

MESSAGE COMPLETE
```

The following example shows sample output from the **show sip peg-counting log** command:

```
se-10.0.0.0(cusp)# show sip peg-counting log
```

Message	Delta In Initial	Delta Out Initial	Delta In Retrans	Delta Out Retrans	Total In Initial	Total Out Initial	Total In Retrans	Total Out Retrans
INVITE	0	0	0	0	0	0	0	0
ACK	0	0	0	0	0	0	0	0
CANCEL	0	0	0	0	0	0	0	0
BYE	0	0	0	0	0	0	0	0
OPTIONS	0	0	0	0	0	0	0	0
REGISTER	0	0	0	0	0	0	0	0
SUBSCRIBE	0	0	0	0	0	0	0	0
NOTIFY	0	0	0	0	0	0	0	0
PRACK	0	0	0	0	0	0	0	0
REFER	0	0	0	0	0	0	0	0
UPDATE	0	0	0	0	0	0	0	0
PUBLISH	0	0	0	0	0	0	0	0
INFO	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0
180	0	0	0	0	0	0	0	0
181	0	0	0	0	0	0	0	0
182	0	0	0	0	0	0	0	0
183	0	0	0	0	0	0	0	0
200	0	0	0	0	0	0	0	0
202	0	0	0	0	0	0	0	0
300	0	0	0	0	0	0	0	0
301	0	0	0	0	0	0	0	0
302	0	0	0	0	0	0	0	0
305	0	0	0	0	0	0	0	0
380	0	0	0	0	0	0	0	0
400	0	0	0	0	0	0	0	0
401	0	0	0	0	0	0	0	0
402	0	0	0	0	0	0	0	0
403	0	0	0	0	0	0	0	0
404	0	0	0	0	0	0	0	0
405	0	0	0	0	0	0	0	0
406	0	0	0	0	0	0	0	0
407	0	0	0	0	0	0	0	0

The following example shows sample output from the **show sip tcp connections detail** command:

```
se-10.0.0.0(cusp)# show sip tcp connections detail
No of connections:166
Fetching connection information will have performance impact, it is recommend to choose
the option of dumping the information to log file Do you want to continue? (yes/no) [no]:
yes
Local IP      Local Port Remote IP      Remote Port
10.64.86.198    6061     10.105.34.180  63549
10.64.86.198    6061     10.105.34.180  63570
10.64.86.198    6061     10.105.34.180  63609
10.64.86.198    6061     10.105.34.180  63658
10.64.86.198    6061     10.105.34.180  63619
10.64.86.198    6061     10.105.34.180  63598
10.64.86.198    6061     10.105.34.180  63555
10.64.86.198    6061     10.105.34.180  63718
10.64.86.198    6061     10.105.34.180  63717
10.64.86.198    6061     10.105.34.180  63566
10.64.86.198    6061     10.105.34.180  63755
10.64.86.198    6061     10.105.34.180  63723
10.64.86.198    6061     10.105.34.180  63750
10.64.86.198    6061     10.105.34.180  63707
10.64.86.198    6061     10.105.34.180  63652
10.64.86.198    6061     10.105.34.180  63674
10.64.86.198    6061     10.105.34.180  63608
10.64.86.198    6061     10.105.34.180  63663
10.64.86.198    6061     10.105.34.180  63728
10.64.86.198    6061     10.105.34.180  63706
10.64.86.198    6061     10.105.34.180  63696
10.64.86.198    6061     10.105.34.180  63614
10.64.86.198    6061     10.105.34.180  63722
10.64.86.198    6061     10.105.34.180  63691
10.64.86.198    6061     10.105.34.180  63560
10.64.86.198    6061     10.105.34.180  63615
10.64.86.198    6061     10.105.34.180  63582
10.64.86.198    6061     10.105.34.180  63729
10.64.86.198    6061     10.105.34.180  63565
10.64.86.198    6061     10.105.34.180  63680
10.64.86.198    6061     10.105.34.180  63734
10.64.86.198    6061     10.105.34.180  63712
10.64.86.198    6061     10.105.34.180  63592
10.64.86.198    6061     10.105.34.180  63587
10.64.86.198    6061     10.105.34.180  63679
10.64.86.198    6061     10.105.34.180  63593
10.64.86.198    6061     10.105.34.180  63733
10.64.86.198    6061     10.105.34.180  63620
10.64.86.198    6061     10.105.34.180  63685
10.64.86.198    6061     10.105.34.180  63653
10.64.86.198    6061     10.105.34.180  63576
10.64.86.198    6061     10.105.34.180  63669
10.64.86.198    6061     10.105.34.180  63603
10.64.86.198    6061     10.105.34.180  63604
10.64.86.198    6061     10.105.34.180  63581
10.64.86.198    6061     10.105.34.180  63745
10.64.86.198    6061     10.105.34.180  63690
10.64.86.198    6061     10.105.34.180  63571
10.64.86.198    6061     10.105.34.180  63701
10.64.86.198    6061     10.105.34.180  63554

<<Enter for MORE>> [confirm]
.....
```

The following example shows sample output from the **show sip tls connections detail** command:

```
se-10.0.0.0(cusp)# show sip tls connections detail
No of connections:412
```

```
Fetching connection information will have performance impact, it is recommended to choose
the option of dumping the information to log file Do you want to continue? (yes/no) [no]:
yes
Local IP       Local Port Remote IP       Remote Port
10.65.125.148  5061       10.105.34.180   48014
10.65.125.148  5061       10.105.34.180   48166
10.65.125.148  5061       10.106.3.105    15221
10.65.125.148  5061       10.105.34.180   48123
10.65.125.148  5061       10.106.3.105    15300
10.65.125.148  5061       10.64.86.70     43748
10.65.125.148  5061       10.105.34.180   48161
10.65.125.148  5061       10.106.3.105    15330
10.65.125.148  5061       10.64.86.70     43726
10.65.125.148  5061       10.106.3.105    15348
10.65.125.148  5061       10.106.3.105    15288
10.65.125.148  5061       10.105.34.180   48177
10.65.125.148  5061       10.105.34.180   48090
10.65.125.148  5061       10.64.86.70     43655
10.65.125.148  5061       10.64.86.70     43623
.....
.....
```

show tcp connections

To display the status of Transmission Control Protocol (TCP) connections, use the **show tcp connections** command in module EXEC mode.

show tcp connections [*summary*]

Syntax Description

summary	(Optional) Displays the summary statement for all the tcp connections for the Cisco Unified SIP Proxy module.

Command History

Cisco Unified SIP Proxy Version	Modification
9.1.4	This command was introduced.

Usage Guidelines

The **show tcp connections** command displays detailed connection information at the operating system level. To obtain information at the application level, use the **show sip tcp connections detail** command.

Examples

The following example shows the current active tcp connections available on the operating system:

```
se-10-64-86-198# show tcp connections

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address        Foreign Address       State      PID/Program name

tcp      0     0 127.0.0.1:389          0.0.0.0:*             LISTEN     1634/slapd

tcp      0     0 0.0.0.0:911            0.0.0.0:*             LISTEN     1106/tclsh

tcp      0     0 0.0.0.0:21             0.0.0.0:*             LISTEN     2637/vsftpd

tcp      0     0 0.0.0.0:22             0.0.0.0:*             LISTEN     1108/sshd
```

```
tcp      0     0 127.0.0.1:5432        0.0.0.0:*           LISTEN     1824/postmaster
tcp      0    96 10.64.86.198:22       10.196.106.64:62609   ESTABLISHED 2693/sshd:
cuspdt [
tcp      0     0 127.0.0.1:389         127.0.0.1:49865       ESTABLISHED 1634/slapd
tcp      0     0 127.0.0.1:58065       127.0.0.1:12345       ESTABLISHED 2751/cli_xconn
tcp      0     0 127.0.0.1:5432        127.0.0.1:45198       ESTABLISHED 2782/postgres: post
tcp      0     0 127.0.0.1:5432        127.0.0.1:56925       ESTABLISHED 2286/postgres: post
tcp      0     0 127.0.0.1:58064       127.0.0.1:12345       ESTABLISHED 2687/cli_xconn
tcp      0     0 10.64.86.198:22       10.196.106.64:62608   ESTABLISHED 2306/sshd:
cuspdt [
```

Commands and Notes: Release 9.1.5

To see the new and modified commands associated with Cisco Unified SIP Proxy Release 9.1.5, see:

- server-group sip ping-503

server-group sip ping-503

To enable the use of ping-503 option to check whether the SIP application service in the remote server element is running or not, use the **server-group sip ping-503** command in Cisco Unified SIP Proxy configuration mode. Cisco Unified SIP Proxy can identify the type of response from the remote server element and decrement the retry count if the response is 503. To restore the SIP ping 503 option to the default value, use the **no** form of this command.

> **server-group sip ping-503**
>
> **no server-group sip ping-503**

Syntax Description   This command has no arguments or keywords.

Defaults   Response 503 from any elements is treated as a successful response.

Command Modes   Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
9.1.5	This command was introduced.

Usage Guidelines   Use this command to identify whether the sip element is down or not. If the **server-group sip ping-503** command is not configured, the 503 response is treated as successful response. If this command is configured, Cisco Unified SIP Proxy considers the 503 response as remote element down. Ping 503 mode must first exist before you can use the **no** command.

Examples   The following example enables the server group sip ping 503 command:

```
se-10-0-0-0(cusp-config)> server-group sip ping-503
```

Related Commands

Command	Description
server-group sip element-retries	Configures the number of retries for a SIP server group element.
server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
server-group sip global-ping	Enables global pinging for all SIP server groups.
server-group sip ping-options	Configures the ping options for the SIP server group.
server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

Commands and Notes: Release 9.1.6

To see the new and modified commands associated with Cisco Unified SIP Proxy Release 9.1.6, see:

- show license smart agent-version

show license smart agent-version

To display the smart agent version, use the **show license smart agent-version** command in module EXEC mode.

> **show license smart agent-version**

Syntax Description   This command has no arguments or keywords.

Command Modes   Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
9.1.6	This command was introduced.

Examples   The following example shows the smart agent version:

```
se-10-65-125-184# show license smart agent-version
SmartAgent Version: 1.3.4
```

Related Commands

Command	Description
show license smart summary	Displays the current state of the Cisco Unified SIP proxy licensing application.
show license smart udi	Displays the Unique Device Identifier (UDI) of Cisco Unified SIP Proxy.
show license smart status	Displays the current state of the licensing agent.

Migration to Cisco Unified SIP Proxy 9.1.x

You can migrate from existing Cisco Unified SIP Proxy 8.x releases to Cisco Unified SIP Proxy Release 9.1.x. However, the following are the limitations during the migration:

- Cisco Unified SIP Proxy Release 9.1.x cannot be installed on SRE Module. You require a virtual machine on VMWare ESXi platform to install Cisco Unified SIP Proxy Release 9.1.x.

- Existing Cisco Unified SIP Proxy 8.x SWIFT licenses cannot be migrated to Cisco Unified SIP Proxy 9.1.x. Contact Cisco sales to enquire about the purchase of current Cisco Unified SIP Proxy licenses.

- The backup configuration files from Cisco Unified SIP Proxy 8.x release does not have network related configuration as Cisco SRE module gets the relevant information through RBCP protocol from the host router when it powers up. Cisco Unified SIP Proxy 9.1.x 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 9.1.x, you must manually enter and configure the IP address, subnet mask, and gateway details during reload.

- Cisco Unified SIP Proxy 8.x release configuration has multiple sub-interfaces. The sub-interface format in Cisco Unified SIP Proxy Release 9.1.x 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 if the IP address of the Cisco Unified SIP Proxy on SRE module and Cisco Unified SIP Proxy 9.1.x are different. You must manually configure the listen points.

To migrate from any of the existing Cisco Unified SIP Proxy Releases to Cisco Unified SIP Proxy Release 9.1.x, follow the below steps:

1. Take a backup of the existing Cisco Unified SIP Proxy 8.x configuration. Refer to Cisco Unified SIP Proxy CLI Configuration Guide for more information.

2. Deploy the Cisco Unified SIP Proxy Release 9.1.x OVA on a virtual machine. Refer to the Installation Guide for Cisco Unified SIP Proxy Release 9.1.x for more information.

3. Restore the configuration backup of Cisco Unified SIP Proxy 8.x in Cisco Unified SIP Proxy 9.1.x. Refer to *CLI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.x* for more information.

4. Configure the Smart licenses. Refer to *GUI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.x* and *CLI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.x* for more information.

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 9.1.x, 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.

Related Documentation

Table 1-1 lists the documentation available for Cisco Unified SIP Proxy Release 9.1.x:

Table 1-1   Related Documentation

Document	Description
Installation Guide for Cisco Unified SIP Proxy Release 9.1.x	Describes how to install the Cisco Unified SIP Proxy software, including licenses. Also includes information about moving from Release 1.x to Release 9.1.x.
	http://www.cisco.com/en/US/products/ps10475/prod_installation_guides_list.html
CLI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.x	Contains administrator information, such as maintenance and troubleshooting, for tasks that are performed from the CLI.
	http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html
CLI Command Reference for Cisco Unified SIP Proxy Release 9.1.x	Contains descriptions of all the Cisco Unified SIP Proxy Release 9.1.x-specific CLI commands.
	http://www.cisco.com/en/US/products/ps10475/prod_command_reference_list.html
GUI Configuration Guide for Cisco Unified SIP Proxy Release 9.1.x	Contains administrator information, such as maintenance and troubleshooting, for tasks that are performed from the GUI. Includes online help.
	http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html

Table 1-1   Related Documentation (continued)

Document	Description
Commercial Open Source Information for Cisco Unified SIP Proxy Release 9.1.x	Lists all the open source software used in this project. http://www.cisco.com/en/US/products/ps10475/products_licensing_information_listing.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.