Oracle® Communications Session Border Controller

ACLI Reference Guide

Release S-Cz9.3.0 - for Service Provider and Enterprise
F92204-12
July 2026

ORACLE

Oracle Communications Session Border Controller ACLI Reference Guide, Release S-Cz9.3.0 - for Service Provider and Enterprise

F92204-12

Copyright © 2024, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Contents

About This Guide

My Oracle Support ii

Revision History

1 How to use the ACLI

The ACLI 1
Using the ACLI 1
- Privilege Levels 1
- Enabling Superuser Mode 1
- Debug Mode 2
- System Access 2
  - Local Console Access 2
  - Remote SSH Access 3
- ACLI Help and Display 3
- Exiting the ACLI 3
- Navigation Tips 3
- Hotkeys 3

Command Abbreviation and Completion 4
- Command Abbreviation 4
- Tab Completion 4
- Configuration Element and System Command Menus 5

Context-Sensitive Help 5
- Context-Sensitive Help for System Commands 5
- Viewing Output With the More Prompt 7
- Disabling the More Prompt 8

Configuring Using the ACLI 8
- Line-by-Line Commands 8

Working with Configuration Elements 9
- Creating configurations 9
- Saving configurations with the done command 9
- Viewing configurations with the show command 10

Copyright © 2024, 2026, Oracle and/or its affiliates.

Navigating the configuration tree with the exit command 10
Choosing configurations with the select command 10
Deleting configurations with the no command 11
Deleting an existing configuration element example 11
ACLI Configuration Summaries 12
Viewing Summaries 12
Data Entry 13
ACLI Field Formats 13
Boolean Format 13
Carrier Format 13
Date Format 13
Date and Time Format 14
Day of Week Format 14
Enumerated Format 14
Hostname (or FQDN) Format 14
IP Address Format 15
Name Format 15
Number Format 15
Text Format 15
Time of Day Format 15
Preset Values 15
Default Values 16
Error Messages 16
Special Entry Types Quotation Marks and Parentheses 16
Multiple Values for the Same Field 17
Multi-Word Text Values 17
An Additional Note on Using Parentheses 18
Option Configuration 18
Append Example 18
Delete Example 18

2 ACLI Commands A-M

acl-show 1
acquire-config 1
activate-config 2
archives 2
archives create 6
archives delete 6
archives display 6
archives exit 7
archives extract 7

Copyright © 2024, 2026, Oracle and/or its affiliates.

archives get 7
archives rename 8
archives send 8
arp-add 9
arp-check 9
arp-delete 10
backup-boot-loader 11
backup-config 11
capture 12
check-space-remaining 13
check-stack 14
check-upgrade-readiness 14
clear-alarm 14
clear-cache 15
clear-cache dns 15
clear-cache enum 15
clear-cache registration 16
clear-cache tls 16
clear-resourcemonitor-actions 17
clear-deny 17
clear-sess 17
clear-trusted 18
cli 19
configure terminal 19
control 20
debug-disable 20
debug-enable 20
delete realm-specifics 21
delete-backup-config 21
delete-boot-file 22
delete-config 22
delete-crashfiles 23
delete-import 23
delete-logfiles 24
delete-status-file 24
display-alarms 25
display-backups 26
display-current-cfg-version 26
display-logfiles 26
display-running-cfg-version 27
dump_csv_format 27
dump_diam_dict 28

Copyright © 2024, 2026, Oracle and/or its affiliates.

enable 28
exit 29
format 29
generate-certificate-request 30
generate-key 30
global-trusted-ca 31
halt 32
import-certificate 33
interface-mapping 33
local-accounts 34
log-level 35
lshell 36
monitor 36
mount 37

3 ACLI Commands N-Z

notify 1
- notify algd 1
- notify algd mgcp-endpoint 2
- notify berpd force 2
- notify mbcd 2
- notify radd reload 3
- notify sipd 3
- notify syslog 3
- notify rotate-logs 4
- notify nosyslog 5

package-crashfiles 5
package-logfiles 6
packet-trace 6
ping 8
prompt-enabled 9
realm-specifics 10
reboot 10
request audit 11
request collection 11
reset 13
restore-backup-config 15
run configuration-assistant 16
save-config 16
secret 17
set-system-state 17

Copyright © 2024, 2026, Oracle and/or its affiliates.

set-boot-file 18
set-boot-loader 19
setup entitlements 19
setup product 19
shell 20
show 21
show about 21
show acl 21
show accounting 22
show arp 22
show backup-config 24
show bfd-stats 25
show buffers 25
show built-in-sip-manipulations 25
show call-recording-server 26
show clock 26
show comm-monitor 26
show configuration 29
show directory 31
show dns 32
show dnsalg rate 33
show entitlements 33
show enum 34
show ext-band-mgr 35
show ext-clf-svr 35
show fax-group stats 36
show features 36
show h323d 36
show health 38
show imports 38
show interface-mapping 39
show interfaces 39
show ip 40
show logfile 40
show loglevel 41
show lrt 41
show mbcd 42
show media 50
show memory 51
show monthly-minutes 51
show mps-stats 51
show msrp statistics 52

Copyright © 2024, 2026, Oracle and/or its affiliates.

show nat 52
show neighbor-table 53
show net-management-control 54
show nsep-stats 54
show ntp 55
show packet-trace 55
show platform 56
show platform limits 56
show platform nftables 57
show policy-server 57
show power 58
show privilege 58
show processes 59
show prom-info 61
show queues 62
show radius 62
show ramdrv 63
show realm 63
show rec 63
show rec srg <srg_name> 64
show rec srs <srs_name> 64
show redundancy 67
show registration 69
show route-stats 70
show routes 71
show running-config 71
show sa 72
show security 72
show sessions 74
show sfps 75
show sipd 75
show sipd srg 83
show sipd srs 84
show sipd siprec <message> 84
show sipd siprec errors 85
show snmp-community-table 86
show snmp-info 86
show spl 87
show support-info 87
show system-state 88
show tacacs 88
show temperature 88

Copyright © 2024, 2026, Oracle and/or its affiliates.

show timezone 89
show trap-receiver 89
show uptime 89
show users 90
show version 90
show virtual-interfaces 91
show voltage 91
show wancom 91
show xcode 92
spl 92
ssh-key 93
stack 94
start learned-allowed-elements 94
stop-task 95
stop learned-allowed-elements 95
switchover-redundancy-link 96
synchronize 96
systime-set 96
tail-logfile-close 97
tail-logfile-open 98
tcb 98
test-audit-log 99
test-pattern-rule 99
test-policy 100
test-translation 100
timezone-set 101
Traceroute Command Specifications 102
unmount 103
verify-config 103
watchdog 104

4 ACLI Configuration Elements A-M

access-control 1
account-config 4
account-config > account-servers 12
account-config > push-receiver 14
account-group 15
allowed-elements-profile 15
allowed-elements-profile > rule-sets 16
allowed-elements-profile > rule-sets > header-rules 17
audit-logging 18

Copyright © 2024, 2026, Oracle and/or its affiliates.

auth-params 19
authentication 20
authentication-profile 22
authentication > multi-factor-functionality-enhancement 23
authentication > online-certificate-status-protocol 23
authentication > radius-servers 24
authentication > tacacs-servers 26
bootparam 27
bfd-config 28
bfd-config > bfd-session 29
capture-receiver 30
certificate-record 31
cert-status-profile 33
class-profile 35
class-profile > policy 35
cluster-config 36
codec-policy 39
system-config > comm-monitor 41
system-config > comm-monitor > monitor-collector 42
data-flow 42
diameter-manipulation 43
diameter-manipulation > diameter-manip-rule 44
diameter-manipulation > diameter-manip-rule > avp-header-rule 46
dnsalg-constraints 46
dns-config 49
dns-config > server-dns-attributes 50
dns-config > server-dns-attributes > address-translation 51
dpd-params 51
emergency-dscp-profile 53
enforcement-profile 54
enforcement-profile > subscribe-event 54
enum-config 55
ext-policy-server 57
filter-config 64
factory-accounts 65
fraud-protection 65
fxo-profile 66
fxs-profile 67
h323 69
h323 > h323-stacks 71
h323 > h323-stacks > alarm-threshold 78
http-client 79

Copyright © 2024, 2026, Oracle and/or its affiliates.

http-server 80
home-subscriber-server 81
host-route 82
ice-profile 83
ike-access-control 84
ike-accounting-param 87
ike-certificate-profile 88
ike-config 89
ike-interface 96
ike-key-id 99
ike-sainfo 100
ikev2-ipsec-wancom0-params 102
ims-aka-profile 105
ipsec 106
ipsec > ipsec-global-config 107
ipsec > security-association 108
ipsec > security-association > manual 108
ipsec > security-association > tunnel-mode 110
ipsec > security-policy 110
ipsec > security-policy > outbound-sa-fine-grained-mask 113
iwf-config 114
ldap-cfg-attributes 115
ldap-transactions 116
license 117
local-address-pool 117
local-address-pool > address-range 118
local-policy 118
local-policy > policy-attributes 122
local-response-map 126
local-response-map > entries 126
local-routing-config 132
media-manager-config 133
media-policy 143
media-policy > tos-settings 143
media-profile 144
media-security 147
media-security > dtls-srtp-profile 147
media-sec-policy 148
media-sec-policy > inbound 149
media-sec-policy > outbound 150
msrp-config 150

Copyright © 2024, 2026, Oracle and/or its affiliates.

5 ACLI Configuration Elements N-Z

net-management-control 1
phy-interface > network-alarm-threshold 3
network-interface 4
network-interface > gw-heartbeat 7
network-parameters 8
npli-profile 10
nsep-stats-profile 11
ntp-sync 12
ntp-sync > auth-servers 13
password-policy 13
paste-config 15
phy-interface 15
phy-interface > network-alarm-threshold 17
policy-group > policy-agent 18
policy-group 19
public-key 20
q850-sip-map 20
q850-sip-map > entries 21
qos-constraints 21
radius-servers 22
realm-config 24
realm-config > in-session-translations 41
realm-config > out-session-translations 42
realm-config > auth-attributes 43
realm-group 44
redundancy 44
redundancy > peers 49
redundancy > peers > destinations 50
remove-isup-param 51
resource-monitor-profile 51
response-code-and-phrase-config 53
response-code-and-phrase-entry 53
rph-policy 54
rph-profile 54
rtcp-policy 55
s8hr-profile 55
sdes-profile 56
security-config 58
security > global-trusted-ca 59
session-agent 60

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-agent > auth-attributes 74
session-agent > in-session-translations 75
session-agent > out-session-translations 75
session-agent > match-identifier 76
session-agent > rate-constraints 77
session-agent-group 78
session-agent-id-rule 80
session-constraints 80
session-constraints > rate-constraints 83
session-recording-group 84
session-recording-server 85
session-router-config 87
session-router > holidays 89
session-timer-profile 90
session-translation 91
session-translation > session-trans-rule 91
schedule-backup 92
schedule-backup > config-backup 93
schedule-backup > config-backup > push-receiver 94
sip-advanced-logging 94
sip-advanced-logging > condition 95
sip-config 96
sip-feature 108
sip-feature-caps 110
sip-interface 110
sip-interface > sip-ports 126
sip-isup-profile 128
sip-manipulation 129
sip-manipulation > header-rules 129
sip-manipulation > header-rules > sip-element-rules 131
sip-manipulation > mime-isup-rules 133
sip-manipulation > mime-isup-rules > mime-header-rules 135
sip-manipulation > mime-isup-rules > isup-param-rules 136
sip-manipulation > mime-rules 137
sip-manipulation > mime-rules > mime-headers 139
sip-manipulation > mime-sdp-rules 140
sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules 141
sip-manipulation > mime-sdp-rules > sdp-media-rules 142
sip-monitoring 143
sip-monitoring interesting-events 144
sip-nat 144
sip-profile 147

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-q850-map 148
sip-q850-map > entries 148
sip-recursion-policy 149
sip-recursion-policy > sip-response-code 150
sip-response-map 150
sip-response-map > entries 151
sipura-profile 152
snmp-community 152
snmp-address-entry 153
snmp-group-entry 154
snmp-user-entry 155
snmp-view-entry 157
spl-config 158
spl-config > plugins 158
ssh-config 158
static-flow 160
sti-config 162
sti-header-mapping-ruleset 165
sti-header-mapping-ruleset > mapping-rules 165
sti-heartbeat-config 166
sti-response-treatment-config 167
sti-response-treatment-config > sti-response-treatment-entry 168
sti-server 169
sti-server-group 171
steering-pool 172
surrogate-agent 173
system-access-list 176
system-config 177
system-config > alarm-threshold 186
system-config > collect 187
system-config > collect > push-receiver 189
system-config > collect > group-settings 189
system-config > syslog-servers 192
system-config > directory-cleanup 193
tcp-media-profile 193
tcp-media-profile > profile-list 193
tdm-config 195
tdm-profile 197
test-policy 202
test-sip-manipulation 202
test-translation 204
tls-global 205

Copyright © 2024, 2026, Oracle and/or its affiliates.

tls-profile 205
translation-rules 207
trap-receiver 208
tunnel-orig-params 209
two-factor-authentication 210
web-server-config 210

Copyright © 2024, 2026, Oracle and/or its affiliates.

About This Guide

The ACLI Reference Guide provides a comprehensive explanation of all commands and configuration parameters available to you in the Acme Command Line Interface (ACLI). This document does not explain configurations and the logic involved in their creation.

This publication is used with Oracle Communications Session Border Controller and Oracle Enterprise Session Border Controller.

Document Organization

- About this Guide—This chapter
- How to Use the ACLI—Explains how to use the ACLI, the CLI-based environment for configuring the Oracle Communications Session Border Controller
- Commands A-M—Lists commands starting with A-M, their syntax, and their usage
- Commands N-Z—Lists commands starting with N-Z, their syntax, and their usage
- Configuration Elements A-M—Lists configuration elements starting with A-M, their syntax, and their usage. Subelements are listed directly after the element where they are located.
- Configuration Elements N-Z—Lists configuration elements starting with N-Z, their syntax, and their usage. Subelements are listed directly after the element where they are located.

Conventions

This section explains the documentation conventions used in this guide. Each of the following fields is used in the ACLI Reference Guide. The following are the fields associated with every command or configuration element in this guide. When no information is applicable, the field is omitted (this occurs mostly with the Notes field).

- Description—Describes each command, its purpose, and use.
- Syntax—Describes the proper syntax needed to execute the command. Syntax also includes syntax-specific explanation of the command.
- Arguments—Describes the argument place holders that are typed after a command. For commands only.
- Parameters—Describes the parameters available in a configuration element. For configuration elements only.
  - Default—Default value that populates this parameter when the configuration element is created.
  - Values—Valid values to enter for this parameter.
- Notes—Lists additional information not included in the above fields.
- Mode—Indicates whether the command is executed from User or Superuser mode.
- Path—Describes the ACLI path used to access the command.
- Example—Gives an example of how the command should be entered using one of the command's valid arguments.

Copyright © 2024, 2026, Oracle and/or its affiliates.

This guide uses the following callout conventions to simplify or explain the text.

Caution or Note: This format is used to advise administrators and users that failure to take or avoid a specified action can result in loss of data or damage to the system.

Documentation Set

The following table describes the documentation set for this release.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Revision History

The following table lists the dates and description of the revisions to this document.

Revision History

Date	Description
March 2024	• Initial release.
May 2024	• Updates the sti-server, sti-attest description for accuracy. • Adds description to show arp's active-count argument. • Clarifies the impact of changing the add-icmp-ip and remove-icmp-ip parameters on established calls. • Corrects issue with package-logfiles command.
July 2024	• Adds features for S-Cz9.3.0p2.
October 2024	• Adds features for S-Cz9.3.0p3. • Adds missing cipher for DTLS-SRTP. • Adds resource-monitoring to system-config. • Adds clarification on the format for specifying IPv6 addressing in the access-control element. • Updates tls-global's session-caching parameter to note that this parameter is not RTC supported. • Updates the network-interface, gw-heartbeat's state parameter default value for accuracy. • Adds a note to the local-account command regarding the resetting of passwords. • Updates media-manager-config to indicate deprecated parameters. • Clarifies the UDP+TCP SA transport-method parameter. • Corrects ipsec, ipsec-global-config's red-ipsec-port parameter's default and valid values. • Removes erroneous references to the deprecated TSCF feature. • Removes ladder-diagram-rows parameter from sip-monitoring.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Date	Description
December 2024	• Clarifies entry requirements for running test-translation. • Adds features for S-Cz9.3.0p4. • Adds an extended key usage configuration requirement for the certificate of a TLS profile with mutual authentication. • Updates sip-interface, add-sdp-invite to include the both option. • Corrects the sdes-profile, mki parameter's description to state that the default value is disabled. • Corrects the show configuration command syntax. • Updates session-recording-group to correct the simultaneous-recording-server parameter's default value.
February 2025	• Adds features for S-Cz9.3.0p5.
April 2025	• Remove IPv6 from address attribute in the syslog-servers element. • Adds IPv6 as valid entry for local and remote-ip-addr-match parameters. • Corrects the syntax for the allow-any parameter within the allowed-elements-profile element. • Adds SNMP limitation on show uptime. • Adds note on restore-backup-config. • Adds features for S-Cz9.3.0p6.
June 2025	• Updates the following for accuracy: – sip-interface, contact-mode – authentication, radius-servers, authentication-mode – ntp-sync • Add the **hops** parameter for use with the **ping-method OPTIONS** configuration syntax. • Adds fault-recovery parameter to system-config. • Adds a note to system-config stating that telnet-timeout is deprecated. • Fixes various typographical errors. • Corrects the description of the ftp-push parameter. • Adds caveat with using 0.0.0.0 as a **source-address**.
August 2025	• Removed claim that SNMP/SSH IP are lists rather than single-value parameters. • Adds note that network-interface and phy-interface are not RTC. • Adds feature for S-Cz9.3.0p8. • Updates the media-profile, average-rate-limit's minimum acceptable value.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Date	Description
November 2025	• Adds network-interface requirement for TACACS and RADIUS. • Adds SIPREC limitation to suppress-hold-resume-reinvite. • Adds right-to-left note on codec-policy. • Clarifies show backup-config. • Clarifies partial RTC support for access-control. • Adds use-rtp-marker-bit option to media-manager-config. • Adds default-teams-realm to realm-config.
July 2026	• Corrects the date format in local-policy, activate-time and deactivate-time and session-router, holidays, date. • Updates the description of password-policy for accuracy. • Updates the crypto-list attribute of the sdes-profile to clarify platform-specific values. • Removes the ssh-password command. This command was deprecated and replaced with the local-accounts command in a previous release. • Adds a note about HA deployments in the show enum command. • Clarifies that changing the log level for some tasks is not RTC-supported in log-level command and system-config topic. • In the certificate-record configuration element, adds values supported for compatibility with imported certificate records in key-usage, extended-key-usage, and digest-algor. • Adds clarity around ping-all-addresses. • Adds note about auto-negotiation and fiber interfaces. • Updates local-error values for local-response-map entries. • Adds **cpu-datapath** and **memory-datapath** as values for the **type** parameter in system-config>alarm-threshold, specifies that **value** must be more than 30 for these. • In the **ping-response** parameter in the **session-agent** topic, adds note about response in offline mode. • In **authentication** configuration element, adds **multi-factor-functionality-enhancement** subelement and corresponding topic. • In **local-accounts** command, adds optional authtype parameter.

Copyright © 2024, 2026, Oracle and/or its affiliates.

1

How to use the ACLI

The ACLI

The ACLI is an administrative interface that communicates with other components of the Oracle Communications Session Border Controller. The ACLI is a single DOS-like, line-by-line entry interface.

The ACLI is modeled after industry standard CLIs. Users familiar with this type of interface should quickly become accustomed to the ACLI.

Using the ACLI

You can access the ACLI either through a direct console connection or an SSH connection.

Privilege Levels

There are two privilege levels in the ACLI, User and Superuser. Both are password-protected.

- User—At User level, you can access a limited set of Oracle Communications Session Border Controller monitoring capabilities. You can:
  - View configuration versions and a large amount if statistical data for the system's performance.
  - Handle certificate information for IPSec and TLS functions.
  - Test pattern rules, local policies, and session translations.
  - Display system alarms.
  - Set the system's watchdog timer.
  - Set the display dimensions for your terminal.
    You know you are in User mode when your system prompt ends in the angle bracket (>).
- Superuser—At Superuser level, you are allowed access to all system commands and configuration privileges. You can use all of the commands set out in this guide, and you can perform all configuration tasks.
  You know you are in Superuser mode when your system prompt ends in the pound sign (#).

Enabling Superuser Mode

To enable Superuser mode:

Copyright © 2024, 2026, Oracle and/or its affiliates.

1. At the ACLI User prompt, type the enable command. You will be asked for your Superuser password.

```
ORACLE> enable
Password:
```

2. Enter your password and press <Enter>.

```
Password: [Your password does not echo on the display.]
ORACLE#
```

If your entry is incorrect, the system issues an error message and you can try again. You are allowed three failed attempts before the system issues an error message telling you that there are excess failures. If this occurs, you will be returned to User mode where you can start again.

Debug Mode

Debug mode refers to a set of commands used to access low level functionality on the Oracle Communications Session Border Controller. Users should not access debug mode commands unless specifically instructed to do so by Oracle Engineering or Support.

After booting your Oracle Communications Session Border Controller for the first time with this image, if you have not executed the **debug-enable** command, you may not run debug level commands. The following appears on the screen:

```
ORACLE# shell

Shell access is disabled on this Session Director
ORACLE#
```

To enable debug mode access, use the **debug-enable** command. See the debug-enable command description in the ACLI Reference Guide.

Once you have executed the **debug-enable** command to set a debug level password, if you downgrade the software image, the password you set with **debug-enable** becomes the new shell password for earlier versions.

System Access

You can access the ACLI using the different means described in this section.

Local Console Access

Console access takes place via a serial connection to the console port directly on the Oracle Communications Session Border Controller chassis. When you are working with the Oracle Communications Session Border Controller at the console, the ACLI comes up automatically.

Accessing the ACLI through a console connection is the most secure method of connection, given that the physical location is itself secure.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Remote SSH Access

SSH provides strong authentication and secure communications over unsecured channels. Accessing the ACLI via an SSH connection gives you the flexibility to connect to your Oracle Communications Session Border Controller from a remote location over an insecure connection.

ACLI Help and Display

The Oracle Communications Session Border Controller's ACLI offers several features that aid with navigation and allow you to customize the ACLI so that you can work more efficiently.

- Alphabetized help output—When you enter either a command followed by a question mark, the output is now sorted alphabetically and aligned in columns. The exception is the exit command, which always appears at the end of a column.
- Partial command entry help—When you enter a partial command followed by a question mark, the new Help output displays only commands that match the letter you type rather than the entire list.
- The more prompt—You can set a more option in the ACLI that controls whether or not you can use more with any of the following commands: show, display, acl-show, and view-log-file. Turning this option on gives you the ability to view output from the command one page at a time. By default, this option is enabled. Your setting is persistent across ACLI sessions.
  With the more feature enabled, the ACLI displays information one page at a time and does so universally across the ACLI. A line at the bottom of the screen prompts you for the action you want to take: view the displays's next line or next page, show the entire display at once, or quit the display. You cannot change setting persistently, and need to change them every time you log in.
- Configurable page size—The page size defaults to 24 X 80. You can change the terminal screen size by using the new cli terminal height and cli terminal width commands. The settings for terminal size are not preserved across ACLI sessions.

Exiting the ACLI

Typing exit at any ACLI prompt moves you to the next "higher" level in the ACLI. After exiting out of the User mode, you are logged out of the system.

Navigation Tips

This section provides information about hotkeys used to navigate the ACLI. This information applies to both User mode and Superuser mode, although the specific commands available to those modes differ.

Hotkeys

Hotkeys can assist you in navigating and editing the ACLI, and they also allow you to scroll through a list of commands that you have recently executed. These hotkeys are similar to those found in many other CLIs. The following table lists ACLI hotkeys and a description of each.

The following list describes general system hotkeys:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- <Ctrl-D>—Equivalent of the done command when used at the end of a command line. When used within a command line, this hotkey deletes the character at the cursor.
- <UParrow>—Scrolls forward through former commands.
- <DOWNarrow>—Scrolls backward through former commands.
- <tab>—Completes a partial command or lists all options available if the characters entered match multiple commands. Executed at the beginning of the command line, this hotkey lists the available commands or configurable elements/parameters.
  The following list describes context-sensitive help hotkeys:
- <?>—Provides context-sensitive help. It functions both for ACLI commands and configuration elements and is displayed in alphabetical order.
  The following list describes hotkeys to move the cursor:
- <Ctrl-B>—Moves the cursor back one character.
- <Esc-B>—Moves the cursor back one word.
- <Ctrl-F>—Moves the cursor forward one character.
- <Esc-F>—Moves the cursor forward one word.
- <Ctrl-A>—Moves the cursor to the beginning of the command line.
- <Ctrl-E>—Moves the cursor to the end of the command line.
- <Ctrl-L>—Redraws the screen.
  The following list describes hotkeys to delete characters:
- <Delete>—Deletes the character at the cursor.
- <Backspace>—Deletes the characters behind the cursor.
- <Ctrl-D>—Deletes the character at the cursor when used from within the command line.
- <Ctrl-K>—Deletes all characters from the cursor to the end of the command line.
- <Ctrl-W>—Deletes the word before the cursor.
- <Esc-D>—Deletes the word after the cursor.
  The following list describes hotkeys to display previous command lines:
- <Ctrl-P>—Scrolls backward through the list of recently executed commands.

Command Abbreviation and Completion

This section describes how you can use abridged commands in the ACLI. Command completion can save you extra keystrokes and increase efficiency.

Command Abbreviation

Commands can be abbreviated to the minimum number of characters that identify a unique selection. For example, you may abbreviate the configure terminal command to “config t.” You cannot abbreviate the command to “c t” because more than one command fits this criteria.

Tab Completion

When you do not supply enough characters to identify a single selection, you can press <Tab> to view a list of commands that begin with the character(s) you entered. After you press <Tab>, the ACLI returns you to the system prompt and reprints the character(s) you originally typed. This enables you to complete the command with the characters that uniquely identify the

Copyright © 2024, 2026, Oracle and/or its affiliates.

command that you need. You can continue this process until enough characters to identify a single command are entered.

```
ORACLE# gen generate-certificate-request  generate-key


ORACLE# generate-key
```

Configuration Element and System Command Menus

Command menus and configuration element menus display similarly in the ACLI. The menus for each are divided into two columns. The first column lists all of the command and configuration elements available to a user working in this mode; the second column offers short explanations of each command or configuration element's purpose.

```
ORACLE(local-policy)# ?
from-address      from address list
to-address        to address list
source-realm      source realm list
description       local policy description
activate-time     policy activation date & time
deactivate-time   policy deactivation date & time
state             enable/disable local policy
policy-priority   priority for this local policy
policy-attributes list of policy attributes
select            select a local policy to edit
no                delete selected local policy
show              show selected local policy
done              write local policy information
exit              return to previous menu
```

Context-Sensitive Help

In addition to the information that ACLI menus offer, context-sensitive help can assist you with navigation and configuration. Within this one-line entry, you have access to context-sensitive help that tells you what values are valid for a given field and when you have completed an entry. When the <ENTER> no further known parameters line appears, the ACLI is informing you that there is no subsequent information to enter.

To use the context-sensitive help, enter the name of the command or field with which you require assistance, followed by a <Space> and then a question mark (?). The context-sensitive help information appears.

In general, context-sensitive help provides more detailed information than within ACLI menus. For system commands, it prompts you about the information you need to enter to execute a system command successfully. For configuration elements, it prompts you with a brief description of the field, as well as available values, ranges of values, and data types.

Context-Sensitive Help for System Commands

The ACLI's context-sensitive help feature displays information you need to complete system commands and the body of subcommands available for each system command. In the following example, the show command menu appears. Typing a ? after a system command

Copyright © 2024, 2026, Oracle and/or its affiliates.

asks if the system requires further information to complete a specific command. The system responds with a list of available subcommands.

```
ORACLE# show ?
about                          credit information for acli
accounting                     accounting statistics
acl                            show host access table
algd                           ALG status
arp                            ARP table
backup-config                  show a backup configuration
balancer                       show session load balancer information
bgfd                           BGFD status
buffers                        show memory buffer statistics
built-in-sip-manipulations     Displays all built-in sip-manipulations
call-recording-server          Call Recording Server Statistics
clock                          system clock
configuration                  show current configuration
directory                      show files in a directory
dns                            DNS information
enum                           ENUM information
ext-band-mgr                   External Bandwidth Manager status
ext-clf-svr                    External CLF Server status
features                       currently enabled features
h248d                          H248D status
h323d                          H323D status
health                         system health information
hosts                          show host table
imports                        show all files available for import
interfaces                     show network interfaces
ip                             IP system information
logfile                        Display a log file, 'enter' to display list
loglevel                       loglevels of current processes
lrt                            LRT (local-routing) information
mbcd                           MBCD status
media                          show media interface information
memory                         memory statistics
monthly-minutes                monthly minutes information for a specified realm
nat                            show NAT table
neighbor-table                 ICMPv6 neighbor table
net-management-control         Network Management Controls Statistics
nsep-stats                     NS/EP RPH call statistics
ntp                            NTP status
packet-trace                   displays the current packet trace addresses
policy-server                  external policy server name
power                          current state of each power supply
privilege                      show current privilege level
processes                      active process statistics
prom-info                      show prom information
qos                            show qos FPGA information
radius                         radius accounting and authentication statistics
ramdrv                         ramdrv space usage
realm                          realm statistics
redundancy                     redundancy status
registration                   SIP Registration Cache status
route-stats                    show routing statistics
routes                         show routing table entries
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
running-config              current operating configuration
sa                          security-associations information
security                    security information
sessions                    Session Statistics
show
sipd                        SIPD status
snmp-community-table        show snmp community table
snmp-info                   show snmp
space                       check the remaining space on the device specified
spl                         SPL information
spl-options                 display information on all SPL options
support-info                show all required support information
system-state                current system-state
tacacs                      tacacs authorization, accounting and
authentication statistics
temperature                 current SD temperature readings
timezone                    show timezone for the system (start and end time
in  mmddHH format)
trap-receiver               show snmp trap receivers
uptime                      system uptime
users                       currently logged in users
version                     system version information
virtual-interfaces          show virtual interfaces
voltage                     current SD voltages (SD-II only)
wancom                      show wancom interfaces
```

The system responds with a no further known parameters if there are no subcommands.

```
ORACLE# show about ?
<ENTER!>  no further known parameters
ORACLE# show about
```

Viewing Output With the More Prompt

When the output of a command is too large to fit your screen, the system displays the output in smaller sections. At the end of a section a message is displayed with your options:

- <Space> —Display the next section of output
- <q>—Quits and returns to the system prompt
- <c>—Displays the rest of the output in its entirety

```
ORACLE# show ?
about                       credit information for acli
accounting                  accounting statistics
acl                         show host access table
algd                        ALG status
arp                         ARP table
backup-config               show a backup configuration
balancer                    show session load balancer information
bgfd                        BGFD status
buffers                     show memory buffer statistics
built-in-sip-manipulations  Displays all built-in sip-manipulations
call-recording-server       Call Recording Server Statistics
clock                       system clock
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
configuration                 show current configuration
directory                     show files in a directory
dns                           DNS information
enum                          ENUM information
ext-band-mgr                  External Bandwidth Manager status
ext-clf-svr                   External CLF Server status
features                      currently enabled features
h248d                         H248D status
h323d                         H323D status
health                        system health information
hosts                         show host table
imports                       show all files available for import
interfaces                    show network interfaces
ip                            IP system information
logfile                       Display a log file, 'enter' to display list
('space' for next page; 'q' to quit; 'enter' for next line; 'c' to
continue)
```

Disabling the More Prompt

If you don’t want the Oracle Communications Session Border Controller to display the More prompt, you can disable it using the cli command.

```
ORACLE# cli more disabled
The ACLI 'more' option has been disabled
ORACLE#
```

Configuring Using the ACLI

This section describes the two ACLI methods available for configuring the Oracle Communications Session Border Controller using line-by-line ACLI commands.

Line-by-Line Commands

Using line-by-line commands, you can target a specific field for editing. Line-by-line commands appear in the ACLI as their name suggests: each argument consists of a parameter followed by a valid value, both on one line.

At any time, you can access either the element menu or the context-sensitive help to guide you. In the following example, you enter values for three parameters, and then issue the show command to check your work. Finally, type done to save your configuration.

```
ORACLE(trap-receiver)# ip-address 10.0.0.1
ORACLE(trap-receiver)# filter-level major
ORACLE(trap-receiver)# community-name acme
ORACLE(trap-receiver)# show
trap-receiver
        ip-address                                              10.0.0.1
        filter-level                                            Major
        community-name                                          acme
ORACLE(trap-receiver)# done
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Working with Configuration Elements

Configuring elements involves entering the ACLI path to the configuration element you want to configure, and then entering the parameter name followed by a space and proper data in accordance with the required format.

A common set of commands appear in all configuration elements, and are not applicable for user and superuser commands. These commands are:

- **select**—Used to select a configuration element to edit or view.
- **no**—Used to delete the current configuration element object.
- **show**—Used to view the current values of parameters in the selected configuration element.
- **done**—Used to save configuration changes.
- **exit**—Used to exit the current configuration element or path to the next higher level.

Creating configurations

Creating configuration elements involves first traversing to the ACLI path to enter configurations. Once you are in the element you want to configure, enter a parameter name followed by a value.

```
ORACLE(trap-receiver)# ip-address 10.0.0.1
ORACLE(trap-receiver)# filter-level major
ORACLE(trap-receiver)# community-name acme
ORACLE(trap-receiver)# done
```

Saving configurations with the done command

At all levels of the ACLI hierarchy, there are several methods of saving your settings and data.

- The **done** command, which is entered within a configuration element.
- The hotkey **<Ctrl-D>**, which is entered within a configuration element. This enters the done command in the command line and saves your information.

The `Save Changes y/n ? #` prompt appears when you **exit** a configuration element without saving your changes . This prompt only appears if you have changed old information and/or entered new information.

Every configuration element contains the **done** command.

We strongly recommend that you save your configuration information as you work. This ensures that your configurations have been written to the system database.

```
ORACLE(snmp-community)# done
    community-name                  acme_community
        access-mode                     READ-ONLY
        ip-addresses
                                        10.0.0.2
        last-modified-by
        last-modified-date
ORACLE(snmp-community)#
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Viewing configurations with the show command

We recommend that you view all of the information you have entered before carrying out the done command or another method of saving. Use the show command to review your configurations. Reviewing your settings will give you the opportunity to make any necessary changes before writing the information to the system database.

To view configuration information, type show when you are finished with a line-by-line entry. The following example illustrates the use of the **show** command before executing the done command.

```
ORACLE(host-route)# show
host-route
        dest-network                        10.1.0.0
        netmask                             255.255.0.0
        gateway                             172.30.0.1
        description                         Test host route
        last-modified-by                    admin@console
        last-modified-date                  2014-01-15 17:12:07
```

Navigating the configuration tree with the exit command

The **exit** command moves you to the next-higher location in the configuration tree. In addition, when you use the **exit** command and have not already saved your changes, the ACLI produces the following message:

```
Save Changes y/n #
```

When this line appears, the ACLI is prompting you to save your configurations. This prompt only appears if you have changed old information or entered new information.

If you type anything other than a y in response to the `Save Changes y/n ? #` prompt, the system will interpret that character as a no response and will not save your work. You must type a y to save your work.

Choosing configurations with the select command

Editing individual configurations in the ACLI involves finding the element or field you need to update, entering the new information, and then saving the element.

To select an existing configuration element:

1. Enter the configuration path of the element for which you want to edit.
2. Use the **select** command to choose an element to update. A list of options appears when you press <Enter> at the key field prompt (e.g., <name:>).
3. Enter the number corresponding to the element you would like to update and press <Enter>. If there are no elements configured, you will still be presented with the prompt, but no list will appear. When you press <Enter> at the key field prompt, you will be returned to the system prompt.

   ```
   ORACLE(phy-interface)# select
   <name>: <Enter>
   1: phyTEST
   ```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
2: phyTEST-RIGHT
3: mn1
selection:3
ORACLE(phy-interface)#
```

4. Use the show command to display all configured values of the selected configuration element.

```
ORACLE(phy-interface)#show
phy-interface
        name                            mn1
        operation-type                  Control
        port                            0
        slot                            0
        virtual-mac
        wancom-health-score             55
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2012-11-12 11:02:09
```

5. Optionally make any changes you to parameters in the selected configuration element. You can also overwrite parameters by entering a new value after a previous value has been created.
6. Use the **done** command to save your updates.

Deleting configurations with the no command

There are two methods of deleting configurations.

- You can delete the information for elements while you are still working with them.
- You can delete all configuration information for a previously configured element.

For either method, use the **no** command to clear configurations. Only Multiple Instance Elements can be deleted from the system. Single Instance Elements can not be deleted; they can only be edited.

Deleting an existing configuration element example

You can only delete configurations from within their ACLI path. Use the select command to choose the configuration element you want to delete.

To delete an existing element:

1. Enter the ALCI path to the element you wish to delete.
2. Enter the **no** command. After you do so the key field prompt (e.g., <name:>) appears with a list of the existing configured elements beneath it.

```
ORACLE(media-profile)# no
<name>: <Enter>
1: PCMU
2: G723
3: G729
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

3. Enter the number corresponding to the element you wish to delete.

```
selection:3
```

4. To confirm the deletion, use the **select** command to view the list of remaining elements.

```
ORACLE(media-profile)# select
<name>: <Enter>
1: PCMU
2: G723
```

ACLI Configuration Summaries

The ACLI offers several ways for you to view configuration summaries. While the most straightforward and commonly-used method is the show command, the ACLI also provides summary information every time you execute the done command.

Viewing Summaries

The show command that appears for each ACLI configuration element allows you to view the configured information for a given element. The following example shows how to view media-profile configuration summaries.

To view the settings for the media-profile element:

1. Enter the media-profile configuration element through the ACLI path.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# media-profile
ORACLE(media-profile)#
```

2. From media-profile, use the select command. The **<name>:** prompt and a list of configured media-profile elements appear.

```
ORACLE(media-profile)# select
<name>:
1: PCMU
2: G723
3: G729
```

3. Select the configured media profile you want to view by entering the corresponding number and press the <Enter> key.

```
selection: 1
```

4. Type **show** and press the <Enter> key.

```
ORACLE(media-profile)# show
media-profile
        name                            PCMU
        subname
        media-type                      audio
        payload-type
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
transport                       RTP/AVP
req-bandwidth                   0
frames-per-packet               0
parameters
average-rate-limit              0
peak-rate-limit                 0
max-burst-size                  0
sdp-rate-limit-headroom         0
sdp-bandwidth                   disabled
police-rate                     0
standard-pkt-rate               0
last-modified-by
last-modified-date
```

Data Entry

To enter data using the ACLI, your entries must conform to required field formats. This section describes these formats, gives information about preset values, default values, and error messages.

The final part of this section covers information about using quotation marks (“”) and parentheses (()) to enhance your data entry options and capabilities.

Note that, unless specified by the criteria of a specific field, the maximum number of characters that you can enter to a single ACLI command is 1023.

ACLI Field Formats

This section describes required data entry formats. You can learn the data type for a field by using the menu or the help function.

Boolean Format

Boolean entries take the form of either enabled or disabled. To choose one of these two values, type either enabled or disabled.

Carrier Format

Carrier entries can be from 1 to 24 characters in length and can consist of any alphabetical character (Aa-Zz), numerical character (0-9), punctuation mark (! ”$ % ^ & * ( ) + - = ‘ | { } [ ] @ / \ ‘ ~ , . _ : ;), or any combination of alphabetical characters, numerical characters, or punctuation marks. For example, both 1-0288 and acme_carrier are valid carrier field formats.

Date Format

Date entries must adhere to the ccYY-mM-dD format, where cc is the century, YY is the year, mM is the month, and dD is the day (e.g., 2005-06-10). The minimum entry requirement for date fields is YY-M-D.

The Oracle Communications Session Border Controller can assign the current century (cc) information, as well as leading zeroes for the month (m) and the day (d). Date fields must be entered in the valid format described above.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Date and Time Format

The date and time format displays both the date and time and adheres to the yyyy-mm-dd hh:mm:ss.zzz or yyyy-mm-dd-hh:mm:ss.zzz where y=year, m=month, d=day, h=hours, m=minutes, s=seconds, and z=milliseconds.

Day of Week Format

Day of week entries set any combination of day(s) of the week plus holidays that the local-policy-attributes can use for preference determination. The day of week field options are:

- U—Sunday
- M—Monday
- T—Tuesday
- W—Wednesday
- R—Thursday
- F—Friday
- S—Saturday
- H—Holiday
  This field format cannot accept spaces. For example, U-S and M,W,F are valid day of week field entries.

Enumerated Format

Enumerated parameters allow you to choose from a preset list of values. To access the list of choices from within the ACLI, use the help function for the appropriate parameter.

Hostname (or FQDN) Format

Hostname (FQDN) entries consist of any number of Domain Labels, separated by periods, and one Top Label. The minimum field value is a single alphabetical character to indicate the top label value (e.g., c to indicate '.com').

All hostname fields support IPv4 addresses as well as hostnames.

For Example: In the hostname acme-packet.domainlabel.example100.com, acme-packet is a domain label, domainlabel is a domain label, example100 is a domain label, and com is the top label.

- domain label—acme-packet, domainlabel, example100
- top label—com
  Note that each label is separated by a period.

  The following describes hostname (FQDN) format label types:
- Domain Label—A domain label consists of any number or combination of alphabetical or numerical characters, or any number or combination of alphabetical or numerical characters separated by a dash (-). A dash must be surrounded on both sides by alphabetical or numerical characters, any number or combination. A dash cannot immediately follow or precede a period (.). A domain label is not required in a hostname field value.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Top Label—A top label is the last segment of the hostname. A top label must start with an alphabetical character; it cannot start with a numerical character or with a dash (-). After the first character, a top label can consist of any number, or combination of alphabetical or numerical characters or any number or combination of alphabetical or numerical characters separated by a dash. Similar to dashes in domain labels, a top label dash must be surrounded on both sides by alphabetical or numerical characters, any number or combination. A single alphabetical character is the minimum requirement for a hostname field value.

IP Address Format

IP address entries must follow the dotted decimal notation format and can only include numerical characters (0-9). Entries for an IP address field should be between 0.0.0.0 and 255.255.255.255.

Name Format

Name entries must start with an upper- or lower- case alpha numeric character(A-Z, a-z, 0-9) or an underscore symbol (_). The length of a name entry can continue for another 127 characters for a total of 128 characters. Additional valid characters in the 2nd -128th position include period (.), dash (-), and additional underscores (_) (e.g., acmepacket_configuration).

Number Format

Number entries (e.g., phone number digits without dashes, any address that is not a hostname, etc.) can be any numerical character (0-9) or alphabetical character from A through F (A-Fa-f) or any combination of numerical and alphabetical characters from A through F (0-9A-Fa-f) (e.g., 18005551212 or 18005552CAB). The minimum number of characters for a number entry is 1, and the maximum number is 32.

Text Format

Text entries (e.g., description fields) do not need to follow a particular format. Text fields can accommodate any combination of printable numerical and alphabetical characters, spaces, and most symbols. Noted exceptions are the ampersand (&), the apostrophe (‘), and the less than symbol (<). Entries with spaces must be entered fully within quotation marks. For example, “This is the official Oracle Communications Session Border Controller configuration” is a valid text entry.

Time of Day Format

Time of day entries must include only numerical characters (0-9) and must follow the 4-digit military time format (e.g., 1400). Time of day entries set the time of day that attributes can be considered for preference determination. The minimum field value is 0000, and the maximum field value is 2400.

Preset Values

All configurations share one field: last-modified-date. This field value is set by the system database and can not be altered. It displays the date and time of the last modified action. The system sets this value automatically.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Default Values

By default, the system populates some ACLI values with preset system values if you do not configure them.

Error Messages

The ACLI produces error messages when information cannot be saved or commands cannot be executed. These events may occur when there is a problem either with the command itself, the information entered, the format of the information entered, or with the system in general.

For example, if you enter several words for a description and you do not put the entry inside quotation marks, the ACLI will tell you that you have entered an invalid number of arguments. In the example below, a user entered a media-type field value of “audio visual,” but did not enclose the value in quotation marks (“”).

```
ORACLE(media-profile)# media-type audio visual
invalid number of arguments
ORACLE(media-profile)#
```

When the value does not conform to format requirements, the ACLI returns a message that you have made an invalid entry for a given field. In the example below, a user entered an invalid IP address.

```
ORACLE(snmp-community)# ip-addresses (1877.5647.457.2 45.124 254.65.23)
invalid IP address
ORACLE(snmp-community)#
```

Message	Description
error invalid data...	You have entered a value not permitted by the system. This error includes numeric values that exceed defined parameters and misspellings of specifically spelled values (such as “enabled” or “disabled”).
% command not found	You entered a command that is not valid. The command may be misspelled, or it may not exist where you are working.
invalid selection...	You have selected an item that does not exist in the system.
invalid number of arguments	You either have entered too many arguments (or commands) on one line or you may not have quotation marks (“”) around your multi-word entry.
error 500 saving ...	The system could not save the data you entered to the system database.

Special Entry Types Quotation Marks and Parentheses

The ACLI uses certain syntax in order to increase ease of use.

- Quotation marks (“”)—The values inside quotation marks are read as being one argument; commonly used in text fields.
- Parentheses (())—The values inside parentheses are read as being multiple arguments for an element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Multiple Values for the Same Field

To enter multiple values for the same field, you can either use quotation marks (“”) or parentheses (()) in order to express these values to the system. In a field that might contain multiple values, you must use either of these when you enter more than one value.

Your use of either of these methods signals to the system that it should read the data within the punctuation marks as multiple values. The following example shows how parentheses (()) are used in an instance of the local-policy element.

In the example that follows, there are three entries for the to-address in the parentheses (()).

Note

If you enter multiple values within either quotation marks (“”) or parentheses (()), be sure that the closing marks are made directly after the final value entered. Otherwise, the system will not read your data properly.

```
ORACLE(local-policy)# to-address (196.154.2.3 196.154.2.4 196.154.2.5)
ORACLE(local-policy)# show
local-policy
        from-address
                                        *
        to-address
                                        196.154.2.3
                                        196.154.2.4
                                        196.154.2.5
        source-realm
                                        public
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by
        last-modified-date
```

Multi-Word Text Values

For many fields, you may want to enter a multi-word text value. This value may either be a series of descriptive words, a combination of words and numbers that identify a location, or a combination of words and numbers that identify a contact person.

To enter a multi-word text value, surround that value either with quotation marks (“”) or parentheses (()). Generally, quotation marks are most commonly used to configure text fields. The example below shows how quotation marks (“”) surround a multi-word value.

```
ORACLE(session-router-config)# holidays
ORACLE(session-router-holidays)# date 2008-01-01
ORACLE(session-router-holidays)# description "new year's day"
ORACLE(session-router-holidays)# done
        holiday
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
date                            2010-10-10
description                     sample day
```

An Additional Note on Using Parentheses

Parentheses can be used in the ACLI to enter multiple arguments on the same line. A command line can contain any number of entries inside parentheses. Single parentheses (()) connote one list, nested parentheses ((())) connote a list within a list, and so forth.

Option Configuration

The options parameter shows up in many configuration elements. This parameter is used for configuring the Oracle Communications Session Border Controller to behave with either non-standard or customer-specific behavior.

Several options might be configured for a single configuration element. Every time you configure the option parameter, you overwrite the previously configured option list for the selected instance of the configuration element.

There is a shortcut to either add or delete a single option to the full option list. By typing a “+” to add or a “-” to subtract immediately before an option, you can edit the currently configured option list.

Append Example

With the forceH245 option preconfigured, you can append a new option without deleting the previously configured option :

```
ORACLE(h323)# options +noAliasInRCF
ORACLE(h323)#  show
h323-config
        state                           enabled
        log-level                       NOTICE
        response-tmo                    4
        connect-tmo                     32
        rfc2833-payload                 101
        alternate-routing               proxy
        codec-fallback                  disabled
        enum-sag-match                  disabled
        remove-t38                      disabled
        options                         noAliasInRCF
        last-modified-by                admin@console
        last-modified-date              2014-01-14 20:17:42
```

Delete Example

You can also delete a single existing option from the options list. Continuing from the previous example:

```
ORACLE(h323)# options -forceH245
ORACLE(h323)# show
h323-config
        state                           enabled
        log-level                       NOTICE
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
response-tmo                4
connect-tmo                 32
rfc2833-payload             101
alternate-routing           proxy
codec-fallback              disabled
enum-sag-match              disabled
remove-t38                  disabled
options                     noAliasInRCF
last-modified-by            admin@console
last-modified-date          2014-01-14 20:19:43
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

2

ACLI Commands A-M

acl-show

The acl-show command shows a list of denied ACL entries.

Syntax

```
acl-show
```

Mode

Superuser

Notes

The acl-show command displays a list of the following denied ACL entries:

- Incoming port, slot, and VLAN tag
- Source IP, bit mask, port, and port mask
- Destination IP address and port
- Protocol
- ACL entry as static or dynamic
- ACL entry index

Example

```
ORACLE# acl-show
```

acquire-config

The acquire-config command retrieves the configuration from one SBC for configuration checkpointing an HA node.

Syntax

```
acquire-config <IPAddress>
```

Arguments

<IPAddress> Enter the IP address of the SBC to acquire a configuration from.

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

Notes

This command forces one SBC in an HA node to learn the configuration from the other system. If configuration checkpointing is already running, the **acquire-config** command has no effect.

The acquire-config command is not supported on wancom interfaces that use both VLANs and IPv6.

Only after the **acquire-config** command is executed and the SBC is rebooted will the process of acquiring the configuration be complete.

Example

```
ORACLE#acquire-config 10.1.1.1
```

activate-config

The activate-config command activates the current configuration on the Oracle Communications Session Border Controller to make it the running configuration.

Syntax

```
activate-config
```

Mode

Superuser

Notes

Before executing this command, be aware of the real time configuration (RTC) consequences on the operation of the Oracle Communications Session Border Controller.
To use RTC, the activate-config command is executed to alert the Oracle Communications Session Border Controller that the current configuration has changed and that it needs reload configuration information.

Example

```
ORACLE# activate-config
```

archives

The archives command is used for creating, moving, and manipulating archived log files. All archive files are created in .tar.gz format in SD Software versions 2.0 and above. All commands are executed from within the archives menu.

Log files contain a record of system events. Log files are stored in the /code/logs directory. The CFG archive type is no longer supported in C6.2.0. When an archive command is entered with the CFG type, the Oracle Communications Session Border Controllerresponds with an error message.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

Type **archives** at the topmost prompt before executing any of the below commands to enter the archives shell.

Syntax

archives > create

```
create LOGS <logfile-name>
```

Arguments

<logfile-name> Enter the name of archive file that contains all logs To create an archive file of a log, type create LOGS and enter a logfile name. Archives are created in .tar.gz (tarred and gzipped) format.

Example

```
ORACLE(archives)# create LOGS jun_30.gz
```

Syntax

archives > delete

```
delete LOGS <logfile-name>
```

Arguments

<filename> Enter the filename of the log archive to delete The archives > delete command deletes the specified archive file from the Oracle Communications Session Border Controller. You must append “.tar.gz” to the filename when using this command. Use the archives > display command to list the available log archives to delete.

Example

```
ORACLE(archives)# delete LOGS july_16.gz
```

Syntax

archives > display

```
display LOGS
```

Arguments

This command lists the log archives currently saved on the Oracle Communications Session Border Controller’s file system.

Example

```
ORACLE(archives)# display LOGS
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

archives > exit

```
exit
```

Example

```
ORACLE(archives)# exit
```

> **Note**
>
> This command exits from the archives session and returns you to the ACLI Superuser system prompt.

Syntax

archives > extract

This command is no longer supported in release C6.2.0.

Syntax

archives > get

```
get LOGS <archive-name> <remote-host> <user-name> <password>
```

Arguments

<remote-name> Enter the full path and filename to retrieve

<host> Enter the IP address of the remote host

<user-name> Enter the user name on remote host

<password> Enter the password on remote host

Example

```
ORACLE(archives)# get LOGS may_31.gz
```

> **Note**
>
> This command retrieves an archived log. If you do not include all the necessary arguments, the get command will prompt you for the arguments you omitted. The get command writes the retrieved file to the /code/logs/<archive-name> path.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

archives > rename

```
rename LOGS <old-archive> <new-archive>
```

Arguments

<current_name> Enter the old archive name

<new_name> Enter the new archive name

Example

```
ORACLE(archives)# rename LOGS june sept
```

> **Note**
>
> Renames an archived log. You do not need to append ".tar.gz" to the filename when using this command.

Syntax

archives > send

```
send LOGS <archive-name> <host-ip-address> <username>
```

Arguments

<archive-name> Enter the name of archive file to send

<host-ip-address> Enter the IP address of FTP server

<username> Enter the FTP username on server

Example

```
ORACLE(archives)# send LOGS Oct_24.gz 1.0.100.7 user1
```

> **Note**
>
> This command sends an archived log file to a remote host using FTP. If you do not include all the necessary arguments, the send command will prompt you for the arguments you omitted.

Copyright © 2024, 2026, Oracle and/or its affiliates.

archives create

Syntax

```
create LOGS <logfile-name>
```

Arguments

- <logfile-name> Enter the name of archive file that contains all logs

To create an archive file of a log, type create LOGS and enter a logfile name. Archives are created in .tar.gz (tarred and gzipped) format.

Example

```
ORACLE(archives)# create LOGS jun_30.gz
```

archives delete

Syntax

```
delete LOGS <logfile-name>
```

Arguments

<filename> Enter the filename of the log archive to delete
The archives > delete command deletes the specified archive file from the Oracle Communications Session Border Controller. You must append ".tar.gz" to the filename when using this command. Use the archives > display command to list the available log archives to delete.

Example

```
ORACLE(archives)# delete LOGS july_16.gz
```

archives display

Syntax

```
display LOGS
```

This command lists the log archives currently saved on the Oracle Communications Session Border Controller file system.

Example

```
ORACLE(archives)# display LOGS
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

archives exit

Syntax

```
exit
```

> **Note**
>
> This command exits from the archives session and returns you to the ACLI Superuser system prompt.

Example

```
ORACLE(archives)# exit
```

archives extract

This command is unsupported.

archives get

Syntax

```
get LOGS <archive-name> <remote-host> <user-name> <password>
```

Arguments

- <remote-name> Enter the full path and filename to retrieve
- <host> Enter the IP address of the remote host
- <user-name> Enter the user name on remote host
- <password> Enter the password on remote host

> **Note**
>
> This command retrieves an archived log. If you do not include all the necessary arguments, the get command will prompt you for the arguments you omitted. The get command writes the retrieved file to the /code/logs/<archive-name> path.

Example

```
ORACLE(archives)# get LOGS may_31.gz
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

archives rename

Syntax

```
rename LOGS <old-archive> <new-archive>
```

Arguments

- <current_name> Enter the old archive name
- <new_name> Enter the new archive name

> **Note**
>
> Renames an archived log. You do not need to append ".tar.gz" to the filename when using this command.

Example

```
ORACLE(archives)# rename LOGS june sept
```

archives send

Syntax

```
send LOGS <archive-name> <host-ip-address> <username>
```

Arguments

- <archive-name> Enter the name of archive file to send
- <host-ip-address> Enter the IP address of FTP server
- <username> Enter the FTP username on server

> **Note**
>
> This command sends an archived log file to a remote host using FTP. If you do not include all the necessary arguments, the send command will prompt you for the arguments you omitted.

Example

```
ORACLE(archives)# send LOGS Oct_24.gz 1.0.100.7 user1
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

arp-add

The arp-add command manually adds ARP entries for media interfaces to the ARP table.

Syntax

```
arp-add <slot> <port> <vlan ID> <ip-address> <mac-address>
```

Arguments

<slot> Select the media interface slot

Values:

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values:

- 0—Leftmost port
- 1— Second from left port
- 2 —Third from left port (not applicable for GigE cards)
- 3 —Rightmost port (not applicable for GigE cards)

<vlan ID> VLAN identifier

<ip-address> Enter the IP address

<mac-address> Enter the MAC address in hexadecimal notation

Mode

Superuser

Example

```
ORACLE# arp-add 1 0 0 172.16.1.102 ab:cd:ef:01:23:14
```

arp-check

The arp-check command forces the SD to send an ARP request for the specified IP address. The command does not send an ARP request if the specified address is already in the ARP table or is in a different subnet.

Syntax

```
arp-check <slot> <port> <vlan-ID> <ip-address>
```

Arguments

<slot> Select the media interface slot

Copyright © 2024, 2026, Oracle and/or its affiliates.

Values

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values

- 0—Leftmost port
- 1— Second from left port
- 2 —Third from left port (not applicable for GigE cards)
- 3 —Rightmost port (not applicable for GigE cards)

<vlan ID> Enter the VLAN identifier

<ip-address> Enter the IP address

Mode

Superuser

Example

```
ORACLE# arp-check 0 0 0 11.21.0.10
```

arp-delete

The arp-delete command manually removes ARP entries from the ARP table.

Syntax

```
arp-delete <slot> <port> <vlan-ID> <ip-address>
```

Arguments

<slot> Select the media interface slot
Values:

- 0—Left slot
- 1—Right slot

<port> Select the media interface port

Values:

- 0—Leftmost port
- 1— Second from left port
- 2 —Third from left port (not applicable for GigE cards)
- 3 —Rightmost port (not applicable for GigE cards)

<vlan ID> Enter the VLAN identifier

<ip-address> Enter the IP address

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# arp-delete 1 0 1 12.11.0.100
```

backup-boot-loader

The **backup-boot-loader** command copies the current bootloader into the `/code/images` directory.

Syntax

```
backup-boot-loader <filename>
```

Arguments

<filename>
Enter the filename of the bootloader.

Mode

Superuser

Example

```
ORACLE# backup-boot-loader bootloader

Successfully copied bootloader to '/code/images/bootloader'
ORACLE#
```

backup-config

The backup-config command backs up the current flash memory configuration to the specified filename in the /code/bkups directory.

Syntax

```
backup-config <name-of-backup> [running | editing] [standard | non-standard]
```

Arguments

<name-of-backup> Enter the name of the backup configuration file
running- Backup the configuration from the running configuration cache. This is an optional argument

editing- Backup the configuration from the editing configuration cache. This is an optional argument.

standard- Use standard XML as the file format

Copyright © 2024, 2026, Oracle and/or its affiliates.

non-standard- Use non-standard, legacy XML for the file format

Mode

Superuser

Example

```
ORACLE# backup-config FEB_BACKUP.gz running
```

> **Note**
>
> If insufficient disk space is available, the Oracle Communications Session Border Controller will not complete the task.

capture

The **capture** command is an ACLI command that specifies a dynamic filter specifying traffic to be sent to the Monitor and Trace GUI interface. This command is only supported by Oracle Enterprise Session Border Controller.

Syntax

The syntax for **capture** follows.

```
capture <start|stop> <main filter> <subfilter(s)>
```

> **Note**
>
> Initiating these commands does not change the values set in the ACLI-configured filters. Dynamic filters remain active until you initiate a stop command.

The syntax for the dynamic filter commands are:

```
capture start <main filter> <subfilter(s)>


capture stop <main filter> <subfilter(s)>
```

You must enter a `<main filter>` and a `<subfilter(s)>` when initiating the **capture start** and **capture stop** commands.

Arguments

<start | stop>—Specifies whether to start or stop the dynamic capture specified by the ensuing filters.

<filter>

- global—Monitors and captures all traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- int-ev <short-session | local-rejection>—Monitors and captures traffic matching the short-session and/or local-rejection configured within the **sip-monitoring** element.
- realm <realm name>—Monitors and captures traffic in the matching realm
- session-agent <session-agent name>—Monitors and captures traffic passing through the matching session agent.

<subfilter>

- * —Monitors and captures all sessions.
- user <Phone Number or User Part URI>—Monitors and captures everything that matches this phone number or user part.
- addr-prefix <IP address or IP address and netmask>—Monitors and captures everything that matches this address or address prefix.

Mode

Superuser

Example

```
ORACLE# capture start realm core1 user user1
```

check-space-remaining

The check-space-remaining command displays the remaining amount of space in the boot directory, code (or flash memory), and ramdrv devices.

Syntax

```
check-space-remaining <device>
```

Argument

<device> Select where to check the remaining space
Values:

- boot
- code
- ramdrv

Mode

Superuser

Example

```
ORACLE# check-space-remaining boot
```

> **Note**
>
> The output of this command is in bytes.

Copyright © 2024, 2026, Oracle and/or its affiliates.

check-stack

This command is not supported in this software release.

check-upgrade-readiness

The check-upgrade-readiness command displays system status information targeting users who are upgrading software. The system runs the command automatically after a reboot during which the system detects a change in software version.

Syntax

```
check-upgrade-readiness < verbose >
```

When issued without the verbose argument, the command presents a summary status on the system. When issued with the verbose argument, the system displays each individual system check, categorized and presented with status and technical detail.

Argument

<verbose> Extends the output beyond status report to present lines on each individual system check.

Mode

Superuser

Example

```
ORACLE# check-upgrade-readiness
```

clear-alarm

The clear-alarm command clears a specified alarm.

Syntax

```
clear-alarm <alarm_id> <task_id>
```

Arguments

<alarm_id> Enter a unique 32-bit integer that contains a 16-bit category name or number and a unique 16-bit identifier for the error or failure within that category

<task_id> Enter the task ID of the task that sent the alarm

Example

```
ORACLE# clear-alarm 65524 sip
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> For alarm identification and task codes for specific alarms, use the **display-alarms** command.

clear-cache

The clear-cache command allows you to clear a specified cache entry on the Oracle Communications Session Border Controller.

clear-cache dns

Syntax

```
clear-cache dns <realm id | “all” > <cache entry key | “all”>
```

This command allows you to clear a specified DNS cache entry or all entries.

Arguments

- <realm id | all> Specify the realm whose DNS cache you want to clear or enter all if you want to clear the cache of all realms
- <cache entry key> Enter a specific cache entry key or enter all for all entries. A specified cache entry key should take one of the following forms.
  - NAPTR entries—NAPTR:test.com
  - SRV entries—SRV:_sip_udp.test.com
  - A entries—A:test.com

Example

```
ORACLE# clear-cache dns public A:test.com
```

clear-cache enum

This command allows you to clear a specified ENUM cache entry or all entries.

Syntax

```
clear-cache enum <EnumConfig Name | “all”> [cache entry key | “all”]
```

Arguments

- <EnumConfig Name> Enter the name of the specific EnumConfig for which you want to clear the cache
- <cache entry key> Enter the cache key of the specific EnumConfig for which you want to clear the cache
- <all> Enter all to clear all caches. In order for this command to work the DNS cache needs to be cleared.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# clear-cache enum enum1
```

clear-cache registration

The clear-cache registration command allows you to clear the registration cache for a specified protocol.

Syntax

```
clear-cache registration <sipd | h323d> <type>
```

Arguments

- <sip> Clear the SIP registration cache. The following are the types of information for which you can clear:
  - all
  - by-ip <IPaddress>
  - by-user <phone number>
  - expirted-contacts [all | by-aor <AOR>]
- <h323> Clear the H.323 registration cache. The following are the types of information for which you can query:
  - all
  - by-alias <terminalAlias>

Example

```
ORACLE# clear-cache registration sip all
```

clear-cache tls

This command allows you to clear the TLS cache.

Syntax

```
clear-cache tls
```

Example

```
ORACLE# clear-cache tls
```

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

clear-resourcemonitor-actions

Clear the cache of resource-monitor actions.

Syntax

```
clear-resourcemonitor-actions [ all | <RESOURCE> ]
```

Arguments

- <all> Clear the cache of all resource-monitor actions.
- <resource> Clear the cache of the resource-monitor actions for a specific resource.

Example

```
ORACLE# clear-resourcemonitor-actions all
```

clear-deny

The clear-deny command deletes a denied ACL entry.

Syntax

```
clear-deny [<index> | “all”]
```

Arguments

- <index> Enter the index number of the ACL entry to delete
- <“all”> Delete all denied ACL entries

Mode

Superuser

Example

```
ORACLE# clear-deny all
```

> **Note**
>
> Use the acl-show command to identify the index of a specific ACL entry. Use the clear-deny all command to delete all of the deny entries. This command replaces the acl-delete command from previous versions.

clear-sess

The clear-sess command deletes SIP, H.323, and IWF sessions from the system.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
clear-sess <sipd | h323d> <“sessions”> <all | by-agent | by-callid | by-ip |
by-user>
```

Arguments

- <all> Delete all sessions for the specified protocol
- <by-agent> Delete sessions for a specified session agent
- <by-callid> Delete sessions for a specified call identifier
- <by-ip> Delete sessions for a specified endpoint IP address (entered in quotation marks)
- <by-user> Delete sessions for a specified calling or called number

Mode

Superuser

Example

```
ORACLE# clear-sess sipd sessions all
```

> **Note**
>
> Use the show <sipd | h323d> sessions with similar arguments to view information about sessions you might want to clear from the system.

clear-trusted

The clear-trusted command deletes a trusted ACL entry.

Syntax

```
clear-trusted [<index> | “all”]
```

Arguments

<index> Enter the index number of ACL entry to delete

<“all”> Delete all trusted ACL entries

Mode

Superuser

Example

```
ORACLE# clear-trusted all
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use the acl-show command to identify the index of a specific ACL entry. Use the **clear-trusted all** command to delete all of the trusted entries.

cli

The cli command allows you to modify ACLI session terminal settings and “more” options on your Oracle Communications Session Border Controller.

Syntax

```
cli ["more" | "terminal-height"]
```

Arguments

more
Enable or disable the more prompt you see when the output on the screen is larger than the size of the screen.

- Values: enabled | disabled

terminal-height
Enter the number of rows in the terminal.

- Disable: 0
- Default: 24
- Range: 5 - 1000

Mode

User

Example

```
ORACLE# cli more disabled


ORACLE# cli terminal-height 500
```

configure terminal

The configure terminal command enters you into the system level where you can configure all operating and system elements on your Oracle Communications Session Border Controller.

Syntax

```
configure terminal
```

Arguments

configure terminal

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# configure terminal
```

control

The **control** command provides debug-level system access. Do not execute this command unless instructed by Oracle Engineering or Support.

Syntax

```
control
```

Mode

Debug

debug-disable

The **debug-disable** command removes access to the **shell**, **control**, and **lshell** commands.

Executing this command prompts you to enter the password you set when you executed the **debug-enable** command. After entering that password, access to the **shell**, **control**, and **lshell** commands is unavailable.

Syntax

```
debug-disable
```

Mode

Superuser

debug-enable

The **debug-enable** command is used to enable access to the **shell**, **control**, and **lshell** commands by setting a single password that provides authorization to executing them.

This command enables and sets the password used to access the **shell**, **control**, and **lshell** commands. Until debug password is set, you may not access the three debug commands.

To remove access to the three debug commands, use the **debug-disable** command. You will be prompted for the previously configured password you set by using **debug-enable**.

If you use the **debug-enable** command to set a debug password, and revert to a previous version of Oracle Communications Session Border Controller, the password set here is used to access the **shell** (or similar) command for earlier versions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
debug-enable
```

Mode

Superuser

delete realm-specifics

The delete realm-specifics command used with a realm identifier deletes the specified realm, and its configuration objects. This command should be used with the utmost care.

Syntax

```
delete realm-specifics <realm identifier>
```

Arguments

- <realm identifier>—Enter the identifier for the realm you want to delete

Mode

Superuser (in addition, you need to be in configuration mode)

Example

```
ORACLE(configure)# delete realm-specifics peer_1
```

> **Note**
>
> This command should be used with the utmost care.

delete-backup-config

The delete-backup-config command deletes a saved configuration file from the Oracle Communications Session Border Controller flash memory.

Syntax

```
delete-backup-config <backup-name>
```

Arguments

- <backup-name> - Enter the name of the backup configuration you want to delete

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE#delete-backup-config JAN_BACKUP.gz
```

> **Note**
>
> Use display-backups to list backup configurations to delete.

delete-boot-file

The **delete-boot-file** command deletes any system image file in the /boot directory.

Syntax

```
delete-boot-file <filename>
```

Arguments

<filename>
Enter the filename of the old boot file located in the /boot directory.

Mode

Superuser

Example

```
ORACLE# delete-boot-file nnSCZ840p1.bz
Verifying signature of /boot/nnSCZ840p1.bz
Version: Acme Packet SCZ8.4.0 Patch 1 (Build 91) 202006281454

Image integrity verification passed

Successfully deleted /boot/nnSCZ840p1.bz

ORACLE#
```

delete-config

The delete-config command deletes the current configuration located in the /code/data and /code/config directories from the system's flash memory.

Syntax

```
delete-config [cached]
```

Arguments

- [cached] Delete the cached configuration. This is an optional argument.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# delete-config
```

> **Note**
>
> When the delete-config command is entered, the system gives the warning asking if you really want to erase either the current config or the current cached config. Enter a y to complete the deletion.

delete-crashfiles

Deletes all crash files in /opt/crash.

Syntax

```
delete-crashfiles [older-than <days>]
```

Arguments

older-than—Specify if you want all crashfiles older than an indicated age, in days, to be deleted.

Mode

Superuser

Example

```
ORACLE# delete-crashfiles 100
```

> **Note**
>
> This command presents you with an Are you sure prompt.

delete-import

This command enables the user to delete imported SIP-manipulation rules as files from the /code/import directory.

Syntax

```
delete-import <file name>
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

- <file name> - The name of the SIP manipulation rules file to delete

Mode

Superuser

Example

```
ORACLE# delete-import 12012009.gz
```

> **Note**
>
> Include the complete file name in the argument, including .gz.

delete-logfiles

Deletes all closed log files in /opt/logs.

Syntax

```
delete-logfiles [older-than <days>]
```

Arguments

older-than—Specify if you want all log files older than an indicated age, in days, to be deleted.

Mode

Superuser

Example

```
ORACLE# delete-logfiles 100
```

> **Note**
>
> This command presents you with an Are you sure prompt.

delete-status-file

The delete-status-file deletes the reboot status file.

Syntax

```
delete-status-file
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

none

Mode

Superuser

Example

```
ORACLE# delete-status-file
```

> **Note**
>
> This command deletes the /code/statsDump.dat file which retains all system data if the Oracle Communications Session Border Controller has to reboot. This command also removes the contents of the /code/taskCheckDump.dat file which contains system failure information.

display-alarms

The display-alarms command displays details about the specific alarms on the Oracle Communications Session Border Controller.

Syntax

```
display-alarms
```

Arguments

none

Mode

User

Example

```
ORACLE# display-alarms
```

> **Note**
>
> This command shows the current alarms on the Oracle Communications Session Border Controller. Each alarm entry lists alarm ID, task ID, alarm severity code, number of occurrences, when the alarm first and last occurred, the number of times it has occurred, and a description of the alarm.

Copyright © 2024, 2026, Oracle and/or its affiliates.

display-backups

The display-backups command displays the configuration backup files located in the /code/bkups directory.

Syntax

```
display-backups [sort-by-name]
```

Arguments

- <sort-by-name> - Sort the output of the display-backups command output. This is an optional command.

Mode

User

Example

```
ORACLE# display-backups
```

display-current-cfg-version

The display-current-cfg-version command displays the current configuration version.

Syntax

```
display-current-cfg-version
```

Arguments

none

Mode

User

Example

```
ORACLE# display-current-cfg-version
```

> **Note**
>
> This command displays the saved version number of the current configuration. This integer value is incremented by one for each new configuration version.

display-logfiles

The display-logfiles command lists the current logfiles located in the `/code/logs` directory.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
display-logfiles
```

Arguments

none

Mode

User

Example

```
ORACLE# display-logfiles
```

display-running-cfg-version

The display-running-cfg-version command displays the current configuration version.

Syntax

```
display-running-cfg-version
```

Arguments

none

Mode

User

Example

```
ORACLE# display-running-cfg-version
```

> **Note**
>
> This command displays the version number of the running configuration, an integer value that is incremented by one for each new configuration version.

dump_csv_format

The **dump_csv_format** command changes the system mode from generating local CDR files to generating files that specify CSV organization. You would use this file to create a template from which you can interpret all the data in your CSV files. The system writes these format files to the same directory as local CDR files using the same naming convention as local CDR files.

Copyright © 2024, 2026, Oracle and/or its affiliates.

While this command is activated, the system produces layout files instead of actual CDRs. After the layout files have been created, turn the generation feature off with the **no_dump_csv_format** command.

Syntax

```
dump_csv_format
no_dump_csv_format
```

Arguments

none

Mode

User

Example

```
ORACLE#dump_csv_format
ORACLE#no_dump_csv_format
```

dump_diam_dict

The **dump_diam_dict** command creates the file /opt/logs/OracleSBCRf.xml, which you can use to decode Oracle-specific Rf AVPs in messages using Wireshark. After creating the file, you install it and establish it as a reference within the Wireshark resource file named 'diameter'.

Syntax

```
dump_diam_dict
```

Arguments

none

Mode

User

Example

```
ORACLE#dump_diam_dict
```

enable

The enable command changes the current ACLI session from User mode to Superuser mode.

Syntax

```
enable
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

none

Mode

User

Example

> **Note**
>
> Observing the command prompt can tell you if the Oracle Communications Session Border Controller is in user or superuser mode. A ">" (close-angle-bracket) indicates User mode and a "#" (pound) sign indicates Superuser mode.

```
ORACLE> enable
ORACLE#
```

exit

The exit command exits from the current command shell or configuration subsystem to the next higher level.

Syntax

```
exit
```

Arguments

none

Mode

User

Example

```
ORACLE# exit
```

format

This command allows the user to partition the Storage Expansion Module into as many as 4 file directories.

Syntax

```
format <device>
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

- <device> - Enter the name of a device

Mode

Superuser

Example

```
ORACLE# format device1
```

generate-certificate-request

For TLS Support, the generate-certificate-request command allows you to generate a private key and a certificate request in the PKCS10 PEM format. The generated private key is stored in the certificate record configuration. If the certificate record is designed to hold a CA certificate, there is no need to generate a certificate request.

Syntax

```
generate-certificate-request <certificate-record-name>
```

Arguments

- <certificate-record-name> - Enter the name of the certificate you want to view.

Mode

Superuser

Example

```
ORACLE# generate-certificate-request acmepacket
```

generate-key

The generate-key command allows you to generate a security key.

Syntax

```
generate-key <type>
```

Arguments

- <type> - Select the type of key you want to generate. The following is a list of valid security keys.
- Values:
  - 3des— Generate a 3DES 192 bit, odd parity key
  - aes-128— Generate an AES 128 bit key
  - aes-256— Generate an AES 256 bit key

Copyright © 2024, 2026, Oracle and/or its affiliates.

- hmac-md5— Generate an HMAC MD5 secret
- hmac-sha1— Generate an HMAC SHA1 secret
- hmac-sha-256— Generate an HMAC SHA-256 secret
- hmac-sha-384— Generate an HMAC SHA-384 secret
- hmac-sha-512— Generate an HMAC SHA-512 secret

Mode

Superuser

Example 2-1 Example

```
ORACLE# generate-key aes-256
```

global-trusted-ca

The **global-trusted-ca** command creates individual global trusted root CA stores that you can apply to one or more tls-profiles. You can also use this command to import certificates directly to new global trusted root CA stores, and generate reports on the contents of these stores.

Syntax

The syntax for **global-trusted-ca** follows.

```
ORACLE# global-trusted-ca [ca-bundle add <all(default):
list (comma separated list of Organization Names) | show [list-brief : list-
detail] ]
 | [import-X509 <certificate-record name>] <global-trusted-ca name>
```

Arguments

<ca-bundle>—Specifies how to create or display your local global-trusted-ca.

- ca-bundle
  - add—Arguments include:
    - <all> (default)—Creates global-trusted-ca using all the valid certificates in the ca-bundle.crt file. You specify a name to create a new global-trusted-ca with the entire list.
    - <list of organization names>—Specifies all the certificates in the ca-bundle.crt file associated with the one or more organization name listed in the command. Create certificate-record for only the certificates with respect to the organization names using a comma separated list of Organization Name
    - global-trusted-ca name—Specifies the name of your new global trusted root CA.
  - show—Additional required arguments include:
    - <list-brief>—Lists all of the Organization Names that are responsible for issuing and managing CA certificates available in the certificate bundle installed on your system.
    - <list-detail> Organization Name—Lists all of the certificates, with details, within the crt-bundle.crt that apply to the Organization Name you specify and are installed on your system.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Both the show argument's list-brief and list-detail arguments do not require admin rights.

- import-X509—Allows you to simultaneously import a new certificate and add that certificate to a new global-trusted-ca. The system names this new global-trusted-ca using the name you provide, or displays an error if that global-trusted-ca name already exists. When you initiate the command, the system tells you to enter the certificate in the PEM format, then terminate your entry with a semi-colon ";". Arguments include:
  - certificate-record name—Specifies the certificate-record name to which you are importing.
  - global-trusted-ca—Specifies the name of your new or existing global trusted root CA.

Mode

Superuser

Example

```
ORACLE# trusted-root-ca ca-bundle add all MyCAList2
```

halt

The **halt** command prepares the platform for a clean system shutdown. This is similar to the **reboot** command, except the halt command does not explicitly reboot the system. The halt command (like the reboot command) may accept a force argument i.e. halt the system regardless of whether it would cause a service outage. The **sysprep** and **exit** arguments should only be used under Oracle direction.

Syntax

```
halt [force | sysprep | exit]
```

Arguments

force—Force the box halt regardless of current state.

sysprep—This command can only be run when in debug mode, and should only be used under Oracle direction.

exit—This command can only be run when in debug mode, and should only be used under Oracle direction.

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

import-certificate

For TLS support, the import-certificate command allows you to import a certificate record.

Syntax

```
import-certificate <type>
```

Arguments

- <type> - Enter the type of certificate you want to import.
- Values
  - pkcs7—Import using a password enhanced mail format
  - x509—Import using a password enhanced mail format
  - try-all—Try importing from both pkcs7 and x509

Mode

Superuser

Example

```
ORACLE# import-certificate x509
```

interface-mapping

The interface-mapping command manages interfaces via MAC address to Oracle Communications Session Border Controller physical interface configuration name mapping. The element includes configuration and management controls. This element is applicable only to COTs and VM deployments; the software recognizes hardware platform during installation and makes the interface-mapping command available only with applicable platforms.

Parameters

show
Allows the user to display a table that shows the current mapping between interface MAC addresses and physical interface configuration names. The output of this command is the same as the show interface-mapping command.

locate <ethernet if name> <seconds>
Allows the user to cause the system to blink the LEDs associated with the specified ethernet interface name for the specified number of seconds. This command allows the user to physically identify an interface based on its interface name. This command is not applicable to virtual machine deployments.

label <ethernet if name> <labeling text>
Allows the user to specify a label used in the mapping table displayed using the interface-mapping show command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

delete <ethernet if name>
Allows the user to remove the specified mapping from the interface-mapping show table. The user cannot use a deleted interface within the Oracle Communications Session Border Controller's configuration.

swap <ethernet if name1> <ethernet if name2>
Allows the user to change the current interface mapping by swapping the specified interface names between each other.

Path

interface-mapping is a command (and branch) at the root path, and is only visible on COTS and VM platform deployments.

local-accounts

Use the local-accounts command to create, modify, or delete local accounts.

Syntax

```
local-accounts add <user> <class> [<authtype>]
local-accounts change-password <user>
local-accounts delete <user>
local-accounts reset <user>
```

Arguments

add <user> <class> [<authtype>]
Create an account specified by a unique username and user class. The **<class>** parameter must be either **user** or **admin**.
The **<authtype>** parameter is valid only with **add**. The supported values are **passwd** and **MFFE**. If omitted, the value defaults to **passwd**. MFFE accounts are supported when you have configured certificate-based authentication, and are created without prompting for a password. You cannot change the authentication type on an existing account; delete and recreate the account to use a different authentication type.

change-password <user>
Change the password of the specified user.
The admin must know the current password for the specified user.

This argument is not valid for accounts with the **MFFE** authentication type.

delete <user>
Delete a specified user.

reset <user>
Reset a user's password by creating a temporary, one-time password for that user.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> After a password reset, the Oracle Communications Session Border Controller (SBC) forces users to choose a new password the next time they login. Users must always create this new password within the CLI. Once users have updated their password in the CLI, they are able to login using the WebGUI.

This argument is not valid for accounts with the **MFFE** authentication type.

Mode

Superuser

Example

```
ORACLE# local-accounts add jamie admin
```

log-level

The log-level command sets the system wide log-level or the log-level for a specific task or process. In addition, you can set the log type for a specific log level on a per-task basis.

Syntax

```
log-level <task-name | all> <log-level>
```

Arguments

<task-name>: Enter the name of the specific task for which you want to set. Use 'all' to set the log level for all tasks or 'system' to set it system-wide.

<log-level>: Select the log level either by name or by number:

- emergency (1)
- critical (2)
- major (3)
- minor (4)
- warning (5)
- notice (6)
- info (7)
- trace (8)
- debug (9)
- detail (10)

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> The log setting changes made by the **log-level** command do not persist after a reboot. You must change the log settings in the system configuration for them to persist after a reboot. When entering multiple log types in the log-type-list argument, use a space for separation.

Exceptions

You cannot change the log level for the following tasks with the **log-level** command; it is set once when they are created at startup:

- authqueue
- fragHandler
- heap
- healthCheckd
- SSHD
- tLFMiBd

To set the log level for the preceding tasks, use **system-log-level** and **process-log-level** in **system-config**.

> **Note**
>
> Although in most cases **system-log-level** and **process-log-level** are RTC-enabled, for the preceding tasks, you must reboot the system for the changes to take affect.

Example

```
ORACLE# log-level system warning
```

lshell

The **lshell** command provides debug-level system access. Do not execute this command unless instructed by Oracle Engineering or Support.

Syntax

```
lshell
```

Mode

Debug

monitor

The monitor command displays real-time media or signaling statistics.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
monitor <media | session>
```

Arguments

- <media> - Enter the media you want to monitor
- <session> - Enter the session you want to monitor

Mode

User

Example

> **Note**
>
> This command outputs real-time media and signaling statistics to the ACLI. Pressing a numerical digit (0-9) changes the refresh rate to that interval in seconds. By default, there is a 2 second refresh rate. Type "q" to exit the monitor display. Monitor session will display the equivalent of show sipd statistics, and monitor media will display the equivalent of show mbcd statistics.

```
ORACLE# monitor media
```

mount

The mount command starts the file system. Mounting the file system is required to bring the storage device volumes back online after they have been unmounted.

Syntax

```
mount <data-disk | system-disk | hard-disk>
```

Arguments

data-disk— Mount the 1 or more data partitions containing the default (/mnt/sys and /mnt/app) or user-defined volumes

system-disk—Mount 2 system partitions: /opt and /opt/crash

hard-disk—Mounts both the system partition and data partition

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

3
ACLI Commands N-Z

notify

The notify command notifies a specific task or process of a condition that it should act. Used for runtime protocol tracing for UDP/TCP sockets, this command provides for all protocol messages for ServiceSocket sockets to be written to a log file or sent out of the Oracle Communications Session Border Controller to a UDP port.

Syntax

```
notify <all | <process-name>> trace <all|<socket-address><file-name>> [<out-
udp-port>]
notify <all | <process-name>> notrace all|<socket-address>
```

Arguments

- <process-name> - Enter the name of the process you want to notify
- <socket-address> - Enter the IP address and the port on which the socket is connected
- <file-name> - Enter the name of the file you want to notify
- <out-udp-port> - Enter the IP address and port to which the log messages are sent; if the<out-udp-port> is not specified, logs are written to the <file-name>

```
ORACLE# notify all trace all aug.gz
```

notify algd

Syntax

```
notify algd <log>
```

Arguments

<log> - Each log argument is listed and described below.

- Values:
  - nolog — Disable MBCD and MGCP message exchanges processed by the ALGD task
  - log — Enable ALGD and MGCP messages in the alg.log

Example 3-1 Example

```
ORACLE# notify algd log
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

notify algd mgcp-endpoint

Syntax

```
notify algd mgcp-endpoint <endpoint>
```

Arguments

- <endpoint> - Delete session and corresponding gateway entries for a specified gateway. The value is the endpoint name from the Audit Name field of the RSIP. If a gateway has multiple endpoints, then the last endpoint that sent the RSIP should be used as the endpoint ID.

Example 3-2 Example

ORACLE# notify algd mgcp-endpoint 1.2.0.1

notify berpd force

Force a manual switchover between Oracle Communications Session Border Controllers in an HA node, regardless of the Oracle Communications Session Border Controller on which the command is executed.

Syntax

```
notify berpd force
```

Example 3-3 Example

ORACLE# notify berpd force

notify mbcd

Syntax

```
notify mbcd <arguments>
```

Arguments

- <arguments> The following are arguments for this command:
- Values:
  - nolog—Disable MBCD logging
  - log—Enable MBCD logging
  - debug—Set the log level for MBCD. Unless a specific log type is specified, this command will use its defaults: FLOW and Media
  - nodebug —Disable setting the log level for MBCD

Example 3-4 Example

```
ORACLE# notify mbcd debug
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

notify radd reload

Changes the configurations for RADIUS dynamically by reloading the configuration data in the accounting configuration.

Syntax

```
notify radd reload
```

Example 3-5 Example

```
ORACLE# notify radd reload
```

notify sipd

Syntax

```
notify sipd <arguments>
```

Arguments

- <arguments> - The following are arguments for this command:
- Values:
  - reload—Update configuration changes dynamically by reloading the configuration data that SIP functionality might need. This command cannot tear down any in-progress sessions, and it cannot tear down any listening sockets.
  - nosiplog—Disable the logging of SIP messages, including SIP messages as seen from the perspective of the Oracle Communications Session Border Controller's SIP proxy
  - siplog—Enable SIP logging messages in the sipmsg.log
  - report—Write all SIP process statistics to the log file
  - dump limit—Write CPU limit information to the log file
  - debug—Set log level for SIP protocol for some SIP activity
  - nodebug —Disable setting the log level for the SIP protocol for some SIP activity

Example 3-6 Example

```
ORACLE# notify sipd nosiplog
```

notify syslog

Syntax

```
notify syslog <arguments>
```

Arguments

- <arguments> - Arguments for this command

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values:
  - ip-address—Add a syslog server with the given IP address to the configured syslog servers. When this command is executed without any arguments, the Oracle Communications Session Border Controller is prompted to re-read the current configuration, replace any pre-existing configuration information for syslog, and begin sending syslog messages to any configured syslog servers.
  - udplog
  - noudplog
  - trace
  - notrace

Example

```
ORACLE# notify syslog 100.1.0.20
```

notify rotate-logs

Syntax

```
notify <task> rotate-logs
```

Arguments

<task> Enter the tasks' process and protocol trace logs to rotate

- Values:
  - sipd
  - sysmand
  - berpd
  - brokerd
  - lemd
  - mbcd
  - h323d
  - algd
  - radd
  - all

> **Note**
>
> This command only applies until a reboot occurs; it is not persistent after a reboot.

Example

```
ORACLE
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

notify nosyslog

Syntax

```
notify nosyslog <ipaddress>
```

Arguments

- <ipaddress> - Enter the IP address of syslog server to disable the logging of syslog messages. The notify nosyslog command executed without an argument prompts the Oracle Communications Session Border Controller to disable the logging of syslog messages sent from the system to all syslog destinations.

Mode

Superuser

Release

First appearance: 1.0 / Most recent update: 1.1

Example

```
ORACLE# notify nosyslog 100.1.20.30
```

package-crashfiles

Create a tar archive of crash files in `/opt/crash` called `crashes-<date>.tar.gz`. In addition to crash files, this command also creates output files created when you execute the **package-logfiles** command.

Syntax

```
package-crashfiles [name <file>.tar.gz] [newer-than <days>] <all>
```

Arguments

name—Specify the path and name of the saved file. Generally, the files should be saved to /opt. If the system's hard drive has been formatted with partitions, /mnt may be used instead.

newer-than—Specify a time limit, in days, on the crash files to be compressed and saved. This option counts backwards, starting with the current day. Thus the option newer-than 5 would compress and save crash files for the past 5 days only.

all—Collects all formed crash files and available log files. Use this argument with caution as it may impact system performance.

Mode

Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

package-logfiles

Create a tar archive of log files in `/opt/logs`, backup configuration, and the `support-info.log` file to `logs-<date>.tar.gz`.

Syntax

```
package-logfiles [name <file>.tar.gz] [newer-than <days>] <all>
```

Arguments

name—Specify the path and name of the saved file. Generally, the files should be saved to /opt. If the system's hard drive has been formatted with partitions, /mnt may be used instead.

newer-than— Specify a time limit, in days, on the log files to be compressed and saved. This option counts backwards, starting with the current day. Thus the option newer-than 5 would compress and save log files for the past 5 days only.

all—Collect the np-stats info, support-info.log, running configuration, and log files. Use this argument with caution as it may impact system performance.

> **Note**
>
> If there are a large number of log files, the CPU core that is processing the package-logfile command may show higher load and an alarm. This does not have impact on the system and the system clears the alarm after the process automatically.

Mode

Superuser

packet-trace

The **packet-trace** command starts or stops packet tracing on the Oracle Communications Session Border Controller. The system can save packet tracing results locally or mirror traffic to another device. The syntax differs slightly between platforms that operate over the DPDK datapath. The software recognizes the platform on which it is installed, and only supports the syntax applicable to that platform.

When the user starts a local trace, the Oracle Communications Session Border Controller stores the packets it captures in a PCAP file. Syntax initiating local packet trace can include pcap_filter syntax, enclosed in quotes, to refine and limit the data to capture on the Oracle Communications Session Border Controller.

When the user starts a remote trace, the Oracle Communications Session Border Controller encapsulates the packets it captures, per RFC 2003, and sends them to a user-configured **capture-receiver**. Syntax initiating remote packet trace includes specifying the endpoint, identified by the IP address, that sent or received the traffic and the Oracle Communications Session Border Controller network interface on which to capture traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

The syntax for packet tracing follows.

```
packet-trace <local|remote> [start|stop] [all] [interface name] [capture-
filter] [ip-address] [local-port] [remote-port]
```

To simplify, the syntax below separates arguments for **packet-trace remote**, **packet-trace local** and platform-based syntax. The syntax for remote packet tracing follows.

```
packet-trace remote <start|stop> <interface name> <ip-address> [local-port]
[remote-port]
```

The syntax for local packet tracing on hardware datapath platforms follows.

```
packet-trace local <interface name> ["capture-filter"]
```

The syntax for local packet tracing on DPDK datapath platforms follows.

```
packet-trace local start <interface name> ["capture-filter"]
```

Arguments

<remote | local> - Specifies the type of trace to run. Note that software-only deployments support only **packet-trace local**.

Remote packet trace supports IPv6 addresses in addition to IPv4. Furthermore, remote packet trace is capable of capturing IPv4 traffic when configured with an IPv6 address and vice-versa. IPv6 Remote packet trace is also capable of decoding TCP handshake traces for MSRP and MSRP traffic.

[capture filter] - Only applicable to local packet tracing. Configure a filter in **pcap_filter** syntax.

[start | stop] - Applicable to remote packet tracing and local packet tracing on DPDK platforms. Start remote packet tracing on the Oracle Communications Session Border Controller. The start argument does not apply to local packet-trace on platforms that do not use the DPDK datapath.

- network-interface—The name of the network interface on the Oracle Communications Session Border Controller from which you want to trace packets; this value can be entered as either a name alone or as a name and subport identifier value (name:subportid)
- ip-address—IP address of the endpoint to and from which the Oracle Communications Session Border Controller will mirror calls
- local-port—Layer 4 port number on which the Oracle Communications Session Border Controller receives and from which it sends. This is an optional parameter; if no port is specified or if it is set to 0, then all ports will be traced.
- remote-port—Layer 4 port to which the Oracle Communications Session Border Controller sends and from which it receives. This is an optional parameter; if no port is specified or if it is set to 0, then all ports are traced.

<stop> - Only applicable to remote packet tracing. Manually stop packet tracing on the Oracle Communications Session Border Controller. With this command you can either stop an

Copyright © 2024, 2026, Oracle and/or its affiliates.

individual packet trace or all packet traces that the Oracle Communications Session Border Controller is currently conducting.

- all—Stops all remote traces currently operating on the system. The **all** argument does not require further arguments.
- network-interface—The name of the network interface on the Oracle Communications Session Border Controller from which you want to stop packet tracing. This value can be entered either as a name alone or as a name and subport identifier value (name:subportid).
- ip-address—IP address of the endpoint to and from which you want the Oracle Communications Session Border Controller to stop mirroring calls.
- local-port—Layer 4 port number on which to stop from receiving and sending. This is an optional parameter; if no port is specified or if it is set to 0, then all port tracing will be stopped.
- remote-port—Layer 4 port number on which to stop the Oracle Communications Session Border Controller from receiving and sending. This is an optional parameter; if no port is specified or if it is set to 0, then all port tracing will be stopped.

Mode

Superuser

Example

```
ORACLE# packet-trace remote start public:0 111.0.12.5 5060 5060
```

> **Warning**
>
> Do not run packet-trace simultaneously with other SBC replication features. See Monitor Warning for a complete list of which replication features can conflict with each other.

ping

The ping command pings a remote IP address.

Syntax

```
ping <ip-address> [if-name:vlan] [source-ip]
```

Arguments

<ip-address> - Enter the IP address of host to ping

<if-name:vlan> - Enter the network interface and vlan that the system must use to send out the ping. The system uses vlan 0 if unspecified. This is an optional argument.

<source-ip> - Enter the source IP address to use. This is an optional argument.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This command sends ICMP echo messages, and displays:
>
> - minimum round trip time (RTT)
> - maximum RTT
> - average RTT
> - number of packets transmitted
> - number of packets received
> - percentage of packets lost
>
> The default ping timeout is 64ms.

> **Note**
>
> The system does not allow you to ping from a secondary SBC media interface, presenting a warning if you try. This prevents you from creating conflicts in the resolution of your interfaces in neighboring switches.

Mode

Superuser

Example

```
ORACLE# ping 100.20.11.30
```

prompt-enabled

The Oracle Communications Session Border Controller lets you know if a configuration has been changed and you've applied the done command, but have not saved and activated yet. When you issue the done command and return to Superuser mode, the ACLI prompt prefixes two asterisks (**). When you have saved, but not yet activated, the ACLI prompt prefixes one asterisk (*).

The prompt-enabled command allows you to decide whether or not you want the Oracle Communications Session Border Controller to give you this prompt. When this command is entered without an argument, the Oracle Communications Session Border Controller displays the current setting of the prompt.

Syntax

```
prompt-enabled <enabled | disabled>
```

Arguments

enabled - Enable the prompt-enabled feature

disabled - Disable the prompt-enabled feature

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# prompt-enabled disabled
```

realm-specifics

The realm-specifics command displays all configuration elements that have a specified realm ID configured.

Syntax

```
realm-specifics <realm-ID>
```

Arguments

<realm-ID> Enter the name of realm

Mode

User

Example

```
ORACLE# realm-specifics test1
```

> **Note**
>
> If a specified realm-ID appears as a configuration parameter in any configuration element, that full element is displayed on the screen. The realm-specifics command acts as a “grep” command for a realm name that appears in any configuration element.

reboot

The reboot command reboots the Oracle Communications Session Border Controller.

Syntax

```
reboot <arguments>
```

Arguments

<arguments> The following are arguments for this command:

- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- force—Reboot the Oracle Communications Session Border Controller system using the last running configuration. The confirmation prompt is bypassed when using this command.
- activate—Reboot the Oracle Communications Session Border Controller system using the last-saved configuration. You are presented with a confirmation prompt when using this command.
- fast—Reboot the Oracle Communications Session Border Controller system using the last-saved configuration. This reboot skips BIOS processes, making the reboot faster. This argument is relevant only to COTS deployments. Issuing the command on Virtual Machine deployments or proprietary Oracle Communications Session Border Controller hardware does not make the reboot faster. You are presented with a confirmation prompt when using this command.
- no argument—Reboot the Oracle Communications Session Border Controller system using the last running configuration

Mode

Superuser

Example

```
ORACLE# reboot activate
```

request audit

The request audit command allows you to request the audit of a specified endpoint for SIP or H.323.

Syntax

```
request audit <registration>
```

Arguments

<registration> Select SIP or H.323 registration

Mode

Superuser

Example

```
ORACLE# request audit SIP
```

request collection

The request collection command allows you to start and stop data collection manually in one or all collection groups.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
request collection [start | stop | restart | status | purge] <collection
object>
```

- start— Start data collection. If a collection object is not specified, collection is performed on all groups.
- stop— Stop data collection. If a collection object is not specified, collection stop is performed on all groups
- restart— Restart data collection in general or for the collection object specified
- purge— Delete all data files resident on the Oracle Communications Session Border Controller for collection function
- status— displays the current status of all record collections and push receivers

<collection-object> — The collection groups you can configure to collect data information from. This is an optional argument and when no group is specified, the Oracle Communications Session Border Controller collects information from all groups. The following is a list of collection groups:

- Values :
  - dnsalg-rate - DNS-ALG rate
  - dnsalg-rate-per-addr - DNS-ALG rate per addr
  - dnsalg-rate-per-realm - DNS-ALG rate per realm
  - enum-rate - ENUM rate
  - enum-rate-per-addr - ENUM rate per addr
  - enum-rate-per-name - Request action in the ENUM rate per name
  - enum-stats - ENUM stats
  - ext-rx-policy-server - external Rx Policy Server group
  - fan - fan group
  - h323-stats - H323 Statistics group
  - interface - interface group
  - msrp-stats: MSRP statistics
  - network-util - network utilization group
  - registration-realm - registration realm group
  - sa-imsaka - Request action on Security Associations for IMS-AKA group. Only Supported for Enterprise Products.
  - sa-srtp - Request action on Security Associations for SRTP group
  - session-agent - session agent group
  - session-realm - session realm group
  - sip-ACL-oper - SIP ACL Operations group
  - sip-ACL-status - SIP ACL Status group
  - sip-agent-method - SIP methods on the session agent

Copyright © 2024, 2026, Oracle and/or its affiliates.

- sip-client - SIP Client Transaction group
- sip-codec-per-realm - SIP codecs per realm group
- sip-errors - SIP Errors/Events group
- sip-interface-method - SIP methods on the interface
- sip-invites - SIP Invites
- sip-method - SIP methods
- sip-policy - SIP Policy/Routing group
- sip-rate - SIP rate
- sip-rate-per-agent - SIP rate per agent
- sip-rate-per-inf - SIP rate per interface
- sip-realm-method - SIP methods on the realm
- sip-server - SIP Server Transaction group
- sip-sessions - SIP Session Status group
- sip-srvcc - SIP SRVCC group. Only Supported for Enterprise Products.
- sip-status - SIP Status group
- sobjects - sobjects group
- space - space group
- survivability-sip-errors - Survivability SIP Errors/Events group. Only Supported for Enterprise Products.
- survivability-sip-invites - Survivability SIP Invites. Only Supported for Enterprise Products.
- survivability-sip-registration - Survivability SIP Registrations. Only Supported for Enterprise Products.
- survivability-sip-status - Survivability SIP Status group. Only Supported for Enterprise Products.
- system - system group
- temperature - temperature group
- thread-event - thread event group
- thread-usage - thread usage group
- voltage - voltage group
- xcode-codec-util - Transcoding Codec Utilization group
- xcode-session-gen-info - general info about transcoding sessions
- xcode-tcm-util - Transcoding TCM Utilization group

Mode

Superuser

reset

The reset command resets statistic counters.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
reset <statistic>
```

Arguments

<statistic> The following is a list of specific statistics which you can tell the Oracle Communications Session Border Controller to reset:

- algd — Reset algd-related statistics shown in the show algd command.
- all — Reset the statistics shown in the following commands: show sipd, show mbcd, show algd, show mbcd redundancy, show algd redundancy, show sipd redundancy, show redundancy mbcd, show redundancy algd, show redundancy, show memory.
- application — Reset the application statistics shown in the show application command.
- auth—Reset statistics related to authorization (RADIUS or DIAMETER) processes.
- bfd—Reset statistics being collected on BFD sessions.
- dns — Reset DNS statistics.
- ebmd — Reset EMBD (External Band Manager Daemon) statistics.
- enum — Reset ENUM statistics.
- h323d — Reset the h323-related signaling statistics.
- lrt — Reset Local Routing statistics.
- mbcd — Reset mbcd-related statistics shown in the show mbcd command (except statistics related to high availability).
- net-management-control — Reset Network Management Control statistics.
- nsep-stats — Reset counters for NSEP-related statistics; to reset counters for a specific r-value, add the specific r-value to the end of the command.
- radd — Reset accounting (RADIUS or DIAMETER accounting connection) statistics.
- redundancy — Resets redundancy statistics for most tasks that implement redundancy including lifetime values that are not reset after a switchover. Exceptions include the sipd redundancy object statistics and the sipd queue command statistics.
- security-associations — Reset Security Association statistics.
- session-agent <hostname> — Reset statistics for a specified session agent.
- sipd — Reset sipd statistics in the show sipd command.
- snmp-community-table — Reset the counters on SNMP community table statistic.
- snmp-stats—Reset the SNMPv3 statistics associated with SNMPv3 entries, which includes entries made using the **snmp-user-entry** and **snmp-address-entry** commands.
- spl <filename> — reloads the supplied filename.
- stir — Reset statistics for STIR servers.
- tacacs-stats — Reset the TACACS+ statistics
- trap-receiver — Reset the counters for trap receiver statistics.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This command is used to clear existing SIP, MBCD, ALGD, high availability, and application statistics and to reset the values for one or all of these statistics to zero. Executing the reset command sets the period and lifetime statistics totals to zero, but the active statistics counts are still retained.

Mode

Superuser

restore-backup-config

The restore-backup-config command restores a named backup configuration.

Syntax

```
restore-backup-config <config-name> [saved | running]
```

Arguments

<config-name> Enter the name of backup configuration to restore<saved> Restore the configuration to the last saved configuration. This is an optional argument.<running> Restore the configuration to the last running configuration. This is an optional argument.

Mode

Superuser

> **Note**
>
> After running the restore-backup-config command, you must reboot your system because some of the configurations are not RTC.

> **Note**
>
> Use the display-backups command to view the backups that are available to be restored.

Example

```
ORACLE# restore-backup-config FEB_07.gz saved
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

run configuration-assistant

Use the `run configuration-assistant` command to launch the Configuration Assistant. After you launching, the Configuration Assistant requests your input to set up the initial configuration for your deployment.

Syntax

```
run configuration-assistant
```

Mode

Superuser

```
<prompt> # run configuration-assistant

Thank you for purchasing the Oracle Enterprise Session Border Controller.
The following Configuration Assistant guides you through the initial
configuration
and restarts the system.
------------------------------------------------------------------------------
------
List of deployments
1. MSTeams
Enter '1' to choose Microsoft Teams v1.1 [MSTeams.gz].
Enter '1?' to get description of Microsoft Teams v1.1 [MSTeams.gz].
Please select a deployment (Enter 'q' to exit):
```

save-config

The save-config command saves the current configuration to the Oracle Communications Session Border Controller's last-saved configuration, stored in flash memory.

Syntax

```
save-config <type>
```

Arguments

<type> Chooses the file format for the internal configuration file.

- Values:
  - standard—Use standard XML as the file format
  - non-standard—Use non-standard, legacy XML for the file format

> **Note**
>
> When this command is executed and resources are sufficient, the Oracle Communications Session Border Controller notifies you that the configuration has been saved successfully and the current configuration number will be incremented by one.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# save-config
```

secret

The secret command sets the User and Superuser passwords.

Syntax

```
secret <user level>
```

Arguments

<user level> Each user level argument is listed and explained below.

- Values:
  - login—Set the SBC's user password
  - enable—Set the SBC's superuser password
  - backup—Set the backup password
  - config—Set the configuration password

> **Note**
>
> The ACLI does not echo the password you enter. You will be prompted to enter the new password twice. The complexity requirements display on the screen.

> **Note**
>
> For security purposes, please use different passwords for the user and superuser accounts.

Mode

Superuser

Example

```
ORACLE# secret login
```

set-system-state

The set-system-state command sets the Oracle Communications Session Border Controller as either online or offline.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
set-system-state <state>
```

Arguments

<state> Select the system state

- Values :
  - online—Enable online system state
  - offline—Enable offline system state

> **Note**
>
> The offline setting puts the Oracle Communications Session Border Controller into a state where it is powered on and available for administrative purposes, but does not accept calls. Existing calls in progress are not affected.

Mode

Superuser

Example

```
ORACLE# set-system-state online
```

set-boot-file

The set-boot-file /boot/<filename> command allows you to change the image running on the SBC.

Syntax

```
set-boot-file /boot/<filename>.bz
```

Argument

<filename> Specify the name of the image file you want to run.

Mode

Superuser

Example

```
ORACLE# set-boot-file /boot/12-1-19.bz
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

set-boot-loader

The **set-boot-loader** command copies the supplied filename to `/boot/bootloader`. Invalid bootloaders that fail the integrity check are not copied but return an error message.

Syntax

```
set-boot-loader <filename-path>
```

Arguments

<filename-path>
Enter the full path to the new bootloader.

Mode

Superuser

Example

```
ORACLE# set-boot-loader /code/images/nnSCZ840p4.boot
Verifying signature of /code/images/nnSCZ840p4.boot
Version: Acme Packet SCZ8.4.0 Patch 4 (Build 219) 202001050218

Image integrity verification passed

Successfully copied /code/images/nnSCZ840p4.boot to /boot/bootloader
ORACLE#
```

setup entitlements

The setup entitlements command is used to self configure entitlements for the product you chose in the setup product command. By executing this command, you will be faced with a list of valid entitlements for the product-platform-software combination you are currently running. You can select entitlements to enable or provision capacity based entitlements from this command.

Syntax

```
setup entitlements
```

Mode

Superuser

setup product

The setup product command is used to assign a product type to this instance of software and hardware combination. By executing this command, you will be faced with a list of valid

Copyright © 2024, 2026, Oracle and/or its affiliates.

products, based on platform, that you may provision this system as. Choose the appropriate product and hit the <Enter> key to accept.

Syntax

```
setup product
```

Mode

Superuser

```
ORACLE# setup product

----------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified
----------------------------------------------------------------
 1 : Product       : Uninitialized

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Product
    1 - Session Border Controller
    2 - Session Router - Session Stateful
    3 - Session Router - Transaction Stateful
    4 - Subscriber-Aware Load Balancer
    5 - Enterprise Session Border Controller
    6 - Peering Session Border Controller
  Enter choice     : 1

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
save SUCCESS
```

shell

The shell command provides debug-level system access. Do not access the shell unless specifically instructed by Oracle Engineering and Support.

Syntax

```
shell
```

Mode

Debug

Copyright © 2024, 2026, Oracle and/or its affiliates.

show

The show command displays Oracle Communications Session Border Controller statistics, configurations, and other information. Many of the show commands display period and lifetime statistic counts.

show about

This command displays credit information including version number for the Oracle Communications Session Border Controller. It also shows current third party licenses applicable to the software image you are running.

Syntax

```
show about
```

Example

```
ORACLE# show about
```

show acl

Syntax

```
show acl <arguments>
```

Arguments

denied—Display denied ACL entries

untrusted—Display untrusted ACL entries

trusted—Display trusted ACL entries

info—Display amount of table space used by ACL entries. Number of entries, percent utilization, and maximum entries are displayed for each ACL type. The following are the ACL types displayed:

- Denied
- Trusted
- Media
- Untrusted
- Dynamic-trusted

reset—Reset the summary counts of all host ACL entries

summary—Displays cumulative and per-interface statistics on ACL traffic and drops, displaying Recent, Total and PerMax counts. The parameter also separates the display of traffic from trusted versus untrusted sites.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ip—Display the same output as show acl all, but takes an IP address as an argument to filter all ACL statistics for the given IP address

all—Display all ACL entries

Example

```
ORACLE# show acl untrusted
```

show accounting

This command displays a summary of statistics for configured external accounting servers.

Syntax

```
show accounting [<IPPort> | All] | [connections] | [ servers ]
```

Arguments

Entered without any arguments, the **show accounting** command displays the global Accounting Status Summary, returning the equivalent of the **show accounting all** command but without per-server message statistics. The command also reports on specific Diameter message for which you want to show information, including:

- CER/CEA—Capabilities Exchange Request /Answer
- ACR/ACA—Accoungint Charging Request/Answer
- DWR/DWA—Device Watchdog Request/Answer
- DPR/DPA—Disconnect Peer Request/Answer

IPPort — identifies the IP address of the accounting server and the specific port for which you want to show information, in the form **IP_Address:port**. This is useful when an Rf server has multiple connections to multiple external servers.

All — displays the statistics for all accounting servers

connections — displays a table listing socket connection information for all Rf servers

servers — displays a table listing server status based on the use of FQDNs to specify diameter servers, and the presence of specific servers within primary or secondary pools.

Example

```
ORACLE# show accounting 192.168.81.81:1813
```

show arp

This command displays the current Internet-to-Ethernet address mappings in the ARP table as well as statistics related to arp resolutions and its traffic.

Syntax

```
show arp [info | statistics]
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

Entered without an argument, the **show arp** command displays the current Internet-to-Ethernet address mappings in the ARP table.

The first section displays the Link Level ARP table including:

- destination address
- ARP gateway
- flags
- reference count
- use
- physical interface on the system.

The second section displays the following information that refers only to media interfaces:

- interface
- VLAN
- IP Address
- MAC address
- time stamp
- type
- active-count—The MBCD application adds multiple flows to steer incoming packets based on your configuration. For the SBC to send a packet to a particular destination, it needs the destination's L2 address (DMAC). To do this, MBCD requests that the L2 application resolve the ARP for that particular destination when the flow is added and that the resolved destination addresses be stored in ARP table. There can be flows whose source address is different but the destination is the same. In these cases, rather than having duplicate entries in the ARP table, the reference count (the active-count value) is incremented. For the Gateway, there is single connection, so this value is always 1. Therefore, a Gateway's active-count value does not change as it is added during the configuration.

The third section shows general ARP table information.

info—Displays the layer 2 and network interface tables for arp database size and number of entries.

statistics—Displays ARP statistics counters for received traffic, transmitted traffic and internal errors.

The first section shows statistics on ARP traffic received.

- Add intf—Number of the added intfs and number of the add failures.
- Delete intf—Number of the deleted intfs and number of the deletion failures.
- Flush intf—Number of the flushed intfs and number of the flushing failures. (L2 resolver flushes the interfaces to get rid of the invalid ports.)
- Add dynamic—Number of the added dynamic l2 entries and number of the add failures.
- Add static—Number of the added static l2 entries and number of the add failures.
- Delete dynamic—Number of the deleted dynamic l2 entries and number of the deletion failures.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Delete static—Number of the deleted static l2 entries and number of the deletion failures.
- Pend—Number of the received l2 messages pending on processing, number of the pending errors, and number of the dropped pending msgs
- Request—Number of the total received l2 requests, number of the request updates, and number of the dropped invalid requests.
- Reply—Number of the total received l2 replies, number of the reply updates, and number of the dropped invalid replies.
- Network—Number of the total received l2 messages from wire, and number of the errors in validating the received l2 messages, which includes invalid l2 packets, subnet errors, ip errors, invalid operations, and net interface errors.
- L2 Pkts—Number of the received invalid l2 packets.
- Subnet—Number of the ip errors.
- Intf—Number of the net intf errors.
- IP—Number of the net intf errors.
- Operation—Number of the net operations errors.

The second section shows statistics on ARP traffic transmitted.

- Request—Number of ARP requests sent for both success and error cases.
- Reply—Number of ARP replies sent for both success and error cases.
- Pend—Number of pending ARP requests for both success and error cases.
- Network—Number of ARP messages sent to network device for both success and error cases.
- Expire—Number of expired/aged ARP entries for both success and error cases.

show backup-config

Syntax

```
show backup-config <config-file>
```

Arguments

<config-file> Enter the name of the saved configuration file
The show backup-config command displays a specified configuration file saved on the Oracle Communications Session Border Controller's standard backup file directory.

Example

```
ORACLE# show backup-config config1_25jun.gz
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

show bfd-stats

Syntax

The bfd-stats command shows Bidirectional Forwarding Detection (BFD) statistics. Use this command to display summary statistics on all BFD sessions, including active session detail and errors. Use the session argument to display detailed statistics on individual sessions.

```
show bfd-stats <errors | session [session-id <detail | messages | errors> ]>
```

Arguments

<errors> Limits the output to system error only.

<session> Presents status information on a per-session basis. Accepts further arguments.

<session-id> Limits the output to the specified session. Accepts one of three further arguments.

<details> Extends the session output.

<messages> Presents message statistics associated with this session.

<errors> Presents error statistics associated with this session.

Mode

Superuser

Example

```
ORACLE# show bfd-stats
```

show buffers

Syntax

```
show buffers <histogram | usage>
```

This command shows memory buffer statistics. Use this command only for debugging purposes under the direction of Oracle support.

Example

ORACLE# show buffers

show built-in-sip-manipulations

This command displays the name of all built-in SIP-manipulations and descriptions.

Syntax

```
show built-in-sip-manipulations
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show built-in-sip-manipulations
```

show call-recording-server

> **Note**
>
> This command is deprecated.

This command displays information regarding the IP call replication for call recording (IPRCR) feature configured on the Oracle Communications Session Border Controller. Entering this command without the optional IPRCR ID displays all IPRCR endpoints configured on the Oracle Communications Session Border Controller along with their state.

Syntax

```
show call-recording-server [crs-id]
```

Arguments

[crs-id] You can specify a IPRCR whose information you want to view. When you specify an ID, the ACLI displays all session agents created for the IPRCR endpoint, it's IP address, its state, and the last time a failover occurred.

Example

```
ORACLE# show call-recording-server crs1
```

show clock

This command displays the current date and time for your Oracle Communications Session Border Controller.

Syntax

```
show clock
```

Example

```
ORACLE# show clock
```

show comm-monitor

Syntax

```
show comm-monitor <by-client client-IP> | <errors> | <internal> | stats
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Displays statistics related to connections between the Oracle Communications Session Border Controller's Communications Monitor probe and any configured Communications Monitor servers. The maximum statistic value is 999999, after which the system restarts the counters from zero.

Running the command without arguments displays the following information:

- Client connection states, presented in a connection sequence order, including:
  - Out-of-Service – Connection is not established.
  - Connecting – Trying to Connect to the Oracle Communications Session Border Controller.
  - Connected – Oracle Communications Session Border Controller connected but not able to collect stats.
  - In-Service – Oracle Communications Session Border Controller connected and able to collect stats.
- Aggregate Socket Statistics, including:
  - Socket Message Sent—Number of Socket Message Sent.
  - Socket Message Dropped—Number of Socket Messages dropped
  - Socket Send Error—Number of Socket Send Errors
  - Socket Not Ready—Number of Sockets Not Ready
  - Socket Timeouts—Number of Socket timeouts
  - Socket Disconnects—Number of Socket disconnects
  - Socket Reconnects—Number of Socket Reconnects
- Client connection statistics, including:
  - Handshake Msg Sent—Count for number of handshakes sent from the Oracle Communications Session Border Controller to the Session Monitor server
  - Handshake Msg ACK—Count for number of handshakes acknowledged by the Communications Monitor server
  - Handshake Msg NAK—Count for number of handshakes not acknowledged by the Communications Monitor server
  - Keep Alive—Signal which keeps the connection between the Oracle Communications Session Border Controller and the Communications Monitor Server
  - SIP UDP Send Msg Sent—UDP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP UDP Recv Msg Sent—UDP Message received sent by the Oracle Communications Session Border Controller to SIP client or the Oracle Communications Session Border Controller to the SIP server
  - SIP TCP Send Msg Sent—TCP Message sent from SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP TCP Recv Msg Sent—TCP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - SIP SCTP Send Msg Sent—SCTP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - SIP SCTP Recv Msg Sent—SCTP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
  - ENUM Sent Msg Sent—ENUM Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
  - ENUM Recv Msg Sent—ENUM Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server

Arguments

by-client <client-IP>—Shows the same statistics as the command presents without arguments, but limits the output to the specified client.

errors—Display information on errors that may occur between the Oracle Communications Session Border Controller and the client.

- Buffer Error—The number of errors occurring on the connection related to Oracle Communications Session Border Controller buffer space.
- Socket Message Dropped—The number of messages traversing the specified socket that the Oracle Communications Session Border Controller has dropped.
- Socket Disconnects—The number of times a connection between the Oracle Communications Session Border Controller and the client has been lost.

internal—Shows the same statistics as the command presents without arguments, but limits the output to statistics related to the Oracle Communications Session Border Controller's perspective. Information displayed includes:

- SIP UDP Send Msg Sent—UDP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP UDP Recv Msg Sent—UDP Message received sent by the Oracle Communications Session Border Controller to SIP client or the Oracle Communications Session Border Controller to the SIP server
- SIP TCP Send Msg Sent—TCP Message sent from SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP TCP Recv Msg Sent—TCP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
- SIP SCTP Send Msg Sent—SCTP Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller
- SIP SCTP Recv Msg Sent—SCTP Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server
- ENUM Sent Msg Sent—ENUM Message sent from the SIP client to the Oracle Communications Session Border Controller or the SIP server to the Oracle Communications Session Border Controller

Copyright © 2024, 2026, Oracle and/or its affiliates.

- ENUM Recv Msg Sent—ENUM Message received sent by the Oracle Communications Session Border Controller to the SIP client or the Oracle Communications Session Border Controller to the SIP server

stats—Shows the same statistics as entering the command without an argument.

Example

```
ORACLE# show comm-monitor by-client 123.1.11.5
```

show configuration

Syntax

```
show configuration [configuration-element] [to-file]
```

This command entered without any arguments displays the current configuration. If you use any configuration element as an argument, this show command displays each instance of only the specified configuration element.

Arguments

<configuration-element> — Specify the configuration element you want to view. This is an optional argument. If you do not specify a configuration element, the Oracle Communications Session Border Controller displays the entire configuration. The following is a list of valid configuration elements:

- Values
  - account-config— Show account-config configuration
  - access-control—Show access-control configuration
  - audit-logging—Show the audit logging configurations
  - auth-params—Show the auth-params configurations
  - authentication—Show the authentication configuration
  - cert-status-profile—Show certificate status profile
  - call-recording-server—Show call-recording-server configurations
  - certificate-record—Show the certificate record configuration
  - class policy—Show all ClassPolicy configuration
  - data-flow—Show the data-flow configurations
  - dns-config—Show all dns-config configurations
  - dpd-params—Show the dpd-params configurations
  - enum-config—Show the enum-config configuration
  - ext-policy-server—Show the external-policy-server configuration
  - h323-config—Show h323 configuration
  - h323-stack—Show all h323-stack configurations
  - ike-certificate-profile—Show the ike-certificate-profile configurations
  - ike-config—Show the ike-config configuration

Copyright © 2024, 2026, Oracle and/or its affiliates.

- ike-interface—Show the ike-interface configurations
- ike-sainfo—Show the ike-sainfo configurations
- ims-aka-profile—Show the ims-aka-profile configurations
- ipsec-global-config—Show the ipsec-global-config configurations
- iwf-stack—Show iwf-stack configuration
- host-route—Show all host-route configurations
- local-address-pool—Show the local-address-pool configurations
- local-policy—Show all local-policy configurations
- local-response-map—Show sip-local-map configuration
- login-config—Show the login configurations
- media-profile—Show all media-profile configurations
- media-manager—Show media-manager configuration
- media-policy—Show all MediaPolicy configurations
- network-interface—Show all network-interface configurations
- network-parameters—Show all network-parameters configurations
- ntp-config—Show ntp-config configuration
- capture-receiver—Show capture-receiver configurations
- phy-interface—Show all phys-interface configurations
- public-key—Show the public-key configurations
- realm-config—Show all realm configurations
- q850-sip-map—Show q850-sip-map configurations
- qos-constraints—Show the qos-constraints configurations
- redundancy-config—Show redundancy-config configuration
- sip-response-map—Show all response map configurations
- rph-profile—Show rph-profile configurations
- rph-policy—Show rph-policy configurations
- session-agent—Show all session-agent configurations
- session-group—Show all session-group configurations
- session-translation—Show all session-translation configurations
- session-router—Show session-router configuration
- sip-config—Show all sip-config configurations
- sip-feature—Show all sip-feature configurations
- sip-interface—Show all sip-interface configurations
- sip-manipulation—Show all of the sip-manipulation configurations
- sip-nat—Show all sip-nat configurations
- sip-profile—Show the sip-profile configurations
- sip-isup-profile—Show the sip-isup-profile configurations
- enforcement-profile—Show enforcement-profile configurations

Copyright © 2024, 2026, Oracle and/or its affiliates.

- sip-q850-map—Show sip-q850-map configuration
- snmp-community—Show all snmp-community configurations
- ssh-config—Show the SSH configurations
- static-flow—Show all static-flow configurations
- steering-pool—Show all steering-pool configurations
- realm-group—Show realm-group configurations
- surrogate-agent—Show all of the surrogate-agent configurations
- system-config—Show system-config configuration
- tls-profile—Show TLS profile configurations
- translation-rules—Show all translation-rules configurations
- trap-receiver—Show all TrapReceiver configurations
- codec-policy—Show all codec-policy configurations
- local-routing-config—Show all local-routing configurations
- net-management-control—Show all net-management-control configurations
- security-association—Show all security-association configurations
- security-policy—Show all security-policy configurations
- password-policy—Show password-policy configuration
- session-constraints—Show all session-constraint configurations
- system-access-list—Show all system-access-list configurations
- tls-global—Show all tls-global configurations
- inventory—Display an inventory of all configured elements on the Oracle Communications Session Border Controller

<to-file> — Send all output from the show config command to a specified file located on the local flash file system instead of to the ACLI. This is an optional argument.

Example

```
ORACLE# show configuration snmp-community
```

show directory

This command displays a list of file directories on the storage expansion module. Disk space on the Storage Expansion Module appears as a local volume on the Oracle Communications Session Border Controller.

Syntax

```
show directory <path>
```

Arguments

<path> Enter the absolute path of the file directory with a forward slash preceding the path name.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# show directory /logs
```

show dns

Sytnax

```
show dns < stats | cache-entry | lookup <arguments> | query <arguments> >
```

Arguments

stats
Show the statistics for the dns configuration. Your entries must follow the following formats:

- NAPTR records—NAPTR:abc.com
- SRV records—SRV:_sip._tcp.abc.com
- A records—A:abc.com

cache-entry
Look in the DNS cache for a specific entry. Your entries must follow the following formats:

- NAPTR records—NAPTR:abc.com
- SRV records—SRV:_sip._tcp.abc.com
- A records—A:abc.com

lookup
Perform a domain name services (DNS) query, first by an internal DNS cache lookup and then, if no results are found, perform an external DNS query from the command line. Subsequent arguments include:

- realm— Realm name to use for DNS cache lookup key
- type— Type of DNS query:
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service records, e.g. SRV_sip_tcp.abc.com
  - NAPTR for naming authority pointers, e.g. NAPTR.abc.com
- name— Fully qualified domain name (FQDN) of DNS name to lookup

query
Perform a manual external Domain Name Services (DNS) query from the command line. Subsequent arguments include:

- realm— Realm name to use for DNS cache lookup key

Copyright © 2024, 2026, Oracle and/or its affiliates.

- type— Type of DNS query:
  - A for IPv4 lookup
  - AAAA for IPv6 lookup
  - SRV for service records, e.g. SRV_sip_tcp.abc.com
  - NAPTR for naming authority pointers, e.g. NAPTR.abc.com
- name— Fully qualified domain name (FQDN) of DNS name to lookup

Example

```
ORACLE# show dns stats
```

show dnsalg rate

show dnsalg rate command

Displays the transaction rate of DNS ALG bound and sourced messages.

show entitlements

Use the **show entitlements** command to display all currently provisioned features and controlled features on the system. You can also use the **setup entitlements** command and type **d** to display the current features. The first time you execute the **setup entitlements** command, the system displays all provisioned features (excluding controlled features). You can edit the existing features, so long as you do not change the product type.

Syntax

```
show entitlements
```

Example 3-7 Show Entitlements Example

```
Provisioned Entitlements:
-------------------------
Session Border Controller Base    : enabled
Session Capacity                  : 32000
  Accounting                      : enabled
  IPv4 - IPv6 Interworking        : enabled
  IWF (SIP-H323)                  : enabled
  Load Balancing                  : enabled
  Policy Server                   : enabled
  Quality of Service              : enabled
  Routing                         : enabled
  SIPREC Session Recording        : enabled
Admin Security                    :
ANSSI R226 Compliance             :
IMS-AKA Endpoints                 : 750000
IPSec Trunking Sessions           : 1024
MSRP B2BUA Sessions               : 128000
SRTP Sessions                     : 128000
Transcode Codec AMR Capacity      : 100
Transcode Codec AMRWB Capacity    : 110
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
Transcode Codec EVRC Capacity     : 120
Transcode Codec EVRCB Capacity    : 130
Transcode Codec EVS Capacity      : 140
Transcode Codec OPUS Capacity     : 150
Transcode Codec SILK Capacity     : 160

Keyed (Licensed) Entitlements
-----------------------------
<CustomerName> License

MGCP
PAC
LI
TLS
Software TLS
H248
H248 SCF
H248 BGF
LI Debug
Session Replication for Recording
Transcode Codec AMR (uncapped AMR transcoding sessions)
Transcode Codec EVRC (uncapped EVRC transcoding sessions)
DoS
RTSP
Transcode Codec EVRCB (uncapped EVRCB transcoding sessions)
Software PCOM
Security Gateway
SIP Authorization/Authentication
Database Registrar (320000 contacts)
SLB (2000000 endpoints)
Software SRTP
Allow Unsigned SPL files
Diameter Director
Transcode Codec AMR-WB (uncapped AMRWB transcoding sessions)
CX
Transcode Codec Opus (uncapped OPUS transcoding sessions)
Transcode Codec SILK (uncapped SILK transcoding sessions)
Fraud Protection
GTP
```

show enum

Sytnax

```
show enum <arguments>
```

Displays ENUM statistics for your Oracle Communications Session Border Controller.

Arguments

Each valid enum argument is listed below:

- all: Shows stats summary of all ENUM Agents
- cache-entry: Look in the ENUM cache for a specific entry

Copyright © 2024, 2026, Oracle and/or its affiliates.

- h323d: Shows stats summary of all h323d ENUM Agents
- lookup: Query an ENUM cache for a specific E.164 number
- sipd: Shows stats summary of all sipd ENUM Agents
- stats: Show the statistics for the ENUM configuration
- status: Show the state of configured ENUM agents.

> **Note**
>
> In HA deployments, because the ENUM server state is stored locally, the active and standby SBC may show different states.

- rate: Displays the transaction rate of ENUM messages

The following information may be displayed for each output:

- Enum Agent: Name of enum agents
- Queries Total: Number of enum queries
- Successful Total: Number of successful enum queries
- Not Found Total: Number of enum queries returning not found
- Timeout Total: Number of enum query timeouts

Example

```
ORACLE# show enum lookup
```

show ext-band-mgr

Sytnax

```
show ext-band-mgr
```

This command shows the external bandwidth manager / PDP/RACF statistics for the active, period, and lifetime monitoring spans. COPS message counts are shown for Recent and lifetime monitoring spans.

Example

```
ORACLE# show ext-band-mgr
```

show ext-clf-svr

Syntax

```
show ext-clf-svr
```

This command shows the CLF connection statistics for the active, period, and lifetime monitoring spans. CLF message counts are shown for Recent and lifetime monitoring spans.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show ext-clf-svr
```

show fax-group stats

Syntax

```
show fax-group stats [fax-group name]
```

Run this command to display statistics about traffic handled by one or more fax-groups.

Example

```
ORACLE# show fax-group stats mygroup
```

show features

Syntax

```
show features
```

This command shows the currently enabled features based on added licenses.

Example

```
ORACLE# show features
```

show h323d

Syntax

```
show h323d <arguments>
```

This command displays H.323 statistics for your Oracle Communications Session Border Controller.

Arguments

status—Display H.323 server status. The following statistics are displayed when this command is entered:

- Incoming Calls—Number of incoming H.323 calls; displayed for period, lifetime, and active counts
- Outgoing Calls—Number of outgoing H.323 calls; displayed for period, lifetime, and active counts
- Connected Calls—Number of currently connected H.323 calls; displayed for period, lifetime, and active counts

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Incoming Channels—Number of established incoming channels; displayed for period, lifetime, and active counts
- Outgoing Channels—Number of established outgoing channels; displayed for period, lifetime, and active counts
- Contexts—Number of established H.323 contexts; displayed for period, lifetime, and active counts
- Queued Messages—Number of messages queued; displayed for current and lifetime durations
- TPKT Channels—Number of TPKT channels open(ed); displayed for current and lifetime durations
- UDP Channels—Number of UDP channels open(ed); displayed for current and lifetime durations

config—Display the H.323 configuration

agentstats—Display H.323 session agent statistics. By typing show h323d agentstats <agent>, you can view activity for the H.323 session agent that you specify.

groupstats—Display session information for session agent groups

h323stats—Display H.323 stacks and statistics on the Oracle Communications Session Border Controller. The display identifies the H.323 stack by its name and then provides the data for each H.323 stack. Adding a stackname h323d h323stats <stack-name> displays detailed statistics for the H.323 stack that you specify. This information is displayed according to the following categories: H.225, H.245, and RAS.

registrations—Display H.323 registration endpoints information

sessions all—Display all H.323 sessions currently on the system

sessions by-agent <agent name>—Display H.323 sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display H.323 sessions for the call ID specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display H.323 sessions for the specified IP address for an endpoint; adding iw to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number.—Display H.323 sessions for the specified user; adding iw to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

stack-alarms—Display a list of H.323 stacks that raised an alarm

stackCallstats—Show a summary of H.323 call statistics for all stacks

stackPvtstats—Show a summary of H.323 stack's internal data structures

stackDisconnectInstats—Show a summary of H.323 pvt statistics for all stacks

tackDisconnectOutstats— Show Summary of H.323 pvt statistics for all stacks

Executing the show h323 command without any arguments will return the same output as using the status argument.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show h323d status
```

show health

Syntax

```
show health
```

In HA architectures, the show health command displays the following information:

- Health score
- Current Oracle Communications Session Border Controller HA state as active, standby, or out of service
- If media flow information is synchronized for both supported protocols: SIP and H.323 (true/false). If media flow information is not available, Media Synchronized disabled will be displayed in the show health output.
- If SIP signaling information is synchronized (true/false). If SIP signaling is not available, SIP Synchronized disabled will be displayed in the show health output.
- If configuration information is synchronized (true/false). If configuration checkpointing is not available, Config Synchronized disabled will be displayed in the show health output.
- IP address of the current HA Oracle Communications Session Border Controller's active peer (no peer is denoted with an IP address of 0.0.0.0)
- Last message received from the HA Oracle Communications Session Border Controller peer
- A switchover log containing the last 20 switchover events

Example

```
ORACLE# show health
```

show imports

This command displays the list of sip-manipulation rules exported as files to the /code/imports directory.

Syntax

```
show imports
```

Mode

Superuser

Example

```
ORACLE# show imports
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

show interface-mapping

Syntax

```
show interface-mapping
```

This command is deprecated. Equal functionality is provided using the **interface-mapping** branch's **show** command and the **show interfaces mapping** command.

show interfaces

Syntax

```
show interfaces [brief] [ethernet] [mapping]
```

The show interfaces command shows all information concerning the Oracle Communications Session Border Controller's rear interfaces:

- Flags (such as loopback, broadcast, promiscuous, ARP, running, and debug)
- Type
- Internet address
- VLAN ID (if applicable)
- Broadcast address (if applicable)
- Netmask
- Subnet mask (if applicable)
- Gateway (if applicable)
- Ethernet (MAC) address (if applicable)
- Route metric
- Maximum transfer unit size
- Number of octets sent and received on this interface (if applicable)
- Number of packets sent and received on this interface
- Number of non-unicast packets sent and received on this interface (if applicable)
- Number of unicast packets sent and received on this interface (if applicable)
- Number of multicast packets sent and received on this interface (if applicable)
- Number of input discards (if applicable)
- Number of input unknown protocols (if applicable)
- Number of input and output errors
- Number of collisions
- Number of drops
  This command also displays information for loopback interfaces.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

<brief> Allows you to view key running statistics about the operational interfaces within a single screen. This is an optional argument.

<ethernet> Allows you to view status information on all configurable interfaces within a single screen. This is an optional argument.

<mapping> Provides the same functionality as the **interface-mapping** branch's **show** command. This is an optional argument available only on VNF or COTS deployments.

> **Note**
>
> When run on a virtual platform, the show interfaces and show interfaces ethernet commands display auto-negotiation as disabled whenever media port is down, regardless of the ACLI configurations.

Example

```
ORACLE# show interfaces
```

show ip

Syntax

```
show ip <arguments>
```

Displays IP statistics for the Oracle Communications Session Border Controller.

Arguments

The following is a list of valid show ip arguments:

- statistics —Display detailed IP statistics
- connections —Display all TCP and UDP connections
- sctp—Display all SCTP statistics, including a list of current connections per SCTP state and systemwide counts.
- tcp —Display all TCP statistics, including a list of current connections per TCP state and differentiated by inbound, outbound, listen and IMS-AKA connections as well as systemwide counts.
- udp —Display all UDP statistics

Executing the **show ip** command with no arguments returns the equivalent of the **show ip statistics** command.

show logfile

Syntax

```
show logfile [filename]
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Display log files saved onto the Oracle Communications Session Border Controller. Entering this command without specifying a filename displays a complete list of log files.

Arguments

[filename] Specify the file whose logs you want to view. This is an optional argument.

Example

```
ORACLE# show logfile
```

show loglevel

Syntax

```
show loglevel <task> [<type> | <verbose>] [filename]
```

This command displays loglevel statistics for your Oracle Communications Session Border Controller.

Arguments

<task> Enter the name of the Oracle Communications Session Border Controller task for which you are requesting information. By typing all, you are given an abbreviated display of all running processes.

<type> Select the log type whose level is to be displayed.

<verbose> Type verbose at the end of the show loglevel command to view a verbose display of either a specified task or all tasks. This is an optional argument.

[file-name] Enter the name of the specific logfile you want to view. This is an optional argument.

Example

```
ORACLE# show loglevel sipd verbose
```

show lrt

Syntax

```
show lrt <route-entry | route-table| “stats”>
```

This command displays Local Routing Table (LRT) statistics on the Oracle Communications Session Border Controller.

Arguments

- <route-entry> - Display a specific entry in the LRT.
  - <lrt-config-name> <user> - Display route for a specific user.
  - <local-route-config> <table record key> - Display route along with the next-hop entries based on a record key in the LRT.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- <route-table> - Display several entries in the LRT.
  - <lrt-config-name> - Display routes along with their priority and weight for a specific route table.
  - <local-route-config> <display-count> - Display routes along with their next-hop entries, with a limit of 10 next-hop entries per route in the LRT.

    The display-count field allows you to specify the number of routes to be displayed ranging from 1 to 10. This is an optional field with a default value of 5.
- <stats> - Display all LRT statistics.
  - <local-route-config> - Display LRT statistics for a specific table.

Example

ORACLE# show route-entry Yt 9212

show mbcd

Syntax

```
show mbcd <arguments>
```

The show mbcd command displays MBCD statistics for your Oracle Communications Session Border Controller.

Arguments

statistics —Display information related media flows established by the MBCD task. The following is a list of the MBCD statistics displayed when you enter this command:

The following counts are given for Period (high and total) and Lifetime (Total, period-max, High) windows. Currently Active counts are also displayed.

- Client Sessions—Number of media sessions established by application clients of the MBCD task. Clients of MBCD include all signaling protocol tasks (SIP and H.323).
- Client Trans—Number of MBCD transactions in the application clients to create, modify and remove flows
- Contexts—Number of Contexts in the MBCD task. A Context represents the MBCD Server side of a media session. It contains all flows for the media session.
- Flows—Number of unidirectional flows established in MBCD. This includes both static flows defined by the signaling configuration, and dynamic flows for media sessions.
- Flow-Port—Number of "anchor" ports established by MBCD. MBCD maintains a mapping of the RTP steering port allocated for a flow so it can recognize flows that hairpin or spiral through the Oracle Communications Session Border Controller. This statistic reflects the number of entries in that table.
- Flow-NAT—Number of entries in the MBCD table that maps CAM entry indexes to flows. An entry is added to this table when a NAT entry is added to the CAM for a flow.
- Flow-RTCP—Number of special NAT table entries for RTCP. For Hosted NAT Traversal (HNT), the RTP and RTCP flows must be treated separately because the source port of the RTCP cannot be predicted.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Flow-Hairpin—Number of hairpined/spiraled flows recognized by MBCD. This occurs when the signaling originates in an access realm, goes into a backbone realm, and then back into the same access realm, or another access realm on the same network interface.
- Flow-Released—Number of hairpined/spiraled flows released back into the original realm (when mm-in-realm or mm-in-network is disabled)
- MSM-Release—Number of flows that have been released as part of the SIP distributed (multi-system) release feature
- Rel-Port—Number of "release anchor" ports established by MBCD. MBCD maintains a mapping of the RTP steering port allocated for a flow so it can recognize flows that hairpin or spiral through the SBC. These "release anchor" ports are retained as part of media flows that are not released immediately after calls. This enables the system to quickly re-establish media-flows that may be hairpinned back it by other network elements To retain IP/port information for all released calls, configure the SBC option "hairpin-released-flows" in "media-manager". The system deletes retained IP/port flows after the guard timer's expiration.
- Rel-Hairpin—Number of retained hairpined/spiraled flows recognized by MBCD. Retained media flows are not released immediately after calls are released, which enables the system to quickly re-establish media-flows that may be hairpinned back to the SBC by other network elements.
- NAT Entries—Number of NAT table entries in the CAM established by MBCD for its flows. The NAT table can be viewed with the show nat commands.
- Free Ports—Number of ports available from configured steering pools
- Used Ports—Number of ports allocated to flows
- Port Sorts—Number of times the free ports list had to be sorted because consecutive ports (for RTP & RTCP) could not be found
- Queued Notify—Number of MBC transactions waiting in queue to be processed by MBCD
- MBC Trans—Number of MBC transactions currently in progress
- MBC Ignored—Number of requests ignored because it is in standby mode in an HA configuration
- ARP Trans—Number of ARP Transactions. In some cases, MBCD must obtain the MAC address of the destination of a flow before an entry can be added to the NAT table. This statistic shows the number of outstanding ARP requests for MBCD flows.
- Relatch NAT—Number of times relatching occurred for NAT RTP flows
- Relatch RTCP—Number of times relatching occurred for NAT RTCP flows
- Media Playback—Number of times media playback occurred
- MSM-SRTP-Passthrough—Number of Multi-system Selective SRTP sessions
- Flow-MSRP—Number of MSRSP flows
- SRTP Only Flows—Number of times only SRTP flows sessions occurred
- SRTCP Only Flows—Number of times only SRTCP flows occurred
- Collapsed Flows—Number of SRTP collapsed flows where RTP and RTCP flows use same port
- SRTP Sessions—Number of SRTP sessions
- DTLS-SRTP Sessions—Number of DTLS SRTP sessions
- ICE-STUN Sessions—Number of ICE-STUN sessions

Copyright © 2024, 2026, Oracle and/or its affiliates.

nat— Display statistics about MBCD's usage of the NAT Table and flow guard timer events. The following is a list of all MBCD NAT statistics:

- Adds—Number of times an entry was added to the NAT table
- Deletes—Number of times an entry was removed from the NAT table
- Updates—Number of times a NAT table entry was updated, including updates due to the "latching" event when the first packet for a flow is received
- Non-Starts—Number of initial flow guard timeouts (i.e. number of times a packet was never received for a NAT table entry)
- Stops—Number of subsequent flow guard timeouts (i.e. number of times that packets stopped for a NAT table entry)
- Timeouts—Number of total session limit timeouts (i.e. number of times the session limit for a flow was exceeded)

acls—Display MBCD Access Control statistics, starting with a time stamp showing when the current period began. The following is a list of each entry count:

- The following ACL statistics are shown for the Period and Lifetime monitoring spans:
- Static Trusted
- Static Blocked
- Dynamic Trusted
- Dynamic Blocked
  The following ACL statistics are shown for the Lifetime monitoring span:
- Add Requests
- Added
- Removed
- Dropped

errors —Display MBCD task error statistics, starting with a time stamp showing when the current period began; statistics for client and server are included. The following is a list of MBCD error statistics displayed when you enter this command:

- Client statistics count errors and events encountered by applications that use the MBCD to set up and tear down media sessions:
- Client Errors—Number of errors in the client application related to MBC transactions that are otherwise uncategorized
- Open Streams Failed—Number of MBC transactions creating or updating a media session that could not be sent to the MBCD because the media session state information could not be located
- Drop Streams Failed—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located
- Client IPC Errors—Number of errors in the client application related to the Inter-Process Communication
- No Session (Open)—Number of MBC transactions creating or updating a media session that could not be sent to MBCD because the media session state information could not be located
- No Session (Drop)—Number of MBC transactions deleting a media session that could not be sent to MBCD because the media session state information could not be located

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Monitor Streams Failed
- Exp Flow Events—Number of flow timer expiration notifications received from the MBCD by all applications
- Exp Flow Not Found—Number of flow timer expiration notifications received from the MBCD by all applications for which no media session or flow information was present in the application
- Transaction Timeouts—Number of MBC transaction timeouts
  Server statistics count errors and events encountered by MBCD:
- Server Errors—Number of uncategorized errors in the MBCD server
- Server IPC Errors—Number of errors on the server related to the IPC
- Flow Dup Replace Failed—Number of times failed to replace duplicate flow additions Doc Update
- Flow Duplicated—Number of times flow collisions observed when adding flows
- NatFlow install Errors—Number of flow errors occurred when installing NAT flows
- NatFlow apply Errors—Number of flow errors occurred when encountered when trying to apply ppm
- NatFlow destry Errors—Number of flow errors occurred when encountered when trying to delete ppm
- Flow Add Failed—Number of errors encountered when attempting to add an entry to the NAT table
- Flow Delete Failed—Number of errors encountered when attempting to remove an entry from the NAT table
- Flow Update Failed—Number of errors encountered when attempting to update an entry in the NAT table upon receipt of the first packet for a media flow
- Flow Latch Failed—Number of errors when attempting to locate an entry in the NAT table upon receipt of the first packet for a media flow
- Pending Flow Expired—Number of flow timer expirations for pending flows that have not been added to the NAT table
- ARP Wait Errors—Number of errors and timeouts related to obtaining the Layer 2 addressing information necessary for sending media
- Exp CAM Not Found—Number that the NAT table entry for an expired flow could not find in the NAT table. This usually occurs due to a race condition between the removal of the NAT entry and the flow timer expiration notification being sent to MBCD.
- Drop Unknown Exp Flow—Number of flows deleted by the MBCD because of a negative response from the application to a flow timer expiration notification
- Drop/Exp Flow Missing—Number of flows not found when trying to delete them
- Unk Exp Flow Missing—Number of negative responses from the application to a flow timer expiration notification for which the designated flow could not be found in MBCD's tables
- Exp Notify Failed—Number of errors encountered when the MBCD attempted to send a flow timer expiration notification to the application
- Unacknowledged Notify—Number of flow expiration notification messages sent from MBCD to the application for which MBCD did not receive a response in a timely manner
- No Flows In Chain—Number of flows which are not part of other flows

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Main Flow Notify Skips—Number of flows for which NOTIFY is sent to other flows but not to the original flow
- Notify Not Sent (Skip)—Number of flows for which NOTIFY was not sent
- Drop Chain Failures—Number of failures observed for flow chain drops
- ACL Deletes—Number of ACL flow deletes
- Saved Flows—Number of saved flows not teared down in case of timeouts
- NoTimeout on otherFlow—Number of flows for which timeout not occurred for other flow
- Ignore TimerOn Relatch—Number of flows for which relatching is ignored as timeout occurred
- Relatching Timeouts—Number of flows for which relatching timeout has occurred
- Invalid Realm—Number of flow setup failures due to an unknown realm in the request from the application
- No Ports Available—Number of times ports were not available for allocating to flows
- Insufficient Bandwidth—Number of flow setup failures due to insufficient bandwidth in the ingress or egress realm
- Stale Ports Reclaimed—For an HA node, this is the number of ports that were reclaimed when the standby had a stale flow that the active system replaced; when the flow is replaced, the steering ports are also reallocated properly (i.e., according to the active system)
- Stale Flows Replaced—For an HA node, this is the number of times that the standby system had entries in its flow tables that did not match those on the active system; the active system replaced the standby's stale flows with valid ones
- Telephone Events Gen—Number of times telephony events were generated
- Media Playback Fails—Number of times media playback failures occurred
- Playback Exh Resources—Number of times media playback failures occurred due to out of resources
- Playback Flow Inactive—Number of times playback was stopped as flow was inactive
- Playback Mismatch—Number of times media playback failures was observed due to playback codec mismatch
- Pipe Alloc Errors—Errors Number of times media pipe allocation failures were observed
- Pipe Write Errors—Number of times failed to write data to pipe
- Not Found In Flows—Number of times flow was not found in NAT table
- MPO Realm Mismatch—Number of times realm mismatch errors were observed in mediarealm list
- XCode Internal Errors—Number of uncategorized errors due to Transcoding session error
- XCode Alloc Errors—Number of times that buffer allocation failed for transcoding tasks
- XCode Update Errors—Number of errors encountered when attempting to update an entry in the transcoding table
- XCode Delete Errors—Number of errors encountered when attempting to delete an entry in the transcoding table
- XCode Over Cap Errors—Number of Transcoding sessions denied once session capacity is reached

Copyright © 2024, 2026, Oracle and/or its affiliates.

- XCode Over License Cap—Number of Transcoding sessions denied once capacity is reached
- SRTP Flow Add Failed—Number of times failed to delete SRTP flows to NAT table
- SRTP Flow Delete Failed—Number of times failed to delete SRTP flows from NAT table
- SRTP Flow Update Failed—Number of times failed to update SRTP flows from NAT table
- SRTP Capacity Exceeded—Number of times SRTP maximum capacity reached
- Adds—Number of SRTP flows added to NAT table
- Deletes—Number of SRTP flows deleted from NAT table
- Updates—Number of SRTP flows updated in NAT table

msrp— Display statistics about MSRP traffic, with subsequent arguments, including:

- realm—Detail on traffic on a per-realm basis. Subsequent arguments include:
  <realm-id>—Limits the output to the realm name used as an argument. Subsequent arguments include:
  - SEND—Detail on SEND method traffic.
  - SEND responses—Limits the output to detail on responses to SEND method traffic.
  - REPORT—Detail on REPORT method traffic.
  - REPORT failure—Limits the output to detail on failure REPORT method traffic.
- send—Detail on SEND method traffic.
- send responses—Limits the output to detail on responses to SEND method traffic.
- report—Detail on REPORT method traffic.
- report failures—Limits the output to detail on failure REPORT method traffic.

add—List statistics of mbcd transactions that include an Add command. Statistics are given for Recent, Total, and PerMax periods. The following is a list of MBCD add statistics displayed when you enter this command:

- Add incoming statistics when an add message is received by the Oracle Communications Session Border Controller
- Incoming requests received—Number of mbcd add commands received
- Incoming replies sent—Number of responses sent in response to an mbcd add
- Incoming errors sent—Number of errors sent in response to an mbcd add
  Add outgoing statistics when an mbcd add message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD add commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent Add message
- Outgoing errors received—Number of errors received in response to a sent Add message

modify —List statistics of mbcd transactions that include a modify command. The following is a list of MBCD modify statistics displayed when you enter this command:

- Add incoming statistics when a modify message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of mbcd modify commands received

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Incoming replies sent—Number of responses sent in response to an mbcd modify
- Incoming errors sent—Number of errors sent in response to an mbcd modify
  Add outgoing statistics when an mbcd modify message is sent by the Oracle Communications Session Border Controller.
- Outgoing requests sent—Number of MBCD modify commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent modify message
- Outgoing errors received—Number of errors received in response to a sent modify message

subtract—List statistics of mbcd transactions that include a subtract command. The following is a list of MBCD subtract statistics that are displayed when you enter this command:

- Add incoming statistics when a subtract message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of mbcd subtract commands received
- Incoming replies sent—Number of responses sent in response to an mbcd subtract
- Incoming errors sent—Number of errors sent in response to an mbcd subtract
  Add outgoing statistics when an MBCD subtract message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD subtract commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent subtract message
- Outgoing errors received—Number of errors received in response to a sent subtract message

notify—List statistics of mbcd transactions that include a notify command. The following is a list of MBCD notify statistics that are displayed when you enter this command:

- Add incoming statistics when a notify message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of mbcd notify commands received
- Incoming replies sent—Number of responses sent in response to an mbcd notify
- Incoming errors sent—Number of errors sent in response to an mbcd notify
  Add outgoing statistics when an mbcd notify message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD notify commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a sent notify message
- Outgoing errors received—Number of errors received in response to a sent notify message

other—List statistics of mbcd transactions related to non-compliant protocols used by specific customers. The following is a list of statistics displayed when you enter this command:

- Add incoming statistics when a customer-specific message is received by the Oracle Communications Session Border Controller:
- Incoming requests received—Number of customer-specific mbcd commands received

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Incoming replies sent—Number of responses sent in response to a customer-specific mbcd command
- Incoming errors sent—Number of errors sent in response to a customer-specific mbcd command
  Add outgoing statistics when a customer-specific mbcd message is sent by the Oracle Communications Session Border Controller:
- Outgoing requests sent—Number of MBCD notify commands sent from the Oracle Communications Session Border Controller
- Outgoing replies received—Number of responses received in response to a customer-specific message
- Outgoing errors received—Number of errors received in response to a sent customer-specific message

realms—Display steering ports and bandwidth usage for home, public, and private realms. The following is a list of statistics displayed when you enter this command:

- Used—Number of steering ports used
- Free—Number of free steering ports
- No Ports—Number of times that a steering port could not be allocated
- Flows—Number of established media flows
- Ingress—Amount of bandwidth being used for inbound flows
- Egress—Amount of bandwidth being used for outbound flows
- Total—Maximum bandwidth set for this realm
- Insuf BW—Number of times that a session was rejected due to insufficient bandwidth

realms <realm-name>—Display mbcd realm statistics for a given realm; given for period and lifetime durations. The following is a list of statistics displayed when you enter this command:

- Ports Used—Number of ports used
- Free Ports—Number of free ports
- No Ports Avail—Number of times no steering ports were available
- Ingress Band—Amount of bandwidth used for inbound flows
- Egress Band—Amount of bandwidth used for outbound flows
- BW Allocations—Number of times that bandwidth was allocated
- Band Not Avail—Number of times a session was rejected due to insufficient bandwidth

redundancy —Display the equivalent of the show redundancy mbcd command

all —Display information related to many of the show mbcd subcommands. Only those MBC messages for which there are statistics are shown. Rather than entering the individual subcommands, all information is displayed for the following:

- MBC status
- NAT entries
- MBC errors
- MBC messages including: add, modify, subtract, notify, and other

stun—Display STUN server statistics

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Servers—The number of STUN servers (the same as the number of realms configured with a STUN server).
- Server Ports—Number of ports per STUN server; there will be four ports per STUN server.
- Binding Requests—Number of STUN Binding Request messages received by all STUN servers.
- Binding Responses—Number of STUN Binding Response messages sent by all STUN servers.
- Binding Errors—Number of STUN Binding Error messages sent by all STUN servers.
- Messages Dropped—Number of messages dropped by all STUN servers.

Example

```
ORACLE# show mbcd errors
```

show media

Syntax

```
show media <media-stats> <slot> <port> <vlan>
```

Arguments

<media-stats> The following is a list of admin state arguments:

- classify —Display network processor statistics by protocol, including BFD; requires slot and port arguments
- host-stats —Display statistics for the host processor including number of packets received at a specific port and types of packets received; requires slot and port arguments
- frame-stats —Display frame counts and drops along the host path; does not require port and slot specification
- network — Display network interface details; does not require port and slot specification
- physical —Display all phy-interface information; does not require port and slot specification
- phy-stats —Display data/packets received on the front interface (media) ports; shows the physical level of front interface statistics according to slot and port numbers and is displayed according to received data/packets and transmitted data/packets; requires slot and port arguments
- tm-stats—Show all of the traffic manager statistics and shows the results of the traffic policing due to NetSAFE configuration. This command is used only for debugging purposes. Do not execute this command unless instructed by Oracle Engineering or Support.
- utilization—Show physical level utilization

<slot>— Select the media interface slot

- Values 0 (left slot) | 1 (right slot)

<port> —Select the media interface port

- Values 0 (leftmost) | 1 | 2 | 3 (rightmost)

<vlan> Enter the VLAN ID if required

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show media network 1 2 0
```

show memory

Syntax

```
show memory [memory-stats]
```

This command displays statistics related to the memory of your Oracle Communications Session Border Controller.

Arguments

[memory-stats] The following is a list of each memory statistic:

- usage—Display system-wide memory usage statistics. If the show memory command is issued without any arguments, the equivalent of this argument is displayed.
- application—Display application memory usage statistics
- l2—Display layer 2 cache status
- l3—Display layer 3 cache status
- sobjects—Displays the number of sobject classes currently consuming system memory. Use this command only for debugging purposes under the direction of Oracle support.

show monthly-minutes

Syntax

```
show monthly-minutes <realm-id>
```

Display the monthly minutes for a specified realm.

Arguments

<realm-id> Enter the specific realm whose monthly minutes you want to view.

Example

```
ORACLE# show monthly-minutes realm1
```

show mps-stats

Syntax

```
show mps-stats [all | rvalue]
```

The show mps-stats command displays information about inbound sessions and r-values from rph-profile configurations.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Arguments

<all> Display information about inbound sessions and r-values for the Oracle Communications Session Border Controller's MPS support feature. This is an optional argument.

<rvalue> View statistics for a specific r-value. An r-value is a namespace and priority combination entered in the following format: namespace.priority. The display also shows the specified r-value for which it is displaying data. This is an optional argument. If there are no configured rph-profiles, the command does not display any r-value data.

Mode

User, Superuser

show msrp statistics

show msrp statistics command.

Displays cumulative MSRP session counts.

> **Note**
>
> If you reset the statistics while calls and sessions are in progress, the system does not keep the existing data or re-synchronize it with the reset. When the calls and sessions are completed, the statistics show negative values. Do not reset show-msrp-stats while calls and sessions are in progress.

show nat

Syntax

```
show nat <display-type>
```

Displays NAT statistics for a specified NAT time on the Oracle Communications Session Border Controller.

Arguments

<display-type> The following is a list of each method to display the nat table:
by-index —Display a specified range of entries in the NAT table, with a maximum of 5024 entries. The default range is 1 through 200. The range corresponds to line numbers in the table, and not to the number of the entry itself. The syntax for using the show nat by-index command is:

```
show nat by-index <starting entry> <ending entry>
```

in-tabular —Display a specified range of entries in the NAT table display in table form, maximum of 5024 entries. The syntax is modeled on the show nat by-index command:

```
show nat in-tabular <starting entry> <ending entry>
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

by-addr—Display NAT table information matching source and destination addresses. You must specify source address (SA) and/or destination address (DA) values. If no addresses are entered, the Oracle Communications Session Border Controller shows all of the table entries. NAT entries can be matched according to SA or DA or both.

```
show nat by-addr <source IPv4 address> <destination IPv4 address>
```

info—Display general NAT table information. The output is used for quick viewing of a Oracle Communications Session Border Controller's overall NAT functions, including the maximum number of NAT table entries, the number of used NAT table entries, the length of the NAT table search key, the first searchable NAT table entry address, the length of the data entry, the first data entry address, and whether or not aging and policing are enabled in the NAT table.

flow-info—Display NAT table entry debug information. You must specify if you want to view NAT data for all entries or if you want to specify an address or a switch ID.

```
show nat flow-info [by-addr | srtp]
```

Example

```
ACMEPACKET# show nat by-index
```

show neighbor-table

Syntax

```
show neighbor-table
```

The show neighbor-table command displays the IPv6 neighbor table and validates that there is an entry for the link local address, and the gateway uses that MAC address.

Example

```
ORACLE# show neighbor-table
LINK LEVEL NEIGHBOR TABLE
Neighbor                              Linklayer Address  Netif Expire    S
Flags
300::100                              0:8:25:a1:ab:43      sp0 permanent ? R
871962224
400::100                              0:8:25:a1:ab:45      sp1 permanent ? R
871962516
fe80::bc02:a98f:f61e:20%sp0           be:2:ac:1e:0:20      sp0 4s        ? R
871962808
fe80::bc01:a98f:f61e:20%sp1           be:1:ac:1e:0:20      sp1 4s        ? R
871963100
------------------------------------------------------------------------------
ICMPv6 Neighbor Table:
------------------------------------------------------------------------------
------------
  entry: slot port vlan IP                                type       flag
pendBlk Hit MAC
------------------------------------------------------------------------------
------------
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
  5    : 1    0    0    fe80::bc01:a98f:f61e:20/64     08-DYNAMIC 1
0       1   be:01:ac:1e:00:20
  4    : 1    0    0    0.0.0.0/64                     01-GATEWAY 0
0       1   be:01:ac:1e:00:20
  3    : 1    0    0    400::/64                       02-NETWORK 0
0       1   00:00:00:00:00:00
  2    : 0    0    0    fe80::bc02:a98f:f61e:20/64     08-DYNAMIC 1
0       1   be:02:ac:1e:00:20
  1    : 0    0    0    0.0.0.0/64                     01-GATEWAY 0
0       1   be:02:ac:1e:00:20
  0    : 0    0    0    300::/64                       02-NETWORK 0
0       1   00:00:00:00:00:00
-------------------------------------------------------------------------
------------
```

show net-management-control

Syntax

```
show net-management-control [string | all]
```

This command displays network management control statistics on the Oracle Communications Session Border Controller.

Arguments

<string> —Enter a name for the net-management-control configuration whose statistics you want to view. This is an optional argument.

<all> Enter all to view statistics for all net-management-control entries. This is an optional argument.

Example

```
ORACLE# show net-management-control
```

show nsep-stats

Syntax

```
show nsep-stats [all | rvalue | realms [ realm-id [ rvalue | dialed-number ]]]
```

The show nsep-stats command displays information about inbound and outbound sessions.

Arguments

<all> Display information about inbound and outbound sessions and r-values for the Oracle Communications Session Border Controller's NSEP support feature. This is an optional argument.

<rvalue> View statistics for a specific r-value. An r-value is a namespace and priority combination entered in the following format: namespace.priority. The display also shows the specified r-value for which it is displaying data. This is an optional argument.

Copyright © 2024, 2026, Oracle and/or its affiliates.

<realms> Groups statistics by enabled realms, or, when used with its own arguments, limits the output to a specific realms. You must enable specific realms to produce this output. This is an optional argument.

realms <realm-id> Requires the realms argument and narrows the output to the specified realm. You must enable specific realms to produce this output. This is an optional argument.

realms <realm-id> <rvalue> Requires the realm-id argument and narrows the output to the specified rvalue in that realm. You must enable specific rvalues to produce this output. This is an optional argument.

realms <realm-id> <dialed-number> Requires the realm-id argument and narrows the output to the specified dialed-number in that realm. You must enable specific dialed-numbers to produce this output. This is an optional argument.

Mode

User, Superuser

show ntp

Syntax

```
show ntp <arguments>
```

The show ntp command displays information about NTP servers configured for use with the system

Arguments

servers—Display information about the quality of the time being used in terms of offset and delay measurement; maximum error bounds are also displayed.

status—Display information about configuration status, NTP daemon synchronization, NTP synchronizations in process, if NTP is down.

Mode

User, Superuser

Example

```
ORACLE# show ntp servers
```

show packet-trace

Syntax

```
show packet-trace
```

The show packet-trace command displays active, REMOTE traces. The command also allows you to check whether the Oracle Communications Session Border Controller's tracing status is currently enabled or disabled.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# show packet-trace
```

show platform

Syntax

```
show platform [all | cpu | cpu-load | errors | heap-statistics | kernel-
drivers | limits | memory | paths | pci components]
```

The show platform command is useful for distinguishing various hardware and software configurations for the current version of software from other hardware platform on which this software may run.

Arguments

- all—Display full platform information
- cpu—Display summary CPU information
- cpu-load—Displays percent CPU consumed on each core during the last 10 second window using calculations similar to the linux top command.
- errors—Display Servicepipe write errors
- heap-statistics—Display total in-use memory for small and large allocations based upon TCMalloc's class and classless sizes.
- kernel-drivers—Display included kernel drivers
- limits—Display platform related limits
- memory—Display current memory usage
- paths—Display filesystem paths
- pci—Display relevant pci bus information
- components—Display the specific versions of the OS packages

> **Note**
>
> No argument concatenates all arguments.

show platform limits

This command displays the current limits for a variety of operating capacities. The output of **show platform limits** is based on the platform this command is executed from and the software version running. The command has no arguments.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

Sample output is displayed below.

```
ORACLE# show platform limits
Maximum number of sessions:3000
Maximum number of ACLS: 60000
Maximum number of common PAC buffers: 8000
Maximum number of kernel-rules: 216256
Maximum CPS rate: 300
Maximum number of TCP Connections: 60000
Maximum number of TLS Connections: 10
Maximum number of packet buffers: 30000
Maximum Signaling rate: 4000
Maximum number of session agents: 125
Maximum number of System ACLs: 256
Maximum number of VLANs: 4096
Maximum number of ARPs: 4104
Maximum number of INTFC Flows: 4096
Maximum number of Static Trusted Entries: 8192
Maximum number of Untrusted Entries: 4096
Maximum number of Media Entries: 6000
Maximum number of Deny Entries: 8192
Maximum number of Internal Flows: 32
Maximum number of Sip Rec Sessions: 512
Maximum number of RFC 2833 Flows: 6000
Maximum number of SRTP Sessions: 500
Maximum number of QoS Sessions: 3000
Maximum number of Xcoded Sessions: 100
Maximum number of HMU Flows: 6000
Maximum number of Transport Sessions: 0
Maximum number of MSRP Sessions: 0
Maximum number of SLB Tunnels: 0
Maximum number of SLB Endpoints: 0
Maximum number of IPSec SAs: 0
Maximum Licensed Capacity: 256000
```

show platform nftables

This command displays the nftables in table format.

Refer to the nftable documentation to understand the syntax of the command output.

Syntax

```
show platform nftables
```

show policy-server

The **show policy-server** command allows you to view specific information about a supplied policy server object.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
show policy-server [[standby | <Name|AgentName> | <IP_Address:Port>]
[<DiamMsg>]] | [connections]
```

Arguments

Name — Accepts the FQDN of the policy server for which you want to show information. Also accepts policy-groups name, providing cumulative statistics. Specifying a policy-agent name after the policy-group name displays statistics specific to that agent.

IP_Address:Port — identifies the IP address of the policy server and the specific port for which you want to show information. This is useful when an Rx server has multiple connections to multiple external servers.

DiamMsg — identifies a specific Diameter message for which you want to show information. The accepted diameter messages are:

- AAR — Authorization-Authentication Request
- ASR — Abort-Session-Request
- CER — Capabilities-Exchange-Request
- DWR — Device-Watchdog-Request. The display table for DWR has two sections: DWR Sent and DWR Received.
- RAR — Re-Authorization-Request
- STR — Session-Termination-Request

connections — displays a table listing the active TCP connections; that is, it identifies the local and remote IP addresses and ports, and the socket state for the policy server. The command also displays multihoming connections and socket stated for agents configured for SCTP.

show power

The show power command allows you to view Oracle Communications Session Border Controller power supply information including the state of the power supply and the installation position.

Example

```
ORACLE# show power
```

show privilege

Syntax

```
show privilege
```

Displays the current level of privilege on which the user is operating:

- Privilege level 0 refers to Level 0: User Mode
- Privilege level 1 refers to Level 1: Superuser Mode

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show privilege
```

show processes

Syntax

```
show processes <process>
```

The show processes command, executed without arguments, displays statistics for all active processes. The following task information is displayed: names of tasks, entries, task identification codes, task priorities, status, program counter, error numbers, and protector domain (PD) identification.

Arguments

<process> The following is a list of each process argument:

- sysmand—Display sysmand process statistics related to the system's startup tasks
- ebmd— Show embd process statistics
- h323d— Show h323d process statistics
- lid— Show lid process statistics
- snmpd— Show snmpd process statistics
- berpd—Display statistics for the border element redundancy protocol tasks; only accessible if your system is operating in an HA node
- lemd—Display lemd process statistics
- brokerd—Display brokerd process statistics
- mbcd—Display mbcd process statistics related to the middlebox control daemon
- radd—Display radd process statistics related to RADIUS; only accessible if your Oracle Communications Session Border Controller is using RADIUS
- algd—Display algd process statistics
- sipd—Display sipd process statistics

current—Show the date and time that the current monitoring period began and statistics for the current application process events. The following fields explain the output of the show processes current command:

- Svcs—Number of times the process performs actions for different services (e.g., sockets, timeout queues, etc.)
- TOQ—Number of active timers (in the Timed Objects) placed in the timeout queue
- Ops—Number of times the process was prompted (or polled) to perform an action
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alrm—Number of alarms the process sent

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage over the last minute
- Now—CPU usage for the last second

total —Display the total statistics for all of the application processes applicable to your Oracle Communications Session Border Controller. The following fields explain the output of the show processes total command:

- Svcs—Number of times the process performed actions for different services (e.g., sockets, timeout queues, etc.)
- Rcvd—Number of messages received by the process
- Sent—Number of messages sent by the process
- Events—Number of times a TOQ entry timed out
- Alarm—Number of alarms the process sent
- Slog—Number of times the process wrote to the system log
- Plog—Number of times the process wrote to the process log
- CPU—Average CPU usage since last reboot
- Max—Maximum percentage of CPU usage in a 60 second period

collect—Show collector process statistics

CPU —Display information about the CPU usage for your Oracle Communications Session Border Controller, categorized on a per task/process basis. The following fields explain the output of the show processes cpu command:

- Task Name—Name of the Oracle Communications Session Border Controller task or process
- Task Id—Identification number for the task or process
- Pri—Priority for the CPU usage
- Status—Status of the CPU usage
- Total CPU—Total CPU usage since last reboot in hours, minutes, and seconds
- Avg—Displays percentage of CPU usage since the Oracle Communications Session Border Controller was last rebooted
- Now—CPU usage in the last second

all — concatenate the show process command for all running prcoesses

memory—Show memory process statistics

top—The show processes top command displays realtime updates of per-process CPU utilization.

Example

```
ORACLE# show processes sysmand
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

show prom-info

Syntax

```
show prom-info <devices>
```

The show prom-info command displays hard-coded information about Oracle Communications Session Border Controller PROM information. The valid arguments which you enter in the show prom-info command depend on the current platform.

The show prom-info command is most immediately used to obtain device part numbers and revisions.

Arguments

<devices> The following is a list of available prom-info devices to query:
Acme Packet 6100/6400

- CPU— CPU PROM information
- MGMT—management interface card PROM information
- PHY0— NIU card PROM information
- POWER—power supply PROM information
- SEC0—security module PROM information
- TCU1-DIMM— lists the populated DSP DIMMs on a TCU card and their PROM information
- all—Show all available PROM information
- mainboard—Display mainboard PROM information

Acme Packet 6300/6350

- CPU— CPU PROM information
- FLEX1—riser card between mainboard and NIU in slot 1 PROM information
- FLEX2—riser card between mainboard and NIU in slot 2 PROM information
- MGMT— management interface card PROM information
- PHY0—NIU card 0 (bottom) PROM information
- PHY1—NIU card 1 (middle) PROM information
- PHY2— NIU card 2 (top) PROM information
- POWER— power supply PROM information
- SEC1—security module 1 PROM information
- SEC2—security module 2 PROM information
- TCU1-DIMM— lists the populated DSP DIMMs on the TCU 1 card and the modules' PROM information
- TCU2-DIMM— lists the populated DSP DIMMs on the TCU 2 card and the modules' PROM information
- all—Show all available PROM information
- mainboard—Display mainboard PROM information

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show prom-info mainboard
```

show queues

Syntax

```
show queues [SIPD [commands <by-id <#>] | atcpd | CCD | DNS | FPE | LBP |
LDAP | LRT | MBCD ]
```

The show queues command displays thread level CPU usage information for the specified protocol threads. Use this command only for debugging purposes under the direction of Oracle support.

show radius

Syntax

```
show radius <radius-stats>
```

This command displays RADIUS statistics.

Arguments

authentication—Show the authentication statistics

all—Show accounting, authentication, and CDR statistics on all RADIUS servers

cdr—Display all CDR statistics

accounting—Display the status of established RADIUS accounting connections. This argument has its own argument: <ALL | IPPORT>, where ALL returns accounting statistics for all RADIUS servers and IPPORT identifies the specific IP address and port of the accounting server for which you want to show information, in the form **IP_Address:port**. If you attempt to execute this argument for a Diameter accounting server, the command will be blocked with the message

```
Accounting configured for DIAMETER.  Please use "show accounting".
```

A successful RADIUS connection is displayed as READY, and an unsuccessful connection is displayed as DISABLED.
The command's output is divided into three sections:

1. Client Display—Display general accounting setup (as established in the account-config element); includes the following information:
   - state of the RADIUS client
   - accounting strategy
   - IP address and port on which the Oracle Communications Session Border Controller's server is listening
   - maximum message delay in seconds
   - number of configured accounting servers

Copyright © 2024, 2026, Oracle and/or its affiliates.

2. Waiting Queue—Display the number of accounting (RADIUS) messages waiting to be sent that are queued on the client side
3. <IP Address:Port>—IP Address and port headings indicated will be per the referenced RADIUS server active on the IP Address and port shown; also includes information about the accounting server's state

Example

```
ORACLE# show radius authentication
```

show ramdrv

Displays RAMdrive usage, including the log cleaner threshold values and the size of the most recently saved configuration.

Example

```
ORACLE# show ramdrv
```

show realm

Syntax

```
show realm <realm-id>
```

Arguments

<realm-id> Specify the realm-id whose realm-specific data you want to view; includes QoS routing data for internal and external transactions

Example

```
ORACLE# show realm realm1
```

show rec

Syntax

```
show rec [redundancy]
```

Shows statistics for Recording Agent for SIP REC. You may add the redundancy argument to show SIPREC redundancy statistics.

Object	Description
Rec Sessions	Number of recording sessions during an active period of time and over a lifetime period.
Comm Groups	Number of active communication session recording groups during an active period of time and over a lifetime period.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Object	Description
Comm Sessions	Number of active communication sessions during an active period of time and over a lifetime period.
Media Streams	Number of active media streams during an active period of time and over a lifetime period.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period.
RDs Terminated	Number of recording dialogs terminated over a lifetime period. This increments when the recording call establishment towards session recording server(SRS) gets failed.
CSs Terminated	Number of communication sessions terminated over a lifetime period. This increments when recording call establishment towards SRS gets failed.
CSs not established	Number of communication sessions not established over a lifetime period. This increments when recording call establishment towards SRS gets failed.

> **Note**
>
> The counters RDs Terminated, CSs Terminated, and CSs Not Established are implemented as counter statistics and increments only when the recording call establishment fails. These statistics have values for only Period Total, Lifetime Total & Lifetime PerMax values.

show rec srg <srg_name>

Run this command to view the statistics for an individual SRG.

Syntax

```
show rec srg srg1
```

show rec srs <srs_name>

Run this command to view the statistics for a specific SRS..

Syntax

```
show rec srs srs1
```

This table provides a description of the statistics displayed in the output of the `show rec srs <srs_name>` command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 3-1 Status description

Status	Description
Comm Groups	Number of active communication session recording groups during an active period of time and over a lifetime period
Comm Sessions	Number of active communication sessions during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
CSs not established	Communication Sessions not established over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed. Note: - The last 3 counters “RDs Terminated”, “CSs Terminated” and “CSs not established” will only get incremented when recording call establishment fails. And also they always remain under Active count, they will never be moved from Active period.
CSs Terminated	Communication Sessions terminated over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed
Media Streams –	Number of active media streams during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
RDs Terminated	Recording dialogs terminated over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed.
Recording Sessions	Number of recording sessions during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.

Note

The counters RDs Terminated, CSs Terminated, and CSs Not Established are implemented as counter statistics. These statistics have values for only Period Total, Lifetime Total and Lifetime PerMax values.

Status Description

The table lists the status displayed in the show rec srs <srs_name> command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 3-2 Status description

Status	Description
Recording Sessions	Number of recording sessions during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Comm Groups	Number of active communication session recording groups during an active period of time and over a lifetime period
Media Streams –	Number of active media streams during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Comm Sessions	Number of active communication sessions during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
Participants	Total number of participants in session recordings during an active period of time and over a lifetime period. This will be incremented when recording call towards SRS gets established.
RDs Terminated	Recording dialogs terminated over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed.
CSs Terminated	Communication Sessions terminated over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed
CSs not established	Communication Sessions not established over a lifetime period. This will be incremented when recording call establishment towards SRS gets failed. Note: - The last 3 counters “RDs Terminated”, “CSs Terminated” and “CSs not established” will only get incremented when recording call establishment fails. And also they always remain under Active count, they will never be moved from Active period.

Note

The last 3 counters `RDs Terminated`, `CSs Terminated` and `CSs not established` are implemented as counter statistics. These statistics have values for only Period Total, Lifetime Total & Lifetime PerMax values.

Copyright © 2024, 2026, Oracle and/or its affiliates.

show redundancy

Syntax

```
show redundancy <taskname> [actions] | [objects] | [journals [size [by-id
<id#>] | [perf [by-id <id#>]
```

The show redundancy command displays HA statistics for a redundant Oracle Communications Session Border Controller (SBC).

Arguments

<taskname> The following is a list of redundancy taskname arguments. A taskname is required, and output varies based on taskname:

- mbcd— Display the synchronization of media flows for the members of an HA SBC pair.
- algd—Display the synchronization of signaling for the members of an HA SBC pair
- sipd—Display the synchronization of SIP signaling for the members of an HA SBC pair
- config—Display the synchronization of configuration information for the members of an HA SBC pair
- collect—Display the Collect redundancy statistics
- rec—Display the SIPREC redundancy statistics
- radius-cdr—Display the number of CDRs that have been synchronized from active to standby when the local CDR storage is enabled
- iked—Display IKE redundancy statistics
- manuald—Display manual redundancy statistics
- rotated-cdr—Display statistics for rotated CDRs on the SBC.

The following HA statistics definitions apply to the applicable command output for Period and Lifetime monitoring spans.

- Queued entries—Number of transactions not yet sent to standby SBC peer.
- Red Records—Total number of HA transactions created
- Records Dropped—Number of HA transaction records lost because the standby SBC fell behind in synchronization
- Server Trans—Number of HA transactions in which the SBC acted was the server
- Client Trans—Number of HA transactions where the SBC was the client
  The following HA transaction statistics are shown for the Lifetime monitoring span.
- Requests received—Number of HA requests received by the SBC, acting as server
- Duplicate requests—Number of situations in which an HA request was received by the SBC, and (acting as the server side in the client-server relationship) the SBC responded to it, but the client system did not receive the response in time and retransmitted its original request
- Success responses—Number of HA requests that were received followed by a successful response to the client
- Error responses—Number of HA requests that were received followed by a error response to the client

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Request sent—Number of HA requests that were sent by the standby SBC
- Retransmission sent—Number of times an HA request was retransmitted after no response
- Success received—Number of HA requests receiving a reply from the other SBC in an HA pair
- Errors received—Number of errors received in response to HA requests
- Transaction timeouts—Number of HA transactions that timed out
- Avg Latency—Calculation based on the Transaction Latency Request-Response RTTs
- Max Latency—The maximum lifetime latency experienced by the current standby
- Last redundant transaction processed—The numerical identifier of the last redundant transaction processed.
- Request-Response Loss—Number of recent and lifetime transactions lost
- Transaction Latency Request-Response RTTs—Request-Response round-trip-time (RTT) values, displayed as the number of times the RTT time result fell into the following ranges:
  - 0 ns – 2 ms
  - 2 – 4 ms
  - 4 – 8 ms
  - 8 – 16 ms
  - 16 – 33 ms
  - 33 - 67 ms
  - > 67 ms

Output to subsequent arguments vary based on the taskname specified. If the argument does not apply to the taskname, the system displays **command not found**. These arguments include:

- actions—Shows flow add, delete and modify counters.
- objects—Shows statistics on the sipd objects supported by redundancy. The system collects these statistics on both the active and standby SBC, and are never reset.
- journals—shows per-task journal size and performance tables. Subsequent arguments specify the desired table, and can limit the output to a specific journal:
  - size— Shows the journal number, journal state, journal size and journal drops for each journal.
    Journal states include:
  - * Resyn—Resynchronizing
    * Sync—Synchronizing
    * Sced— Synchronized

    To execute for a single journal, include the **by-id <number>** argument after the **size** argument, where <number> is the journal number. Journal numbering is 0-based.
  - perf— Shows the journal number, journal latency (recent period average, number of samples used for average calculation and maximum latency), journal queue rates (enqueue rate and dequeue rate) and journal overflows (i.e. full) on 1 line for each journal.
    To execute for a single journal, include the **by-id <number>** argument after the **size** argument, where <number> is the journal number. Journal numbering is 0-based.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Journal statistics only have meaning on the active SBC; initially, these values are 0 on a standby SBC. For debugging purpose, however, the system does not reset these statistics during a switchover. You can reset these counters using the **reset redundancy** command.

Example

```
ORACLE# show redundancy sipd
```

show registration

Syntax

```
show registration <protocol> <by-ip | by-user> <ip-address | by-endpoint> |
<statistics> | surrogate-agent <realm-id> | <unregistered>
```

To expand the capabilities of the show registration command, enter either by-user or by-ip after the protocol argument.

Arguments

<protocol> Select the protocol whose registration you want to view

- sipd
- h323

by-user <user> — Show registration information for a specific IP address of an endpoint, or a wildcard IP address value with an asterisk (*) at the end.

by-realm <realm> — Display information for calls that have registered through a specified ingress realm whose registration cache information you want to view. The realm value can be a wildcard.

by-registrar <registrar> — Display information for calls that use a specific registrar. Add the IP address of the registrar whose registration cache information you want to view. This value can be wildcarded.

by-route <IP address> — Display information for calls by their IP address which is able to be routed. This allows you to view the endpoints associated with public addresses. Enter the IP address whose registration cache information you want to view. This value can be wildcard.

by-endpoint <IP address> — Show registration information for a specific phone number or username. Provide the IP address of an endpoint, or a wildcard IP address value with an asterisk (*) at the end. This command is only available if you configure the reg-via-key parameter in the SIP interface configuration prior to endpoint registration. The **reg-via-key** parameter keys all registered endpoints by IP address and username.

Surrogate Agent — Displays all surrogate agents and their state including the last time of registration for each agent. The <unregistered> option displays all unregistered surrogate agents.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Phone number or username— Full phone number or username, or a wildcard number/username with an asterisk (*) . The display shows statistics for the Period and Lifetime monitoring spans.

- User Entries—The number of unique SIP Addresses of Record in the cache
- Local Contacts—The number of contact entries in the cache
- Free Map Ports—The number of ports available in the free signaling port pool
- Used Map Ports—The number of signaling ports allocated for registration cache entries
- Forwards—Number of registration requests forwarded to the real registrar
- Refreshes—Number of registrations the Oracle Communications Session Border Controller answered without having to forward registrations to the real registrar
- Rejects—Number of unsuccessful registrations sent to real registrar
- Timeouts—Number of times a refresh from the HNT endpoint was not received before the timeout
- Fwd Postponed—The number of times sipd responded out of the cache instead of forwarding to the registrar due to the max-register-forward threshold
- Fwd Rejected—The number of REGISTER 503s done after checking for a cached entry
- Refr Extension—The number of times the max-register-refresh threshold was exceeded. The "Active" and "High" show the number of seconds added to the expiration
- Refresh Extended—The number of times the expire time in a REGISTER response was extended due to the max-register-refresh threshold
- Surrogate Regs— The total number of surrogate registers
- Surrogate Sent— The total number of surrogate registers sent
- Surrogate Reject—The total number of surrogate register rejects
- Surrogate Timeout— The total number of surrogate register timeouts
- Transport—The transport protocol used in registration
- Secure—Whether or not the transport protocol is secure.

statistics— Display a table of counters showing the total and periodic number of registrations, by protocol.

Example

```
ORACLE# show registration sipd by-user *
```

show route-stats

Syntax

```
show route-stats
```

The show route-stats command shows routing statistics including bad routing redirects, dynamically created routes, new gateway due to redirects, destinations found unreachable, and use of a wildcard route.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show route-stats
```

show routes

Syntax

```
show routes
```

The show routes command displays the current system routing table. This table displays the following information:

- destination
- netmask
- TOS
- gateway
- flags
- reference count
- use
- interface
- protocol information

Example

```
ORACLE# show routes
```

show running-config

Syntax

```
show running-config <to-file> | <configuration-element> <element key field>
```

The show running-config entered without any arguments displays the running configuration information in use on the Oracle Communications Session Border Controller. If you use any configuration element key field as an argument, this show command will display only that specified configuration element.

Arguments

<to-file> — Send all output from the show config command to a specified file located on the local flash file system instead of to the ACLI. This is an optional argument.

<configuration-element> — Specify the configuration element you want to view. This is an optional argument. If you do not specify a configuration element, the Oracle Communications Session Border Controller displays the entire configuration.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show running-config host-route
```

show sa

Syntax

```
show sa
```

or

```
show sa stats
```

This command displays the security associations information for IMS-AKA. The srtp option is not available for the ETC NIU.

Example

```
ORACLE# show sa stats
```

show security

Syntax

```
show security <argument>
```

This command displays configured security information on the SBC

Arguments

authorized-key [brief | detail] <name>
Displays information about the authorized key of an SSH client.

ca-key [brief | detail] <key-name>
Displays information about the CA key.

ca-user-revoke [brief | detail] <key-name>
Displays information about the keys that have been revoked.

certificates <argument>
Show certificate information.

- brief—Display a brief certificate description
- detail—Display a detailed certificate description
- list-names—Display a list of all installed certificates omitting detail and presenting certificate names only
- pem—Display certificate information in Privacy Enhanced Mail (PEM) form

Copyright © 2024, 2026, Oracle and/or its affiliates.

- wancom0—Display certificate information for the wancom0 interface

crl <certificate-record>
Show CRL issued by this certificate-record

dtls-srtp [all | realm_id]
Display DTLS-SRTP statistics.

ike <arguments>
Displays statistics for IKE transactions.

- data-flow—Display data-flow information for IKE2
- local-address-pool <pool ID | brief> —Display local address pool information for IKE2
  - pool ID—Display a specific local address pool in detail
  - brief—Display all local address pools briefly

ipsec <arguments>
Show IPSEC related information. You can specify the name of the network interface whose IPSEC information you want to view.

- sad—Display IPSEC SAD information
- spd—Display IPSEC SDP information
- statistics—Display IPSEC statistics
- status—Display the interface IPSEC status

known-host [brief | detail] <name>
Displays information about the known host key of an SSH server.

ocsp stats
Display OCSP statistics.

public-host-key < dsa | rsa >
Show the system's RSA or DSA public host key.

srtp <arguments>
Show SRTP related information.

- sad—security-association database entries (Only the brief option is valid for ETC NIU)
- sessions—number of active SRTP sessions (not valid for ETC NIU)
- spd—security-policy database entries
- statistics—interface and SA entry statistics (not valid for ETC NIU)
- status—display interface IPSEC status (not valid for ETC NIU)
- check-mini-cert <sipuraProfileName>—reads the XML file corresponding to the given sipura profile from /code/sipura/ directory of the SBC, then parses and checks the validity of the Sipura mini-certificate present in the file by verifying the signature and the expiration date of the certificate. It outputs if the mini-certificate is verified successfully or not
- display-mini-cert <sipuraProfileName>—reads the file corresponding to the given sipura profile from /code/sipura directory of the SBC, then parses the file and decodes the base-64 encoded information. It outputs the information present in the mini-certificate in text format. This includes the user name, user ID, expiration date, public key and the signature.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- update-mini-cert <sipuraProfileName>—If a user wishes to change the content of a certificate file (thus the minicertificate and keys) and would like the SBC to use this updated certificate and keys during call setup, then the user can accomplish this by first changing the content of the file and then executing this ACLI command specifying the Sipura profile that uses this file. This command when executed will attempt to read the file that is configured in the given Sipura profile and then will parse the file and update the minicertificate and keys that is used for this sipura profile. This command assumes that the file is present in /code/sipura directory and the user has not changed the file name configured in the Sipura profile.

ssm-accelerator
Display the SSM status.

stun [all | realm_id]
Show STUN statistics

tls
Display TLS related information.

- session-cache—Display TLS session cache information
- stats—Display TLS/DTLS statistics for signaling traffic.

Example

```
ORACLE# show security ipsec spd m10
```

show sessions

Syntax

```
show sessions
```

Displays session capacity for license and session use.

Total session capacity of the system list listed from this command.

The following statistics are available in a table for Period and Lifetime monitoring spans:

- Total Sessions—The aggregation of all current active subscriber sessions (H.323 call/SIP session) and is the total session count against the capacity license.
- SIP Sessions—The total current active SIP sessions
- H.323 Calls—The total current active H.323 calls
- Established Tunnels—
- H.248 ALG Contexts— not used

The IWF Statistics are shown for the Period and Lifetime monitoring spans.

- H.323 to SIP Calls—The calls that come in H.323 and go out SIP. These calls are included in “H.323 Calls” in the Session Statistics.
- SIP to H.323 Calls—The calls that come in SIP and go out H.323. These calls are included in “SIP Sessions” in the Session Statistics.

SIP Statistics including Audio, and video call counts are shown for the Period and Lifetime monitoring spans.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Session-based Messaging Session counts are shown for the Period and Lifetime monitoring spans.

show sfps

Syntax

```
show sfps
```

The show sfps command displays the EEPROM contents of the SFP modules in the system (Small Form-Factor Pluggable (optical transceiver module)).

show sipd

Syntax

```
show sipd <arguments>
```

The show sipd command displays SIP statistics on your Oracle Communications Session Border Controller.

Arguments

status—Display information about SIP transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. The following statistics are displayed when using the show sipd status command.

- Dialogs—Number of end-to-end SIP signaling connections
- CallID Map—Total number of successful session header Call ID mappings
- Sessions—Number of sessions established by an INVITE
- Subscriptions—Number of sessions established by SUBSCRIPTION
- Rejections—Number of rejected INVITEs
- ReINVITEs—Number of ReINVITEs
- Media Sessions—Number of successful media sessions
- Media Pending—Number of media sessions waiting to be established
- Client Trans—Number of client transactions
- Server Trans—Number of server transactions that have taken place on the Oracle Communications Session Border Controller
- Resp Contexts—Number of current response contexts
- Saved Contexts—Total number of saved contexts
- Sockets—Number of active SIP sockets
- Req Dropped—Number of requests dropped
- DNS Trans—Number of DNS transactions
- DNS Sockets—Number of DNS Sockets
- DNS Results—Number of dns results

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Session Rate—The rate, per second, of SIP invites allowed to or from the Oracle Communications Session Border Controller during the sliding window period. The rate is computed every 10 seconds
- Load Rate—Average Central Processing Unit (CPU) utilization of the Oracle Communications Session Border Controller during the current window. The average is computed every 10 seconds. When you configure the load-limit in the SIPConfig record, the system computes the average every 5 seconds

errors —Display statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Errors are only displayed for the lifetime monitoring span.

- SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)
- SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)
- Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog or session; or c) a BYE initiated by the system due to a timeout notification from MBCD
- Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session
- Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found
- Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized
- Media Exp Events—Flow timer expiration notifications received from MBCD
- Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction
- Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application
- Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy
- Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle Communications Session Border Controller
- Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session
- Non-ACK 2xx Drops—Number of sessions terminated because an ACK was not received for a 2xx response
- Invalid Requests—Number of invalid requests; an unsupported header for example
- Invalid Responses—Number of invalid responses; no Via header for example
- Invalid Messages—Number of messages dropped due to parse failure
- CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded
- Expired Sessions—Number of sessions terminated due to the session timer expiring

Copyright © 2024, 2026, Oracle and/or its affiliates.

- CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth
  Lifetime displays show information for recent, total, and period maximum error statistics:
- Recent—Number of errors occurring in the number of seconds listed after the time stamp
- Total—Number of errors occurring since last reboot
- PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring

policy—Display SIP local policy / routing statistics for lifetime duration

- Local Policy Lookups—Number of Local policy lookups
- Local Policy Hits—Number of successful local policy lookups
- Local Policy Misses—Number of local policy lookup failures
- Local Policy Drops—Number of local policy lookups where the next hop session agent group is H323
- Agent Group Hits—Number of successful local policy lookups for session agent groups
- Agent Group Misses—Number of successful local policy lookups where no session agent was available for session agent group
- No Routes Found—Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance
- Missing Dialog—Number of local policy lookups where the dialog is not found for a request addressed to the Oracle Communications Session Border Controller with a To tag or for a NOTIFY-SUBSCRIBE sip request
- Inb SA Constraints—Number of successful local policy lookups where inbound session agent exceeded constraints
- Outb SA Constraints—Number of successful outbound local policy lookups where session agent exceeded constraints
- Inb Reg SA Constraints—Number of successful inbound local policy lookups where registrar exceeded constraints
- Out Reg SA Constraints—Number of successful outbound local policy lookups where registrar exceeded constraints
- Requests Challenged—Number of requests challenged
- Challenge Found— Number of challenges found
- Challenge Not Found—Number of challenges not found
- Challenge Dropped—Number of challenges dropped

server—Display statistics for SIP server events when the Oracle Communications Session Border Controller acts as a SIP server in its B2BUA role. Period and Lifetime monitoring spans for SIP server transactions are provided.

- All States—Number of all server transactions
- Initial—Number of times the “initial” state was entered after a request was received
- Queued—Number of times the “queued” state is entered because resources are temporarily unavailable
- Trying—Number of times the “trying” state was entered due to the receipt of a request
- Proceeding—Number of times a server transaction has been constructed for a request
- Cancelled—Number of INVITE transactions that received a CANCEL

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Established—Number of times the server sent a 2xx response to an INVITE
- Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state
- Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state
- Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

client —Display statistics for SIP client events when the Oracle Communications Session Border Controller is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

- All States—Number of all client transactions
- Initial—State when initial server transaction is created before a request is sent
- Trying—Number of times the “trying” state was entered due to the sending of a request
- Calling—Number of times that the “calling” state was entered due to the receipt of an INVITE request
- Proceeding—Number of times that the “proceeding” state was entered due to the receipt of a provisional response while in the “calling” state
- Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state
- Completed—Number of times that the “completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “calling” or “proceeding” state
- SetMedia—Number of transactions in which the Oracle Communications Session Border Controller is setting up NAT and steering ports
- Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing
- Terminated—Number of times the “terminated” state was entered after a 2xx message

acls—Display ACL information for Period and Lifetime monitoring spans

- Total entries—Total ACL Entries, including both trusted and blocked
- Trusted—Number of trusted ACL entries
- Blocked—Number of blocked ACL entries
- Blocked NATs—Number of blocked entries that are behind NATs
  Lifetime monitoring span is displayed for SIP ACL Operations.
- ACL Requests—Number of ACL requests
- Bad Messages —Number of bad messages
- Promotions—Number of ACL entry promotions
- Demotions—Number of ACL entry demotions
- Trust->Untrust—Number of ACL entries demoted from trusted to untrusted
- Untrust->Deny—Number of acl entries demoted from untrusted to deny

sessions—Display the number of sessions and dialogs in various states for the Period and Lifetime monitoring spans, in addition to the current Active count:

- Sessions—Identical to the identically named statistic on the show sipd status command
- Initial—Displays sessions for which an INVITE of SUBSCRIBE is being forwarded

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Early—Displays sessions for which the first provisional response (1xx other than 100) is received
- Established—Displays sessions for which a success (2xx) response is received
- Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established" session or forwarding an error response for an "Initial" or "Early" session. The session will remain in the "Terminated" state until all the resources for the session are freed.
- Dialogs—Identical to the identically named statistic on the show sipd status command
- Early—Displays dialogs that were created by a provisional response
- Confirmed—Displays dialogs that were created by a success response. An "Early" dialog will transition to "Confirmed" when a success response is received
- Terminated—Displays dialogs that were ended by receiving/sending a BYE for an Established" session or receiving/sending error response "Early" dialog. The dialog will remain in the "Terminated" state until all the resources for the session are freed.

sessions all—Display all SIP sessions currently on the system

sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

redundancy—Display sipd redundancy statistics. Executing the show sipd redundancy command is the equivalent to the show redundancy sipd command.

agents [hostname][method][-t]—Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For a specific session agent, identified by IP address, the show sipd agents command lists:

- session agent state
  - D—disabled
  - I—in-service
  - O—out-of-service
  - S—transitioning from out-of-service to in-service
- inbound and outbound statistics
- average and maximum latency for each session agent
- maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field

Copyright © 2024, 2026, Oracle and/or its affiliates.

Inbound Statistics:

- Active—Number of active sessions sent to each session agent listed
- Rate—Average rate of session invitations (per second) sent to each session agent listed
- ConEx—Number of times the constraints have been exceeded
  Outbound Statistics:
- Active—Number of active sessions sent from each session agent
- Rate—Average rate of session invitations (per second) sent from each session agent listed
- ConEx—Number of times the constraints have been exceeded
  Latency:
- Avg—Average latency for packets traveling to and from each session agent
- Max—Maximum latency for packets traveling to and from each session agent listed

-t—Append to the end of the command to specify the current time period for the max-burst value.

interface [interface-id][method] - Display SIP interface statistics. Entering this command without any arguments displays whether the SIP interface is in service or not. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view. The show sipd interface command lists:

- Name of the SIP interface
- State - A **D** indicates that the particular SIP interface is disabled and **I** indicates an in service SIP interface. This is the second column, without a label
- Inbound Statistics:
  - Active - number of active sessions sent to each SIP interface listed
  - Rate - average rate of session invitations (per second) sent to each SIP interface listed
  - ConEx - number of times the constraints have been exceeded
- Outbound Statistics:
  - Active - number of active sessions sent from each SIP interface listed
  - Rate - average rate of session invitations (per second) sent from each SIP interface listed
  - ConEx - number of times the constraints have been exceeded
- Latency Statistics:
  - Avg: average latency for packets traveling to and from each SIP interface listed
  - Max: maximum latency for packets traveling to and from each SIP interface listed
- Max Burst: total number of session invitations sent to or received from the SIP interface within the amount of time configured for the burst rate window. You can set the burst-rate-window in session-constraints and also set the corresponding constraint name in the sip-interface.

ip-cac <IP address>—Display CAC parameters for an IP address

publish—Display statistics related to incoming SIP PUBLISH messages

agent <agent>—Display activity for the session agent that you specify

- Inbound Sessions:

Copyright © 2024, 2026, Oracle and/or its affiliates.

Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions

- Num Exceeded—Number of times time constraints were exceeded for inbound sessions Outbound Sessions:
- Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions
- Burst—Number of times burst rate was exceeded for this session agent
- Out of Service—Number of times this session agent went out of service
- Trans Timeout—Number of transactions timed out for this session agent
- Requests Sent—Number of requests sent by way of this session agent
- Requests Complete—Number of requests that have been completed for this session agent
- Messages Received—Number of messages received by this session agent

realm—Display realm statistics related to SIP processing

routers—Display status of Oracle Communications Session Border Controller connections for session router functionality

directors—Display the status of Oracle Communications Session Border Controller connections for session director functionality

<message>—Add one of the following arguments to the end of a show sipd command to display information about that type of SIP message:

- INVITE—Display the number of SIP transactions including an INVITE method
  The INVITE message type also supports the <detail> argument, which displays the data generated when you enable the **response-code-and-phrase** feature in addition to the information displayed without this argument.
- REGISTER—Display the number of SIP transactions including a REGISTER method
- OPTIONS—Display the number of SIP transactions including an OPTIONS method
- CANCEL—Display the number of SIP transactions including a CANCEL method
- BYE—Display the number of SIP transactions including a BYE method
- ACK—Display the number of SIP transactions including an ACK method
- INFO—Display the number of SIP transactions including an INFO method
- PRACK—Display the number of SIP transactions including a PRACK method
- PRECONDITIONS-TRFO—Display Asymmetric preconditions TrFO statistics
- SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method
- NOTIFY—Display the number of SIP transactions including a NOTIFY method
- REFER—Display the number of SIP transactions including a REFER method
- UPDATE—Display the number of SIP transactions including an UPDATE method
- other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers
  The following lists information displayed for each individual SIP message statistic. Some or all of the following messages and events may appear in the output from a show sipd command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- INVITE Requests—Number of times method has been received or sent
- Retransmissions—Information regarding sipd message command requests received by the Oracle Communications Session Border Controller
- 100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located
- 180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user
- 200 OK—Number of times request has succeeded
- 408 Request Timeout—Number of times server could not produce a response before timeout
- 481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction
- 486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls
- 487 Terminated—Number of times request was cancelled by a BYE or CANCEL request
- 4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred
- 503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server
- 5xx Server Error—Number of times the 5xx class of status code appeared
- Response Retrsns—Number of response re-transmissions sent and received
- Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261
- Locally Throttled—Number of locally throttled invites. Does not apply to a server.
  show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

groups—Display cumulative information for all session agent groups on the Oracle Communications Session Border Controller. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the show sipd groups command accesses the sub-commands described in this section, the main show sipd groups command (when executed with no arguments) displays a list of all session agent groups.

groups -v—Display statistics for the session agents that make up the session agent groups that are being reported. The -v (meaning “verbose”) executed with this command must be included to provide verbose detail.

groups <specific group name>— Display statistics for the specified session agent group

endpoint-ip <phone number> —Displays registration information for a designation endpoint entered in the <phone number> argument; also show IMS-AKA data

all—Display all the show sipd statistics listed above

sip-endpoint-ip—See show sipd endpoint-ip

Copyright © 2024, 2026, Oracle and/or its affiliates.

sa-nsep-burst—Display NSEP burst rate for all SIP session agents

subscriptions-by-user—Display data for SIP per user subscribe dialog limit

rate—Displays the transaction rate of SIP messages

codecs—Displays codec usage per realm, including counts for codecs that require a license such as SILK and Opus.

pooled-transcoding—Pooled transcoding information for the client and server User Agents on the A-SBC.

srvcc—SRVCC handover counts including ATCF and EATF sessions.

•

tcp—Displays TCP connection state information for the following

- inbound
- outbound
- listen
- IMS-AKA
- total

tcp connections—Dump TCP connections for analysis. Options include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start display. This can be a negative number. If the number selected for the start variable is greater than the number of TCP connections, nothing will be displayed
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Dump all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

show sipd srg

Run this command to view the current status for all the session recording groups configured in the system.

Syntax

```
show sipd srg
```

This command shows the status from the different servers confirgured in the system. The status can be summarized as:

Table 3-3 Status Description

Status	Description
I	In service
O	out of service
S	Transitioning from out-of-service to in-service

Copyright © 2024, 2026, Oracle and/or its affiliates.

show sipd srs

Run this command to view the current status for all session recording servers configured in the system.

Syntax

```
show sipd srs
```

This command shows the status from the different servers confirgured in the system. The status can be summarized as:

Table 3-4 Status Description

Status	Description
I	In service After a normal configuration, or when ping is enabled and a response is obtained, then the SRS status is in-service.
O	Out of service If OPTIONS ping is enabled but not responded then SRS will be marked as out-of-service. When an SRS is out-of-service, and the OPTIONS ping is responded back, then for a small duration the SRS remains in the transitioning state.
S	Transitioning from an out of service status to an in service status. When the SRS is out-of-service and the OPTIONS ping is responded back, then for a small amount of time the SRS remains in the transitioning state - S.

show sipd siprec <message>

Run this command to view information about a specific type of SIP message related to all SIPREC sessions towards SRS.

Syntax

```
show sipd siprec <message>
```

The `<message>` parameter in the command can take any one of the following values:

Table 3-5 Message Parameter

Parameter	Description
ACK	Display the number of SIP transactions including an ACK method
BYE	Display the number of SIP transactions including a BYE method
CANCEL	Display the number of SIP transactions including a CANCEL method

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) Message Parameter

Parameter	Description
INVITE	Display the number of SIP transactions including the INVITE method
OPTIONS	Display the number of SIP transactions including an OPTIONS method
other	Display the number of SIP transactions including non-compliant methods and protocols used by specific customers.

This table lists the information displayed for each SIP message statistic. Some or all of the messages and events may appear in the output using a `show sipd siprec` command.

Table 3-6 Statistics Displayed

Statistic or Message	Description
200 OK	Number of times the request has succeeded.
408 Request Timeout	Number of times the server could not produce a response before timeout.
487 Terminated	Number of times a request was cancelled by a BYE or CANCEL request
4xx Client Error	Number of times the 4xx class of status code appeared for cases where the client seems to have erred
503 Service Unavail	Number of times the server was unable to handle the request due to a temporary overloading or maintenance of the server
5xx Server Error	Number of times the 5xx class of status code appeared
Message Requests	The number of requests for a SPECIFIC message type
Retransmissions	Information regarding sipd message command requests received by the SBC
Transaction Timeouts	Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261

show sipd siprec errors

Run this command to view errors related to the SIP media event.

Syntax

```
show sipd siprec errors
```

The table lists descriptions for all errors that are displayed in the output:

Copyright © 2024, 2026, Oracle and/or its affiliates.

Table 3-7 SIP Media Event Related Errors

Error	Description
Drop Media Errors	Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog or session; or c) a BYE initiated by the system due to a timeout notification from MBCD. For example,500 error response to INVITE.
SDP Answer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/ Answer model (RFC 3264). For example, steering pool ports not available on receiving answer. This can be achieved by configuring only one steering pool on uas side realm, and in answer send two m-lines , it will fail as no steering ports are there.
SDP Offer Errors	Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264). For example, steering pool ports not available on receiving offer.

show snmp-community-table

Syntax

```
show snmp-community-table
```

The show snmp-community-table command displays all information for configured SNMP communities including request and responses for each community.

Example

```
ORACLE# show snmp-community-table
```

show snmp-info

Syntax

You can view summary SNMP agent run-time configuration and statistical packet-count information by using this command with no additional parameters.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> All arguments of this command display run-time configuration information.

```
show snmp-info [addresses | all | groups | statistics | summary | users |
views]
```

Arguments

- **addresses**—Display device IP addresses, their subnet mask entries and request, reply, and trap counters.
- **all**—Display detailed system-level SNMPv3 counters.
- **groups**—Display user group entries.
- **statistics**—Display SNMP agent statistics and device SNMP IP address entry statistics.
- **summary**—SNMPv3 agent information.
- **users**— Display SNMP user entries and statistics.
- **views**—Display SNMP view entries.

Release

Initial release: S-CX8.1.0

show spl

The show spl command displays the version of the SPL engine, The filenames and version of the SPL plugins currently loaded on the Oracle Communications Session Border Controller, The signature state of each plugin , The system tasks that each loaded plugin interacts with, enclosed in brackets.

show spl <task> — command displays SPL file information including the signature state.

show support-info

Syntax

```
show support-info [custom | standard | media | signaling] [config] [file-only]
```

This command allows you to gather a set of information commonly requested by Oracle Support.

Arguments

custom — Display information in the /code/supportinfo.cmds file to determine what commands should be encompassed. If the file does not exist, then the system notifies you.

standard — Display information for all commands the show support-info command encompasses.

media — Display and write out only the show media commands to the log file.

Copyright © 2024, 2026, Oracle and/or its affiliates.

signaling — Display and write out all commands and exclude the show media commands to the log file.

config — Optionally add the show running-config output to the output of the standard arguments.

file-only—Optionally disable the output of commands to stdout and append to the `support-info.log` file.

Example

```
ORACLE# show support-info standard
```

show system-state

Syntax

```
show system-state
```

Displays the system state based on the latest setting of the set-system-state command.

Example

```
ORACLE# show system-state
```

show tacacs

Syntax

```
show tacacs stats
```

Displays statistics related to communications between the Oracle Communications Session Border Controller and configured TACACS servers, including:

- number of ACLI commands sent for TACACS+ accounting
- number of successful TACACS+ authentications
- number of failed TACACS+ authentications
- number of successful TACACS+ authorizations
- number of failed TACACS+ authentications
- the IP address of the TACACS+ daemon used for the last transaction

show temperature

Syntax

```
show temperature
```

Displays the temperature in Celsius for all given components with temperature sensors.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show temperature
```

show timezone

Syntax

```
show timezone
```

This command displays the information set with the **timezone-set** command including the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time.

The **show timezone** command also displays the DST settings. If rules-based DST configuration is used, the Oracle Communications Session Border Controller converts the rule into the absolute DST start or end time for the current year.

Example

```
ORACLE# show timezone
America/New_York
```

show trap-receiver

Syntax

```
show trap-receiver
```

The **show trap-receive**r command displays trap receiver information for each configured SNMP community. An IPv6 address is valid as a parameter.

Example

```
ORACLE# show trap-receiver <IP-address>
```

show uptime

Syntax

```
show uptime
```

The show uptime command displays information about the length of time the system has been running in days, hours, minutes, and seconds, as well as the current date and time information.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> When polled via SNMP, uptime is represented in a 32-bit value. After 497 days, 10 hours, 27 minutes, the SNMP value resets even though the system does not experience a reboot. The `show uptime` command does not have this limitation.

Example

```
ORACLE# show uptime
```

show users

Syntax

```
show users [detail]
```

The show users command displays all users currently logged into the Oracle Communications Session Border Controller by index number. Other display information includes:

- Index Identifier
- remote IP address
- IdNumber
- Duration of connection
- Connection Type
- State
  - * denotes the current connection
  - C denotes the user has the configuration lock
- User

Example

```
ORACLE# show users
```

show version

Syntax

```
show version [image | boot]
```

The show version command shows the OS version information including: the OS version number, the date that the current copy of the OS was made, and other information.

Arguments

image — Displays kernel information and boot parameters.

Copyright © 2024, 2026, Oracle and/or its affiliates.

boot — Displays bootloader version, BIOS detail, and mainboard information, including serial number.

Example

```
ORACLE# show version
```

show virtual-interfaces

Syntax

```
show virtual-interface
```

The show virtual-interface command shows the virtual interfaces forOracle Communications Session Border Controller signaling services; for example, SIP-NAT external address and H.323 interface (stack) IP interface.

Example

```
ORACLE# show virtual-interfaces
```

show voltage

Syntax

```
show voltage
```

Displays current operating voltages for components in the Oracle Communications Session Border Controller.

Mode

User and Superuser

Example

ORACLE# show voltage

show wancom

Syntax

```
show wancom
```

Displays negotiated duplex mode and speed for all Oracle Communications Session Border Controller system control interfaces.

Mode

User and Superuser

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# show wancom
```

show xcode

Syntax

```
show xcode [api-stats | dbginfo | dsp-events | load | session-all | session-
bitinfo | session-byattr | session-byid | session-byipp | session-config |
xlist | codecs]
```

Displays transcoding hardware statistics and operating information. Commands of note:

show xcode load—Displays currently used transcoding resources.

show xcode codecs—Displays counts of codec pairs (and ptime transrating) in use.

Mode

User and Superuser

spl

Syntax

```
spl save acli encr-surrogate-passwords
```

```
spl start acli [ show | wizard ] [ entitlements | product ]
```

Arguments

- **encr-surrogate-passwords**—Encrypt the surrogate-agent password.
  This command is obsolete because this is the default behavior in the latest version of all supported releases.
- **show entitlements**—Display the entitlements.
  This is identical to the command **show entitlements**.
- **wizard product**—Start the wizard that selects the product.
  This is identical to the command **setup product**.
- **wizard entitlements**—Start the wizard that selects the entitlements.
  This is identical to the command **setup entitlements**.

Mode

Superuser

Example

```
ORACLE# spl start acli show entitlements
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

ssh-key

The ssh-key command allows you to import, generate, display and delete public keys on the Oracle Communications Session Border Controller.

Syntax

```
ssh-key <key type> <action> <other parameters>
```

Arguments

Supported key types:

authorized-key
Manage the keys of SSH clients who connect using public key authentication.
Supported actions:

export <name>
Export an authorized key in RFC 4716 format.

import <name> <class>
Import an authorized key in RFC 4716 format. The `<class>` parameter may be either `user` or `admin`.

delete <name>
Delete an authorized key that was previously imported.

known-host
Manage the known hosts for when the SBC acts as an SSH client.
Supported actions:

import <name>
Import a key in RFC 4716 format into the known_hosts file.
The <name> parameter is the IP address or hostname of the SFTP server.

delete <name>
Delete a key from the known_hosts file.
The <name> parameter is the IP address or hostname of the SFTP server.

private-key
Manage the private key of the SBC
Supported actions:

generate [rsa | dsa] [<size>]
Regenerate the RSA or DSA public and private key of the SBC.
RSA key size may be 2048, 3072, or 4096. The default value of 2048 is used if no size is selected.
DSA key size is always set to 1024.

ca-key
Manage the certificate authority keys.
Supported actions:

Copyright © 2024, 2026, Oracle and/or its affiliates.

import <key-name> <class>
Import a CA key in RFC 4716 format. The `<class>` parameter may be either `user` or `admin`.

delete <key-name>
Delete a key from the known_hosts file.

ca-user-revoke
Manage certificate authority user revocation. Users are added to the revocation list by importing their public key.
Supported actions:

import <key-name>
Import the public key of the user or users who are authorized with this ca-key. Or import the public key of a CA to revoke all keys signed by that CA.

delete <key-name>
Remove a key-name from the revocation list.

x509
Manage certificates for OCSP-based authentication of SSH clients.

> **Note**
>
> Requires Admin Security entitlement and FIPS entitlement.

Supported actions:

import <login-name> <ocsp-server> <class>
Import the end-entity certificate and certificate chain for an SSH client. The login-name should match the username that the SSH client uses to authenticate; the ocsp-server should be the FQDN of the OCSP server; and the class parameter may be either `user` or `admin`.

delete <login-name>
Remove the end-entity certificate and certificate chain for an SSH client.

Mode

Superuser

Example

```
ORACLE# ssh-key authorized-key import jdoe
```

stack

The stack <task> command is not supported in this release.

start learned-allowed-elements

The start learned-allowed-elements command begins the Oracle Communications Session Border Controller to analyze traffic and create an allowed-elements-profile configuration element to match and pass that traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
start learned-allowed-elements [method] [msg-type] [params]
```

Arguments

Entered without any arguments, the system captures and parses all messages sent through to create an allowed-elements-profile, based on headers only.

method—Adding this argument writes out rule set information that includes message method criteria.

msg-type—Adding this argument writes out rule set information that includes message type criteria, including any, request, or response.

params—Adding this argument writes out rule set information that includes header parameter criteria, that appears in the header-rules subelement.

Mode

Superuser

stop-task

The stop-task command shuts down a specified task.

Syntax

```
stop-task <task>
```

Arguments

<task> Enter a task name or task ID

> **Note**
>
> Use this command with caution as there is no direct way to restart a task without rebooting the Oracle Communications Session Border Controller.

Mode

Superuser

Example

```
ORACLE# stop-task sipd
```

stop learned-allowed-elements

The stop learned-allowed-elements command stops the Oracle Communications Session Border Controller from analyzing traffic and closes all created configuration elements. You must then perform a save and activate for created elements to be saved to the running config

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
stop learned-allowed-elements <configuration name>
```

Arguments

<configuration-name>—Enter a name that will become the allowed-elements-profile configuration name that reflects passing the traffic captured during the start learned-allowed-elements task.

Mode

Superuser

switchover-redundancy-link

The switchover-redundancy-link command allows you to switchover the physical interface to standby in a redundant link configuration.

arguments

<slot> Select the slot number to switchover the link from active to standby.

- Values 1 | 2

Mode

Superuser

Example

```
ORACLE# switchover-redundancy-link 2
```

synchronize

The synchronize command is used to synchronize files across HA nodes.

arguments

lrt <filename>—Synchronizes specific file from the /code/lrt directory.

lrt <path><filename>—Synchronize Local Routing Tables (LRT) files between active and standby (e.g. synchronize lrt /code/lrt/filename.xml).

Mode

Superuser

systime-set

The systime-set command sets the system clock.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
systime-set
```

> **Note**
>
> The systime-set command prompts the user for the date and time and updates the system clock. The command will not set the system time if an invalid year, month, or day is entered. Attempting to change the date and time on the Oracle Communications Session Border Controller displays a warning message as use of this command could be service affecting.

Mode

Superuser

Example

```
ORACLE# systime-set
```

tail-logfile-close

The tail-logfile-close command ends the echoing of a process's logfile to the screen as initiated by the tail-logfile-open command.

Syntax

```
tail-logfile-close <process> [<logfile>]
```

Arguments

<process> — Enter the name of the process that is writing to the specified logfile.

<logfile> — Enter the logfile's name that you want to stop being echoed to the screen. This argument is optional.

> **Note**
>
> Must be a valid logfile that is currently being written to.

Mode

Superuser

Example

```
ORACLE# tail-logfile-close sipd
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

tail-logfile-open

The tail-logfile-open command displays all messages on the console that are normally written to a specified logfile. As a message is written to the logfile, it is also displayed on the screen. The specified logfile will continue to be updated on the Oracle Communications Session Border Controller's filesystem.

Syntax

tail-logfile-open <process> [<logfile>]

Arguments

<process> — Enter the name of the process that is writing to the specified logfile

<logfile> Enter an alternate logfile's name for which you want new entries echoed to the console screen. Not entering the logfile argument forces the default log for the named process to be displayed on the screen. This argument is optional.

Mode

Superuser

> **Note**
>
> Must be a valid logfile that is currently being written to. The level of detail displayed on the screen is related to the loglevel of the process.

Example

```
ORACLE# tail-logfile-open sipd
```

tcb

The tcb command displays task control block (TCB) information for a particular task.

Syntax

```
tcb <task>
```

> **Note**
>
> This command returns a pointer to the TCB for a specified task. Although all task state information is contained in the TCB, you must not modify it directly. This command is used only for debugging purposes.

Arguments

<task> — Enter a task name or task ID

Copyright © 2024, 2026, Oracle and/or its affiliates.

Mode

Superuser

Example

```
ORACLE# tcb sipd
```

test-audit-log

The test-audit-log command allows the user to test audit log functionality.

Arguments

<log-msg> Enter the audit log string to be written into the audit file

Syntax

```
test-audit-log <log-msg>
```

Mode

Superuser

Example

```
ORACLE# test-audit-log log1
```

test-pattern-rule

The test-pattern-rule command allows you to test header manipulation pattern rules for expression validation.

Arguments

<expression> Enter the regular expression that you want to test. The Oracle Communications Session Border Controller informs you whether or not there is a match.<string> Enter the string against which you want to compare the regular expression<show> View the test pattern you entered, whether there was a match, and if so, the number of matches<exit> End the test User

Mode

User

Example

```
ORACLE# test-pattern-rule expression '.*;tgid=(.+).*'
```

> **Note**
>
> This command exists both as a command and as a configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

test-policy

The test-policy element tests and displays local policy routes from the ACLI.

Parameters

source-realm
Enter the name set in the source-realm field of a configured local policy. Entering an “*” in this field matches for any source realm. Leaving the field empty indicates that only the “global” realm will be tested.

from-address
Enter the “from” address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

to-address
Enter the “to” address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

time-of-day
Enable or disable use of the time of day value set in the start-time and end-time fields you set in configured local-policy elements

- Values: enabled | disabled

carriers
Enter the names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma separated text strings enclosed in quotation marks.

media-profile
Enter a list of media profiles

show
Show the next hop and the associated carrier information for all routes matching the “from” and “to” addresses entered

Path

test-policy is available under the session-router path.

Notes

Type the show command to perform the actual test lookup after parameters have been entered.

The test-policy element can also be configured in Superuser mode as a command.

test-translation

The test-translation command is used to test translation rules configured for the address translation feature. This command is also found in the session-router path. Details on its use are found in the Configuration Elements N-Z chapter.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Syntax

```
test-translation <argument>
```

Arguments

<argument> The following is a list of test-translation arguments:

- Values :
  - called-address—Enter the address on which the called rules are be applied. This entry is required.
  - calling-address—Enter the address on which the calling rules will be applied. This entry is required.
  - show—Show results of translation
  - translation-id—Enter translation rules to test
  - exit—Exit the test translationUser

Mode

User

Example

```
ORACLE# test-translation show
```

timezone-set

The timezone-set command sets the time zone and daylight savings time on the Oracle Communications Session Border Controller.

Syntax

```
timezone-set
```

> **Note**
>
> The timezone-set command prompts the user for time zone, UTC offset, and daylight saving time information. If daylight savings time for your time zone changes start and stop dates yearly, this command must be set yearly.

Mode

Superuser

Example

```
ORACLE# timezone-set
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

If you need to exit the **timezone-set** command before completing it, use the key sequence **Ctrl-D**.

Traceroute Command Specifications

The traceroute command traces the route of an IP packet to an Internet host by sending probe packets with small maximum time-to-live (TTL) values and listening to responses from gateways along the path. This diagnostic command provides the route (path) and the round trip times of packets received from each host in a route.

The traceroute command works by sending probe packets starting with a maximum time-to-live (TTL) value of one, listening for an ICMP error message in response to the TTL expiry, and recording the source that sent it. This process is repeated by incrementing the TTL value by 1 each time until the final destination is reached. This information allows the path to be traced for the packet to reach its destination.

Syntax

```
traceroute <destination-address> <options>
```

Arguments

<destination-address> — Specifies the destination IP address for the route to be traced.

<intf-name:vla> — Specifies the network interface and VLAN to use.

<max_ttl> — Specifies the maximum number of hops before timeout.

- Default — 30
- Values — Min: 1 / Max: none

<probes> — Specifies the number of probes to send.

<source-ip> — Specifies the source IP address from which to trace the route to the destination IP address.

<timeout> — Specifies the maximum time (in seconds) to wait for a response.

- Default — 3
- Values — Min: 1 / Max: none

Mode

Superuser

Example

```
ORACLE# traceroute 172.30.0.167 probes 4
traceroute to 172.30.0.167
1 172.44.0.1 (0.669003 ms) (2.140045 ms) (2.290964 ms) (2.40891 ms)
2 172.30.0.167 (0.25602 ms) (0.219822 ms) (0.604868 ms) (0.398874)
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

unmount

The mount command stops the file system from running. Unmounting the file system is required to resize user partitions or replace a storage device.

Syntax

```
unmount <data-disk | system-disk | hard-disk>
```

Arguments

data-disk— Mount the 1 or more data partitions containing the default (/mnt/sys and /mnt/app) or user-defined volumes

system-disk—Mount 2 system partitions: /opt and /opt/crash

hard-disk—Mounts both the system partition and data partition

Mode

Superuser

verify-config

The verify-config command verifies the Oracle Communications Session Border Controller's current configuration. The verify-config command checks the consistency of configuration elements that make up the current configuration and should be carried out prior to activating a configuration on the Oracle Communications Session Border Controller.

Syntax

```
verify-config
```

Mode

Superuser

Notes

The verify-config command, entered either directly or via the save-config command, checks for address duplication for a given network-interface within a configuration. Addresses are checked for duplication based on the following criteria:

- Every address entered is checked against the Primary and Secondary Utility addresses
- All UDP, TCP, and TFTP addresses are checked against other UDP, TCP, and TFTP addresses respectively within the same port range

> **Note**
>
> For detailed information, refer to the Maintenance and Troubleshooting Guide.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE# verify-config
```

watchdog

The watchdog command sets or queries the state of the watchdog timer. If the system becomes unstable causing the watchdog timer to not reset, the system reboots.

Syntax

```
watchdog <arguments>
```

Arguments

<arguments> The following is a list of valid arguments:

- Values:
  - enable—Enable the watchdog timer
  - disable—Disable the watchdog timer
  - fetch—Display the watchdog timer configuration

> **Note**
>
> The fetch argument can be accessed from user mode.

Mode

User

Example

```
ORACLE# watchdog enable
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

4

ACLI Configuration Elements A-M

access-control

The access-control configuration element is used to manually create ACLs for the host path in the Oracle Communications Session Border Controller.

> **Note**
>
> The access-control configuration object is partially supported by RTC. You can add and delete static ACLs without rebooting. Modifying existing static ACLs or fixing configuration typos, however, require a reboot.

Parameters

realm-id
Enter the ingress realm of traffic destined to host to apply this ACL

description
Provide a brief description of the access-control configuration element

destination-address
Enter the destination address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. This parameter is entered in the following format: <ip-address>[/<num-bits>] [:<port>][/<port-bits>]

- Default: 0.0.0.0

An IPV6 address is valid for this parameter. But when you set the source-address and destination-address parameters in the access-control configuration, you use a slightly different format for IPv6 than for IPv4.
Since the colon (:) in the IPv4 format leads to ambiguity in IPv6, your IPv6 entries for these settings must have the address encased in brackets ([]). For example, [7777::11]/64:5000/14. In addition, IPv6 entries are allowed up to 128 bits for their prefix lengths

source-address
Enter the source address, net mask, port number, and port mask to specify traffic matching for this ACL. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address. This parameter is entered in the following format: <ip-address>[/<num-bits>] [:<port>][/<port-bits>]

- Default: 0.0.0.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Oracle recommends that you avoid creating static ACLs using the source address 0.0.0.0 unless explicitly directed to so. Static ACLs using source address 0.0.0.0 can conflict with internally created ACLs (Realm based default global ACLs) that also use source-address 0.0.0.0. If you create these static ACLs, the system may drop traffic or experience unpredictable behavior after you delete them and may require a reboot to resume forwarding that traffic.

An IPV6 address is valid for this parameter. But when you set the source-address and destination-address parameters in the access-control configuration, you use a slightly different format for IPv6 than for IPv4.
Since the colon (:) in the IPv4 format leads to ambiguity in IPv6, your IPv6 entries for these settings must have the address encased in brackets ([]). For example, [7777::11]/64:5000/14. In addition, IPv6 entries are allowed up to 128 bits for their prefix lengths

application-protocol
Select the application-layer protocol configured for this ACL entry

- Values: SIP | H323 | MGCP | DIAMETER | NONE

> **Note**
>
> If application-protocol is set to none, the destination-address and port will be used. Ensure that your destination-address is set to a non-default value (0.0.0.0.)

transport-protocol
Select the transport-layer protocol configured for this ACL entry

- Default: ALL
- Values: UDP | TCP | SCTP | ALL

access
Select the access control type for this entry

- Default: permit
- Values:
  - permit—Puts the entry in trusted or untrusted list depending on the trust-level parameter. This gets promoted and demoted according to the trust level configured for the host.
  - deny—Puts this entry in the deny list.

average-rate-limit
On hardware platforms that are not the Acme Packet 1100 or the Acme Packet 3900, enter the allowed sustained rate in bytes per second for host path traffic from a trusted source within the realm. A value of 0 disables the policing.

- Default: 0
- Values: Min: 0 / Max: 4294967295

On virtual platforms, enter the allowed sustained rate as a percentage of the maximum signaling rate for host path traffic from a trusted source within the realm. A value of 0 disables the policing.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 0 / Max: 100

trust-level
Select the trust level for the host

- Default: None
- Values:
  - none—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to deny list
  - low—Hosts can be promoted to trusted-list or can get demoted to deny-list
  - medium—Hosts can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in deny-list.
  - high—Hosts always remain trusted

minimum-reserved-bandwidth
Enter the minimum reserved bandwidth in bytes per second that you want for the session agent, which will trigger the creation of a separate pipe for it. This parameter is only valid when the trust-level parameter is set to high. Only a non-zero value will allow the feature to work properly.

- Default: 0
- Values: Min: 0 / Max: 4294967295

invalid-signal-threshold
Enter the rate of signaling messages per second to be exceeded within the tolerance-window that causes a demotion event. This parameter is only valid when trusted-level is configured as low or medium. A value of 0 means no threshold.

- Default: 0
- Values: Min: 0 / Max: 4294967295

maximum-signal-threshold
Enter the maximum number of signaling messages per second that one host can send within the tolerance-window. The host will be demoted if the Oracle Communications Session Border Controller receives messages more than the configured number. This parameter is only valid when trusted-level is configured low or medium. A value of 0 means no threshold.

- Default: 0
- Values: Min: 0 / Max: 999999999

untrusted-signal-threshold
Enter the maximum number of signaling messages from untrusted sources allowed within the tolerance window.

- Default: 0
- Values: Min: 0 / Max: 999999999

deny-period
Enter the time period in seconds a deny-listed or deny entry is blocked by this ACL. The host is taken out of deny-list after this time period elapses.

- Default: 30

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 / Max: 999999999

nat-trust-threshold
Enter maximum number of denied endpoints that set the NAT device they are behind to denied. 0 means dynamic demotion of NAT devices is disabled.

- Default: 0
- Values: Min: 0 | Max: 65535

max-endpoints-per-nat
Maximum number of endpoints that can exist behind a NAT before demoting the NAT device.

- Default: 0 (disabled)
- Values: Min: 0 | Max: 65535

nat-invalid-message-threshold
Enter the acceptable number of invalid messages from behind a NAT.

- Default: 0
- Values: Min: 0 | Max: 65535

cac-failure-threshold
Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue.

- Default: 0
- Values: Min: 0 / Max: 4294967295

untrust-cac-failure-threshold
Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue.

- Default: 0
- Values: Min: 0 / Max: 4294967295

Path

access-control is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **access-control**.

> **Note**
>
> This is a multiple instance configuration element.

account-config

The account-config configuration element allows you to set the location where accounting messages are sent.

Parameters

hostname
Enter the hostname of this SBC; must be set to “localhost” or the accounting configuration does not work properly.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: Localhost name

port
Enter the UDP port number from which RADIUS messages are sent

- Default: 1813
- Values: Min: 1025 / Max: 65535

strategy
Select the strategy used to select the current accounting server

- Default: Hunt
- Values:
  - hunt—Selects accounting servers in the order in which they are listed
  - failover—Uses first and subsequent servers in accounting server list until a failure is received from that server
  - roundrobin—Selects accounting server in order, distributing the selection of each accounting server evenly over time
  - fastestrtt—Selects accounting server with the fastest RTT observed during transactions with the servers
  - fewestpending—Selects accounting server with the fewest number of unacknowledged accounting messages

protocol
Set the type of message protocol type for accounting CDRs.

- Default: radius
- Values: radius | diameter

state
Enable or disable the accounting system

- Default: enabled
- Values: enabled | disabled

dns-realm
The realm where the DNS server from which the system can obtain resolutions to an FQDN hostname for a Diameter server.

max-msg-delay
Enter the time in seconds the SBC continues to send each accounting message

- Default: 60
- Values: Min: 0 / Max: 4294967295

max-wait-failover
Enter the number of accounting messages held in message waiting queue before a failover situation status is enacted

- Default: 100
- Values: Min: 1/ Max: 4096

Copyright © 2024, 2026, Oracle and/or its affiliates.

trans-at-close
Enable the SBC to transmit accounting message information at the close of a session only. Setting this parameter to disabled tells the SBC to transmit accounting information at the start of a session (Start), during the session (Interim), and at the close of a session (Stop).

- Default: disabled
- Values: enabled | disabled

generate-start
Select the type of SIP event that triggers the SBC to transmit a RADIUS Start message

- Default: ok
- Values:
  - none—RADIUS Start message is not generated
  - ""—When two quotation marks are entered next to each other (empty), behavior is identical to none value
  - start—RADIUS Start message should not be generated
  - invite—RADIUS Start message is generated once a SIP session INVITE is received
  - ok—RADIUS Start message is generated an OK message in response to an INVITE is received

generate-interim
SBC to transmit a RADIUS Interim message

- Default: reinvite-response
- Values:
  - OK—RADIUS Start message is generated when an OK message is received in response to an INVITE
  - Reinvite—RADIUS Interim message is generated when a SIP session reINVITE message is received
  - Reinvite-Response—RADIUS Interim message is generated when a SIP session reINVITE is received and the system responds to it
  - Reinvite-Cancel—RADIUS Interim message is generated when a SIP session reINVITE is received, and the Reinvite is cancelled before the SBC responds to it
  - Unsuccessful-Attempt—RADIUS Interim message is generated when a session set-up attempt from a preference-ordered list of next-hop destinations is unsuccessful. This can happen when a local policy lookup, LRT lookup, ENUM query response, or SIP redirect returns a preference-ordered list of next-hop destinations. The interim message contains: the destination IP address, the disconnect reason, a timestamp for the failure, and the number that was called
  - Egress-Invite—Sends additional Interim message is generated when applicable VoLTE and WiFi INVITEs egress the system

generate-event
Enter one or more valid events that prompt creation of an Event record. Current valid values are register and local-register. Multiple values are entered enclosed in parenthesis and separated by spaces.

- Default:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: register | local-register | message

file-output
Enable or disable the output of comma-delimited CDRs

- Default: disabled
- Values: enabled | disabled

file-path
Enter the path in which to save the comma-delimited CDR file. The default path is /opt/cdr. Do not use the /opt/logs directory. You cannot set this parameter to the /code or /boot directories.

max-file-size
Set the maximum file size in bytes for each CDR file

- Default: 1000000
- Values: Min: 1000000 / Max: 100000000

max-files
Set the maximum number of files to store on the SBC. The parameter's value range is from 0 to unlimited. The user should consider the **max-file-size** setting and available space to specify this value.

- Default: 5

file-sequence-number
When enabled, the system assigns a 9 digit file sequence number to append to a CDR file.

- Default: disabled
- enabled

file-compression
Enable or disable compression of CDR files; when enabled, comma-delimited CDR files are zipped on the backup device to maximize storage space

- Default: disabled
- Values: enabled | disabled

file-rotate-time
Set the time in minutes that the SBC rotates the CDR files; the SBC will overwrite the oldest file first

- Default: 0
- Values: Min: 0 / Max: 2147483647

file-delete-alarm
Enable or disable the raising of an alarm when CDR files are deleted due to lack of space.

- Default: disabled
- Values: enabled | disabled

ftp-push
Enable or disable the FTP push feature.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

ftp-address
Enter the IP address for the FTP server used with the FTP push feature.

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

ftp-port
Set the TCP port on the FTP server to use with the FTP push feature

- Default: 21
- Values: Min: 1 / Max: 65535

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

ftp-user
Enter the username the Oracle Communications Session Border Controller will use to log in to the FTP server.

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

ftp-password
Enter the password the Oracle Communications Session Border Controller will use to log in to the FTP server.

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

ftp-remote-path
Enter the file path the SBC will use to work in on the FTP server.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

ftp-strategy
Set the strategy for the SBC to use when selecting from multiple push receivers.

- Default: hunt
- Values:
  - hunt—The SBC selects the push receiver from the available list according to the priority level
  - failover—The SBC selects the push receiver based on priority level and continues to use that same push receiver until it fails over
  - roundrobin—The SBC selects push receivers systematically one after another, balancing the load among all responsive push receivers
  - fastestrtt—The SBC selects the push receiver based on best average throughput. For this situation, throughput is the number of bytes transferred divided by the response time. The system uses a running average of the five most recent throughput values to accommodate for network load fluctuations

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

intermediate-period
Set the time interval used to generate periodic interim records during a session

- Default: 0
- Values: Min: 0 / Max: 2147483647

interim-stats-id-types
A space separated field comprising interim stats correlation ID.

- Default: none
- Values: none | calling | called | session

account-servers
Access the account-server subelement

cdr-output-redundancy
Enable or disable the redundant storage of comma-delimited CDR files. The standby-push value ensures consistent and accurate CDR collection in the event of a failover.

- Default: enabled
- Values: enabled | disabled | standby-push

Copyright © 2024, 2026, Oracle and/or its affiliates.

ftp-max-wait-failover
Enable or disable the prevention of duplicate accounting attributes

- Default: 120
- Values: Min: 1 / Max: 4096

> **Note**
>
> This parameter is deprecated and is only used if no **account-config > push-receiver** configuration element has been defined. All new push receivers must be defined in the **account-config > push-receiver** configuration element.

prevent-duplicate-attrs
Enable this parameter to prevent the SBC from duplicating attributes in the accounting records it generates. This duplication can be caused, for example, by multiple media sessions within the context of a call. Retaining the default (disabled) allows the SBC to include duplicate attributes in RADIUS, Diameter and Local accounting records. This can result in attribute placement and counts that are less consistent.

- Default: disabled
- Values: enabled | disabled

vsa-id-range
Enter the range of accounting attributes to include in CDRs. A blank field means this feature is turned off and all attributes are included.

cdr-output-inclusive
Enable or disable the guarantees placement of attributes in CSV files used for local CDR storage and FTP push

- Default: disabled
- Values: enabled | disabled

push-receiver
Access the push-receiver subelement.

watchdog-ka-timer
Sets the value in seconds that the SBC waits between sending DWRs.

- Default: 0
- Values: 0,6-65535

msg-queue-size
Sets the message queue sizefor both RADIUS and Diameter accounting interfaces.

- Default: 5000
- Values: 5000-150000

diam-srvc-ctx-ext
Value to substitute in the extension portion of the Service-Context-ID AVP value. This value can be any string.

diam-srvc-ctx-mnc-mcc
Value to substitute in the MNC.MCC portion of the Service-Context-ID AVP value. This value must follow the NUM1.NUM2 format.

Copyright © 2024, 2026, Oracle and/or its affiliates.

diam-srvc-ctx-rel
Value to substitute in the release portion of the Service-Context-ID AVP value. This value can be any number>=1.

diam-acme-attr-id-range
The range of Acme-specific AVP's to include in ACR messages.

max-acr-retries
The maximum number of times that the SBC can resend an ACR for a session.

- Default: 0
- Values: 0 - 4

acr-retry-interval
The time in seconds for the SBC to wait before resending an ACR for a session.

- Default: 10
- Values: 5 - 20

acr-buffer-upper-threshold
The upper threshold for the ACR buffer after which the SBC will select an alternate server.

- Default: 90
- Values: 0 - 100

acr-buffer-lower-threshold
The lower threshold for the ACR buffer which, when reached, the SBC will select the primary server again.

- Default: 70
- Values: 0 - 100

maintain-ccf-affinity
Enable an affinity between ACRs and CCFs so that all ACRs within a single session are sent to the same CCF (unless it goes down).

- Default: disabled
- Values: enabled | disabled

send-disconnect-peer-msg
Enable or disable sending the disconnect message to a peer.

- Default: disabled
- Values: enabled | disabled

next-priority-selection-interval
The time interval in minutes between routing the new call session to the next lower priority CCF after the first switch.

- Default: 0
- Values: 0 - 60

Path

account-configis an element of the session-router path. The full path from the topmost ACLI prompt is. **configure terminal**, and then **session-router**, and then **account-config**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This is a single instance configuration element.

account-config > account-servers

The account-server configuration subelement stores the accounting server information for the account-config.

Parameters

hostname
Enter the hostname of the accounting server. This entry can be an IP Address for Diameter or RADIUS servers, or an FQDN for Diameter servers.

fqdn-pool-type
Identify whether the resolution(s) to this server's hostname belong to the primary pool or the secondary pool of diameter server(s). This setting only applies to diameter servers with an FQDN hostname. The system uses the primary pool for diameter server access. The system uses the secondary pool if all servers in the primary pool are unavailable.

- Default: primary
- Values: primary | secondary

port
Enter the UDP port number associated with the accounting server is configured here

- Default: 1813
- Values: Min: 1025 / Max: 65535

state
Enable or disable this account-server

- Default: enabled
- Values: enabled | disabled

min-round-trip
Enter the time in milliseconds of the minimum RTT for an accounting message for use with the fastest RTT strategy method

- Default: 250
- Values: Min: 10 / Max: 5000

max-inactivity
Enter the maximum time in seconds the Oracle Communications Session Border Controller waits when accounting messages are pending without a response before this account server is set as inactive for its failover scheme

- Default: 60
- Values: Min: 1 / Max: 300

Copyright © 2024, 2026, Oracle and/or its affiliates.

restart-delay
Enter the time in seconds the Oracle Communications Session Border Controller waits after declaring an accounting server inactive before resending an accounting message to that same accounting server

- Default: 30
- Values: Min: 1 / Max: 300

bundle-vsa
Enable or disable the bundling of the VSAs within RADIUS accounting on the account-server

- Default: enabled
- Values: enabled | disabled

secret
Enter the secret passed from the account-server to the client server; entries in this field must follow the Text Format

NAS-ID
Enter the value the account-server uses to identify the Oracle Communications Session Border Controller so messages can be transmitted; entries in this field must follow the Text Format

priority
Enter the number corresponding to the priority for this account server to have in relation to the other account servers to which you send traffic. The default is 0, meaning there is no set priority.

- Default: 0
- Values: Min: 0

diameter-out-manip
Specifies the diameter manipulation to be applied to outbound traffic from this Oracle Communications Session Border Controller.

diameter-in-manip
Specifies the diameter manipulation to be applied to inbound traffic from this Oracle Communications Session Border Controller.

watchdog-ka-timer
Specifies the interval in seconds for watchdog/keep-alive messages. This is the time in which the Oracle Communications Session Border Controller must receive a COPS-KA message from the policy server to ensure collection is still valid.

- Default: 0
- Values: Min: 6 / Max: 65535

domain-name-suffix
Sets the suffix for Origin-Realm and Origin-Host AVPs that have a payload string constructed as a domain name. If your entry does not include the dot, the system prepends one.

origin-realm
Specifies the originating realm of DIAMETER accounting request.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

account-server is a subelement of the account-config element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **account-config** , and then **account-servers**.

> **Note**
>
> This list can contain as many accounting servers as necessary. By default, this list remains empty. RADIUS will not work unless an account server is configured. This is a multiple instance configuration element.

account-config > push-receiver

You can configure multiple CDR push receivers for use with the FTP push feature.

Parameters

server
Set the IP address of the SFTP server to which you want the Oracle Communications Session Border Controller to push CDR files

- Default: 0.0.0.0

port
Enter the port number on the FTP/SFTP server to which the Oracle Communications Session Border Controller will send CDR files.

- Default: 21
- Values: Min: 1 / Max: 65535

admin-state
Set the state of an FTP/SFTP push receiver to enabled for the Oracle Communications Session Border Controller to send CDR files to it

- Default: enabled
- Values: enabled | disable

remote-path
Enter the absolute path on which the CDR files are sent to the push receiver. CDR files are placed in this location on the FTP/SFTP server.

- Default: empty
- Values: <string> remote pathname

filename-prefix
Enter the filename prefix to prepend to the CDR files the Oracle Communications Session Border Controller sends to the push receiver. The Oracle Communications Session Border Controller does not rename local files.

- Default: none
- Values: <string> prefix for filenames

Copyright © 2024, 2026, Oracle and/or its affiliates.

priority
Enter a number 0 through 4 to set the priority of this push receiver in relation to the others you configure on the system. The highest priority—and the push receiver the system uses first—is 0. The lowest priority—and the push receiver the system uses last—is 4.

- Default: 4
- Values: Min: 0 (highest) / Max: 4 (lowest)

protocol
Select the transport protocol to be used for this push receiver.

- Default: ftp
- Values: ftp | sftp

username
Enter the username the Oracle Communications Session Border Controller uses to connect to push receiver.

password
Enter the paissword corresponding to the username of this push receiver.

public-key
Leave blank, regardless of authentication type.

temp-remote-file
When enabled, the system prepends the characters "tmp-" to a CDR file during transfer.

- Default: disabled
- enabled

Path

push-receiver is a subelement under the account-config element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > account-config > push-receiver.**

account-group

This element is unsupported.

Path

account-group is an element under the **session-router** path. The full path from the topmost ACLI prompt is **configure terminal**, **session-router**, **account-group**.

allowed-elements-profile

This configuration element is used to configure SIP allowlists which controls the passage of unknown headers and parameters in request and response traffic.

Parameters

name
A unique identifier of this allowed-elements-profile

Copyright © 2024, 2026, Oracle and/or its affiliates.

description
A textual description for the allowed-elements-profile

allow-any
Enter list of headers that are allowed (with any parameter). When header-rules are added to a rule-set, they are automatically removed from this list. A header list is entered separated by a space, but without the ":" part of the header name. This parameter is initially populated with many allowed headers. Example syntax is shows below.

- allow-any (Accept Accept-Resource-Priority Acme-Codec-Policy Acme-Rfc2833 Alert-Info Allow Allow-Events Authentication-Info Authorization Call-ID Contact Content-Disposition Content-Encoding Content-Length Content-Type CSeq Diversion Event Expires From History-Info Join Max-Forwards Min-Expires Min-SE P-Access-Network-Info P-Asserted-Identity P-Associated-URI P-Called-Party-ID P-Charging-Function-Addresses P-Charging-Vector P-DCS-LAES P-DCS-Redirect P-Preferred-Identity P-Subscription-MSISDN P-Visited-Network-ID Path Privacy Proxy-Authenticate Proxy-Authorization Proxy-Require RAck Reason Record-Route Refer-To Replaces request-uri Require Resource-Priority Retry-After Route RSeq Security-Client Security-Server Security-Verify Service-Route Session-Expires Session-ID Subscription-State Supported To Via WWW-Authenticate User-to-User)

rule-sets
See the rule-sets subelement that follows.

Path

allowed-elements-profile is an element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > allowed-elements-profile**

allowed-elements-profile > rule-sets

This configuration subelement is used to configure SIP allowlists which controls the passage of unknown headers and parameters in request and response traffic.

Parameters

name
A unique identifier of this rule set.

unmatched-action
Identifies the action that the Oracle Communications Session Border Controller performs when it encounters a non-allowlisted header.

- Default: Reject
- Values: reject | delete

msg-type
Specifies the message type to which the rule applies

- Default: any
- Values: any | request | response

methods
Specifies list of methods to which the rule applies. This applies to all methods when none are specified. Enter this as a comma separated list.

Copyright © 2024, 2026, Oracle and/or its affiliates.

logging
Enables logging when an unmatched element is intercepted.

- Default: disabled

Path

rule-sets is a subelement under the allowed-elements-profile element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **session-router**, and then **allowed-elements-profile**, and then **rule-sets.**

allowed-elements-profile > rule-sets > header-rules

This configuration subelement is used to configure SIP allowlists which controls the passage of unknown headers and parameters in request and response traffic.

Parameters

header-name
The name of the header in the allowlist that theOracle Communications Session Border Controller allows from incoming messages. It is case-insensitive and supports abbreviated forms of header names. For example, “Via”, “via”, or “v” all match against the same header. A header name of “request-uri” refers to the request URI of requests, while a header name of “*” applies to any header-type not matched by any other header-rule. The default value is “*”. This default value provides the ability to have header-rules for commonly known headers that remove unknown parameters, but leave unknown headers alone.

unmatched-action
The action for the Oracle Communications Session Border Controller to perform when an incoming header’s parameters do not match the relevant allowed parameters specified for this header-name. This parameter applies to non-matching header names only (not non-matching URI parameters).

- Default: reject
- Values:
  - reject—Rejects all incoming messages that have header parameters that do not match the parameters specified in this header-name.
  - delete — Deletes the non-matching elements from incoming messages with header parameters that do not match those specified in this header-name.

allow-header-param
The header parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is “*”, which allows all header parameters to pass through. If you leave this field empty, no header parameters are allowed.

- Deafult: *

allow-uri-param
The URI parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is “*”, which allows all URI parameters to pass through. If you leave this field empty, no URI parameters are allowed.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Deafult: *

allow-uri-user-param
The URI user parameter that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is “*”, which allows all URI user parameters to pass through. If you leave this field empty, no URI user parameters are allowed.

- Deafult: *

allow-uri-header-name
The URI header name that the Oracle Communications Session Border Controller allows from the headers in incoming messages. You can enter up to 255 characters, including a comma (,), semi-colon (;), equal sign (=), question mark (?), at-symbol (@), backslash (\), or plus sign (+). The default value is “*”, which allows all URI header name parameters to pass through. If you leave this field empty, no URI header name parameters are allowed.

- Deafult: *

Path

header-rulesheader-rules is a subelement under rule-sets under the allowed-elements-profile element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal >terminal > session-router > allowed-elements-profile rule-sets header-rules**

audit-logging

The **audit-logging** element controls the settings for the audit log.

Parameters

state
Whether audit logging is enabled.

- Default: disabled
- Values: enabled | disabled

detail-level
Specifies the level of detail in audit log entries.

- Default: brief
- Values: brief | verbose

audit-trail
Whether to record every successful ACLI command.

- Default: disabled
- Values: enabled | disabled

audit-http
Whether HTTP methods and headers are logged.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

audit-record-output
Define where audit records are logged.

- Default: file
- Values: syslog | file | both

file-transfer-time
Specify the maximum interval in hours between audit-log transfers to a previously configured SFTP server. The value 0 disables SFTP pushes.

- Default: 720
- Min: 0 | Max: 65535

max-storage-space
Specifies the maximum disk space in megabytes available for audit log storage.

- Default: 32
- Min: 1 | Max: 32

percentage-full
Specifies a file size threshold (as a percentage of max-storage-space) that triggers audit file transfer to a previously configured SFTP server or servers.

- Default: 75
- Min: 0 | Max: 99

max-file-size
Specifies a file size threshold (as an absolute file size measured in megabytes) that triggers audit file transfer to a previously configured SFTP server or servers.

- Default: 5
- Min: 0 | Max: 10

storage-path
The local path where audit logs are stored.

- Default: /code/audit/

push-receiver
Enter the push-receiver configuration element.
See the Admin Security Guide for configuring the audit logging push receiver.

Path

The full path is **security**, and then **admin-security**, and then **audit-logging**.

auth-params

The auth-params element provides a list of RADIUS servers used for authentication, along with protocol and operation details that define RADIUS access.

Parameters

name
Enter the name of this instance of the auth-params configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

protocol
Enter the protocol to use for obtaining authentication data from a RADIUS server.

- Default: eap
- Values: eap

> **Note**
>
> The current software version only supports EAP.

strategy
Enter the management strategy used to distribute authentication requests. This parameter is only relevant if multiple RADIUS servers have been identified by the servers parameter.

- Default: hunt
- Values: round-robin | hunt

server
Enter a RADIUS server by IP address.

Path

auth-params is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **security**, and then **auth-params**.

authentication

The authentication configuration element is used for configuring an authentication profile, which applies to your configured authentication type.

Parameters

source-port
Enter the port number on the SBC to send messages to the RADIUS server.

- Default: 1812
- Values: 1645 | 1812 | 3799

type
Enter the type of user authentication

- Default: local
- Values: local | radius| tacacs

protocol
Select the protocol type to use with your RADIUS server(s)

- Default: pap
- Values: pap | chap | mschapv2 | ascii | IKEv2-IPsec

tacacs-authentication-only
When enabled, restricts remote login to TACACS+ when available.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

tacacs-authorization
Enable or disable command-based authorization of admin users for TACACS.

- Default: enabled
- Values: enabled | disabled

tacacs-authorization-arg-mode
Enable or disable sending commands and arguments separately to the TACACS server. Values include:

- Default: disabled, which sends command and arguments together to TACACS+ server.
- enabled—Sends command and arguments separately to TACACS+ server, with the exception of the **show** command.
- enabled-for-show—Sends command and arguments separately to TACACS+ server including the **show** command.

tacacs-accounting
Enable or disable accounting of admin ACLI operations.

- Default: enabled
- Values: enabled | disabled

server-assigned-privilege
Enables a proprietary TACACS+ variant that, after successful user authentication, adds an additional TACACS+ request/reply exchange.

- Default: enabled
- Values: enabled | disabled

allow-local-authorization
Enable this parameter if you want the SBC to authorize users to enter Super (administrative) mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA.

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> When enabled, the SBC ignores RADIUS or TACACS restrictions and allows all users to locally enable Superuser (administrative) mode.

login-as-admin
Enable this parameter if you want users to be logged automatically in Superuser (administrative) mode.

- Default: disabled
- Values: enabled | disabled

management-strategy
Enter the management strategy used to distribute authentication requests.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: hunt
- Values: round-robin | hunt

ike-radius-params-name
Enter the auth-params instance to be assigned to this element.

- Default: None
- Values: Name of an existing auth-params configuration element

management-servers
Enter a list of servers used for management requests.

radius-servers
Enter the radius-servers subelement.

tacacs-servers
Enter the tacacs-servers subelement.

two-factor-authentication
Enter the two-factor-authentication subelement.

> **Note**
>
> This element is only visible if you have the Admin Security entitlement installed.

multi-factor-functionality-enhancement
Enter the multi-factor-functionality-enhancement subelement.

> **Note**
>
> This element is only visible if you have the Admin Security and Data Integrity entitlements installed.

Path

The **authentication** element is under the security path.

```
ADMINSEC# conf term
ADMINSEC(configure)# security
ADMINSEC(security)# authentication
ADMINSEC(authentication)#
```

authentication-profile

This element is reserved for future use. Use authentication-profile for creating an authentication scheme profile. Other configurations, such as HTTP Client and HTTP Server, require the authentication profile.

Parameters

name
Set the name of this authentication profile.

Copyright © 2024, 2026, Oracle and/or its affiliates.

authentication-scheme
Set the authenticaton strategy. Default: Bearer.

preshared-key
Set the authenticaton password.

Path

authentication-profile is an element under the System path. The full path from the topmost ACLI prompt is: **configure terminal > security > authentication-profile**.

> **Note**
>
> This is a multi-instance element.

authentication > multi-factor-functionality-enhancement

Use the **multi-factor-functionality-enhancement** configuration element to enable or disable client certificate-based authentication for the web GUI.

Parameters

MFFE
When enabled, allows client certificate-based authentication for the web GUI for local accounts configured with the **MFFE** authentication type.

- Default: disabled
- Values: enabled | disabled

Constraints

Enable the Admin Security and Data Integrity (FIPS) entitlements to configure this element.

Path

The **multi-factor-functionality-enhancement** element is under the security path.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# authentication
ORACLE(authentication)# multi-factor-functionality-enhancement
ORACLE(multi-factor-functionality-enhancement)#
```

authentication > online-certificate-status-protocol

The online-certificate-status-protocol configuration element is used to configure OCSP validation of clients.

Parameters

ocsp-access-method-list
Select which authentication interfaces will use OCSP validation.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: "" | SSH | GUI | SSH,GUI

dns-resolver-ip
Enter the IP address of the DNS resolver to use for OCSP validation.

dns-resolver-port
Enter the port of the DNS resolver to use for OCSP validation.

ocsp-responder-fqdn
(Optional) Enter the FQDN of the OCSP resolver to use for OCSP validation.
When this value is set, the SBC uses the value to overwrite the URL found in the Authority Information Access (AIA) field of the client certificate.

Constraints

Enable the Admin Security and FIPs entitlements to configure this element.

This element can only be set after the two-factor-authentication element has been set.

> **Warning**
>
> To prevent lockout, import your client X.509 certificates before configuring this element.

Path

The **online-certificate-status-protocol** element is under the security path.

```
ORACLE# conf term
ORACLE(configure)# security
ORACLE(security)# authentication
ORACLE(authentication)# online-certificate-status-protocol
ORACLE(online-certificate-status-protocol)#
```

authentication > radius-servers

The radius-servers subelement defines and configures the RADIUS servers that the Oracle Communications Session Border Controller communicates with.

Constraints

This element is not visible if FIPS is enabled.

Parameters

address
Enter the IP address for the RADIUS server. An IPv4 or IPv6 address is valid for this parameter.

port
Enter the port number on the remote IP address for the RADIUS server

- Default: 1812

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: 1645 | 1812

state
Enable or disable this configured RADIUS server

- Default: enabled
- Values: enabled | disabled

secret
Enter the password the RADIUS server and the Oracle Communications Session Border Controller share. This password is not transmitted between the two when the request for authentication is initiated.

nas-id
Enter the NAS ID for the RADIUS server

realm-id
Enter the RADIUS server realm ID.
If you use the **realm-id**, you must configure a dedicated network-interface element for RADIUS.

retry-limit
Set the number of times the Oracle Communications Session Border Controller retries to authenticate with this RADIUS server

- Default: 3
- Values: Min: 1 / Max: 5

retry-time
Enter the time in seconds the Oracle Communications Session Border Controller waits before retrying to authenticate with this RADIUS server

- Default: 5
- Values: Min: 5 / Max: 10

maximum-sessions
Enter the maximum number of sessions to maintain with this RADIUS server

- Default: 255
- Values: Min: 1 / Max: 255

class
Select the class of this RADIUS server as either primary or secondary. A connection to the primary server is tried before a connection to the secondary server is tried.

- Default: primary
- Values: primary | secondary

dead-time
Set the time in seconds before the Oracle Communications Session Border Controller retries a RADIUS server that it has designated as dead

- Default: 10
- Values: Min: 10 / Max: 10000

Copyright © 2024, 2026, Oracle and/or its affiliates.

authentication-methods
Select the authentication method the Oracle Communications Session Border Controller uses when communicating with the RADIUS server

- Default: pap
- Values: all | pap | chap | mschapv2 | eap

Path

radius-servers is a subelement under the **authentication** configuration element under the security path. The full path from the topmost prompt is: **configure terminal** , and then **security** , and then **authentication** , and then **radius-servers.**

authentication > tacacs-servers

The tacacs-servers subelement defines and configures the TACACS+ servers that the Oracle Communications Session Border Controller communicates with.

Parameters

address
Enter the IP address for the TACACS server. This address must be reachable over the system's media interfaces.

port
Enter the port number on the remote IP address for the TACACS server.

- Default: 49
- Values: 0 - 65535

state
Enable or disable this configured TACACS server

- Default: enabled
- Values: enabled | disabled

secret
Enter the password the TACACS server and the Oracle Communications Session Border Controller share. This password is not transmitted between the two when the request for authentication is initiated.

realm-id
Enter the TACACS server realm ID. This realm must be reachable from the system's media interfaces. If you use the **realm-id**, you must configure a dedicated network-interface element for TACACS.

dead-time
Set the time in seconds before the Oracle Communications Session Border Controller retries a TACACS server that it has designated as dead

- Default: 10
- Values: Min: 10 / Max: 10000

authentication-methods
Select the authentication method the Oracle Communications Session Border Controller uses when communicating with the TACACS server

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: all
- Values: all | pap | chap | ascii

tacas-authorization-arg-mode
This parameter is unsupported.

Path

tacacs-servers is a subelement under the **authentication** configuration element under the security path. The full path from the topmost prompt is: **configure terminal** , and then **security** , and then **authentication** , and then **tacacs-servers.**

bootparam

The bootparam command establishes the parameters that a Oracle Communications Session Border Controller uses when it boots.

> **Note**
>
> In the physical interface and the network interface configuration elements, you can set values that may override the values set within the boot configuration parameters. If you are configuring these elements and enter information that matches information in the boot configuration parameters, the system will warn you that your actions may change the boot configuration parameters. The bootparam command presents you with the parameters to enter on a line-by-line basis. You can press <Enter> to accept a given default parameter and move to the next parameter.

Parameter

Boot File
Enter the path of the software image you are booting. Include the absolute path for a local boot from the local /boot volume and for a net boot when a path on the FTP server is needed.

IP Address
Enter the IP address of wancom0.

VLAN
Enter the LAN of management network.

> **Note**
>
> The acquire-config command is not supported on management interfaces that use both VLANs and IPv6.

Netmask
Enter the Netmask portion of the wancom0 IP Address.

Gateway
Enter the Network gateway that this wancom0 interface uses.

Copyright © 2024, 2026, Oracle and/or its affiliates.

IPv6 Address
Enter the Version 6 IP address/mask of wancom0. Configure the mask as a forslash (/) after the address followed by the mask in number of bits.

IPv6 Gateway
Enter the Version 6 network gateway that this wancom0 interface uses.

Host IP
Enter the IP Address of FTP server from where to download and execute a software image.

FTP username
Enter the FTP server username.

FTP password
Enter the FTP server password

flags
Set the Oracle Communications Session Border Controller to know from where to boot. Also sets how to use the files in the booting process. This sequence always starts with 0x (these flags are hexadecimal).

- 0x00000008 Bootloader ~7 seconds countdown
- 0x00000040 Autoconfigure wancom0 via DHCP enable - VM platforms only
- 0x00000080 Use TFTP protocol (instead of FTP) enable - VM platforms only
- 0x00000080 Use TFTP protocol (instead of FTP) enable - VM platforms only

Target Name
Enter the name of this Oracle Communications Session Border Controller. This field also sets the name of the Oracle Communications Session Border Controller as it appears in the system prompt (e.g., ORACLE> or ORACLE#). You need to know the target name if you are setting up an HA node.
This name must be unique among Oracle Communications Session Border Controllers in your network. This name can be 63 characters or less.

Console Device
Enter the Serial output device type that is dependent on platform. COM1 applies to virtual serial consoles, VGA to virtual video console. VGA is the default on VMware and KVM. COM1 is the default on OVM and EC2.

Console Baudrate
Enter the speed in bits per second which the console port operates at. The options can be 115200 BPS, 8 data bits, no stop bit, parity NONE.

Other
This allows to set miscellaneous and deployment-specific boot settings for internal use only.

Path

bootparam is in the configuration path. The full path from the topmost prompt is: **configure terminal** , and then **bootparam**.

bfd-config

The bfd-config configuration element is used for configuring BFD parameters that apply to all BFD sessions on the interface.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

state
Specifies whether or not the interface can support BFD sessions.

- Default: disabled
- Values: enabled/disabled

health-score
Specifies the change in the system's health-score value when any BFD session fails or recovers.

- Default: 0
- Values: 0 - 100

options
Augments the command with customer-specific features and/of parameters. This optional field allows for a comma separated list of "feature=<value>" or "feature" parameters for the BFD element.

bfd-session
Enters the **bfd-session** multi-instance subelement. Configure individual BFD session parameters in this subelement.

Path

bfd-config is an element under the network-interface path. The full path from the topmost prompt is: **configure terminal** , and then **system** , and then **network-interface**, and then **bfd-config**

bfd-config > bfd-session

The bfd-session configuration element is used for configuring individual BFD sessions.

Parameters

bfd-sess-type
Specifies the type for this specific session.

- Default: primary
- Values: vip/primary/secondary

admin-state
Specifies whether this specific session is enabled.

- Default: disabled
- Values: enabled/disabled

admin-session-state
Allows you to put this specific session in admin-down state.

- Default: adminDown
- Values: up/adminDown

Copyright © 2024, 2026, Oracle and/or its affiliates.

min-tx-interval
Specifies the min-tx-interval in milleseconds. Refer to RFC 5880 for more details.

- Default: 1000
- Values: 1 - 65535

min-rx-interval
Specifies the min-rx-interval in milleseconds. Refer to RFC 5880 for more details.

- Default: 1000
- Values: 1 - 65535

detect-multiplier
Specifies the detect-multipler as an integer. Refer to RFC 5880 for more details.

- Default: 3
- Values: 1-255

hold-down-time
Specifies the duration, in milliseconds, after which an up transition is reported to the application to prevent rapid state flapping.

- Default: 0 (disabled)
- Values: 0-10000

local-discriminator
Specifies the integer used by the system to identify this session. Values range from 1 - 4294967295.

- Default: 3
- Values: 1-4294967295

Path

bfd-session is an element under the network-interface path. The full path from the topmost prompt is: **configure terminal** , and then **system** , and then **network-interface**, and then **bfd-config**, and then **bfd-session**

capture-receiver

The capture-receiver configuration element allows you to specify a target for packet mirroring from the Oracle Communications Session Border Controller to that target. This command is only applicable to **packet-trace remote**.

Parameters

state
Enable or disable the Oracle Communications Session Border Controller’s TRACE capability.

- Default: disabled
- Values: enabled | disabled

Disable capture receivers you are not actively using for traces to prevent potential service outages caused by the capture's system resource utilization.

Copyright © 2024, 2026, Oracle and/or its affiliates.

address
Enter the TRACE server IP address.

network-interface
Enter the TRACE server outbound interface. The argument accepts the full interface name, including the sub-port-id. The command assumes sub-port-id 0 if it is not specified.

Path

capture-receiver Is an element of the system path. The full path from the topmost ACLI prompt is: **configure terminal > system > capture-receiver.**

certificate-record

This configuration element configures certificate records for TLS support.

Parameter

name
The name of this certificate record object.

country
Enter the name of the locality for the state

- Default: US

state
Enter the name of the locality for the state

- Default: MA

locality
Enter the name of the organization holding the certificate

- Default: Burlington

organization
Enter the name of the organization holding the certificate

- Default: Engineering

unit
Enter the name of the unit for holding the certificate within the organization.

common-name
Enter the common name for the certificate record.

key-size
Set the size of the key for the certificate.

- Default: 2048
- Values: 1024 | 2048 | 4096 (on systems with appropriate hardware)

alternate-name
The alternate name of the certificate holder which can be expressed as an IP address, DNS host, or email address. Configure this parameter using the following syntax to express each of these 3 forms.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- **IP:<IP address>**
- **DNS:<DNS IP address/domain>**
- **email:<email address>**

> **Note**
>
> This field adheres to the standard ACLI character limit of 1024.

```
ORACLE(certificate-record)# alternate-name
IP:10.2.2.2,IP:10.3.3.3,DNS:bar.example.com,DNS:foo.example.com
```

trusted
Enable or disable trust of this certificate

- Default: enabled
- Values: enabled | disabled

key-usage-list
Enter the usage extensions to use with this certificate record; can be configured with multiple values.

- Default: digitalSignature and keyEncipherment
- Values: digitalSignature | nonRepudiation | keyEncipherment | dataEncipherment | keyAgreement | encipherOnly | decipherOnly
- Additional values supported for imported certificate records: keyCertSign | cRLSign

  These values are intended only for compatibility with certificate records imported using the **global-trusted-ca** command; Oracle does not recommend using them when creating a certificate record manually.

extended-key-usage-list
Enter the extended key usage extensions you want to use with this certificate record.

- Default: serverAuth
- Values: serverAuth | clientAuth
- Additional values supported for imported certificate records: codeSigning | emailProtection | OCSPSigning | timeStamping

  These values are intended only for compatibility with certificate records imported using the **global-trusted-ca** command; Oracle does not recommend using them when creating a certificate record manually.

> **Note**
>
> When you enable a **tls-profile** for **mutual-authentication**, you must also configure the **extended-key-usage-list** parameter within the associated **end-entity-certificate** to both the **serverAuth** and **clientAuth** values.

key-algor
Set a key algorithm.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: rsa | rsapss | ecdsa

digest-algor
Set a digest algorithm.

- Values: sha1 | sha256 | sha384

When the FIPS entitlement is enabled, you cannot select **sha1**.
For certificate records imported using the **global-trusted-ca** command, **sha512** is also supported. Oracle does not recommend using this when creating a certificate record manually.

> **Note**

ecdsa-key-size
When **key-algor** is set to **ECDSA**, set the ECDSA key size.

- Values: p256 | p384

cert-status-profile-list
Enter a list of configured cert-status-profile names.

Path

certificate-record is an element under the security path. The full path from the topmost prompt is: **configure terminal** , and then **security** , and then **certificate-record**.

cert-status-profile

The cert-status-profile configuration element identifies an OCSP responder, the transport protocol used to access the responder, and the certificates used to sign the OCSP request and to validate the OCSP response.

Parameters

name
Enter the name of this cert-status-profile instance, thus allowing the configuration of multiple configuration elements of this type. This parameter is required.

- Default: None
- Values: Any valid object name — the name must be unique within the cert-status-profile namespace

ip-address
Enter the IPv4 address of the destination OCSP responder. This parameter is required.

- Default: None
- Values: Any valid IPv4 address

hostname
hostname of the OCSR. If this parameter and the ip-address parameter are both configured, the Oracle Communications Session Border Controller uses the IP address.

port
Enter the destination port number. This parameter is optional.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 80
- Values: Any valid port number

type
Enter the protocol type used for certificate checking. This parameter is optional.

- Default: ocsp
- Values: ocsp | crl

trans-proto
Enter the protocol used to transmit the OSCP request; the single currently supported value is http. This parameter is optional.

- Default: http
- Values: http

requester-cert
Enter the name of the certificate configuration element used to sign the outgoing OCSP request; this parameter is required only if the OCSP responder mandates a signed request.

- Default: None
- Values: An existing certificate configuration element name

trusted-cas
Enter a list of trusted Certificate Authority certificate records.

responder-cert
Enter the name of the certificate configuration element used to validate the incoming OCSP response.

- Default: None
- Values: An existing certificate configuration element name

realm-id
Enter the name of the realm used for transmitting OCSP requests. This parameter is optional.

- Default: wancom
- Values Any valid realm name

retry-count
Enter the maximum number of times to retry an OCSP responder in the event of connection failure.

- Default: 1
- Values: Min: 0/Max: 10

dead-time
Enter the interval (in seconds) between the trigger of the retry-count(er) and the next attempt to access the unavailable OCSP responder. This parameter is optional.

- Default: 0 (seconds)
- Values: Min: 0/Max: 3600

crl-update-interval
Specify the interim, in seconds, between CRL updates.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 86400
- Values: 600-2600000

crl-list
Enter a list of trusted Certificate Authority certificate records.

Path

cert-status-profile is a subelement under the security configuration element. The full path from the topmost ACLI prompt is: **configure-terminal**, and then **security**, and then **cert-status-profile**.

> **Note**
>
> This is a multiple instance configuration.

class-profile

The class-profile configuration element lets you access the class-policy configuration element for creating classification policies for ToS marking for SIP or H.323.

Parameters

policy
Enter the class-policy subelement

Path

class-profile is an element under the session-router path. The full path from the topmost prompt is: **configure terminal** , and then **session-router** , and then **class-profile.**

class-profile > policy

The class-policy configuration subelement lets you create classification policies that are used to create a ToS marking on incoming traffic based upon a matching media-policy and destination address.

Parameters

profile-name
Enter the classification profile name

to-address
Enter a list of addresses to match for when determining when to apply this class-policy. Addresses can take the forms:

- Values:
  - +<number>—E164 address
  - <number>—Default address type

Copyright © 2024, 2026, Oracle and/or its affiliates.

- [<host>].domain—Host and/or domain address

media-policy
Enter the media-policy used for this class-policy

Path

class-policy is a subelement under the session-router path. The full path from the topmost prompt is:**configure terminal** , and then **session-router** , and then **class-profile** , and then **policy.**

cluster-config

Use **cluster-config** to manage basic SLB interaction with clustered SBCs.

Constraints

Only systems with SLB configured support **cluster-config**.

Parameters

The **cluster-config** configuration element contains the following parameters:

state
Enable or disable the cluster configuration.

- Default: enabled
- Values: enabled | disabled

log-level
Enter the log level.

- Default: CRITICAL
- Values: ZERO | NONE | EMERGENCY | CRITICAL | MAJOR | MINOR | WARNING | NOTICE | INFO | TRACE | DEBUG | DETAIL

auto-rebalance
Enable or disable the automatic rebalancing of the cluster when a new SBC becomes available.

- Default: enabled
- Values: enabled | disabled

source-rebalance-threshold
Enter the percentage of advertised registration capacity an SBC must be above to be considered a source of rebalanced endpoints.

- Default: 50
- Min: 0 | Max: 100

dest-rebalance-threshold
Enter the percentage of advertised registration capacity an SBC must be below to be considered a destination of rebalanced endpoints.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Min: 0 | Max: 4294967295

dest-rebalance-max
Enter the maximum occupancy rate that the SLB transfers to the new cluster member during a rebalance operation.

- Default: 80
- Min: 0 | Max: 100

tunnel-check-interval
Enter the interval in milliseconds between SLB tunnel audits.

- Default: 15000
- Min: 0 | Max: 4294967295

During a tunnel audit, the SLB checks the status of each tunnel and removes all tunnels flagged as dead.

tunnel-fail-interval
Enter the interval in milliseconds between periodic keepalive messages sent from a clustered SBC to the SLB.

- Default: 10000
- Min: 0 | Max: 4294967295

rebalance-request-delay
Enter the interval in milliseconds between endpoint request messages sent from the SLB to a clustered SBC.

- Default: 500
- Valid value: 0
- Min: 50 | Max: 4294967295

session-multiplier
Enter a factor that when multiplied by an SBC's licensed session limit, determines the maximum number of endpoints that the SBC can support (that is, its maximum occupancy).

- Default: 10
- Min: 1 | Max: 100

atom-limit-divisor
Enter a factor of contacts to endpoints that can be used in occupancy and occupancy rate calculations.

- Default: 1
- Min: 0 | Max: 4294967295

rebalance-skip-ahead
Restrict the target set of SBCs eligible for rebalancing to those whose re-registration is not scheduled within the number of milliseconds specified by this parameter.

- Default: 0
- Min: 0 | Max: 4294967295

Copyright © 2024, 2026, Oracle and/or its affiliates.

rebalance-max-refresh
Restrict the target set of SBCs eligible for rebalancing to those whose re-registration is not scheduled until after the number of milliseconds specified by the parameter.

- Default: 0
- Min: 0 | Max: 4294967295

ignore-tgt-svcs-on-rebalance
Not currently supported.

- Default: disabled
- Values: enabled | disabled

rebalance-del-app-entries
Set to enabled to remove cached registration entries after the rebalance operation completes.

- Default: enabled
- Values: enabled | disabled

inactive-sd-limit
Enter the maximum silent interval in seconds before the SLB flags the SBC as dead and removes it from the cluster.

- Default: 1800
- Min: 0 | Max: 31536000

red-port
Enter the port to listen on for redundancy flow sync messages.

- Default: 2001
- Valid value: 0
- Min: 1025 | Max: 65535

red-max-trans
Enter the maximum number of redundancy sync transactions to keep alive.

- Default: 10000
- Min: 0 | Max: 50000

red-sync-start-time
The maximum period of time (in milliseconds) that the standby SBC waits for a heartbeat signal from the active SBC before assuming the active role.

- Default: 5000
- Min: 0 | Max: 4294967295

red-sync-comp-time
The interval between synchronization attempts after the completion of a redundancy check.

- Default: 1000
- Min: 0 | Max: 4294967295

service-ports
Access the **service-ports** subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

The **cluster-config** configuration element is in the **session-router** element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# cluster-config
ORACLE(cluster-config)#
```

codec-policy

The codec-policy configuration element allows you to configure codec policies, sets of rules that specify the manipulations to be performed on SDP offers.

Parameters

name
Enter the unique name for the codec policy. This is the value you will use to refer to this codec policy when you apply it to realms or session agents. This is a required parameter.

allow-codecs
Enter the list of media format types (codecs) to allow for this codec policy. In your entries, you can use the asterisk (*) as a wildcard, the force attribute, or the no attribute so that the allow list you enter directly reflect your configuration needs. The **text:no** value strips "m=text" occurrence in the outbound INVITE and enables T.140 to Baudot transcoding. The codecs that you enter here must have corresponding media profile configurations. This field accepts conditional codec policy syntax.

add-codecs-on-egress
Enter the codecs to be appended to an offer. Excluding keywords add and delete when a list is already configured replaces the entire list. This field accepts conditional codec policy syntax.

- [add | delete] <name> [name>...]

> **Note**
>
> Only codecs that can be transcoded may be specified. See your version's Release Notes for the list of applicable codecs.

> **Note**
>
> The codecs are processed from right to left in the list.

order-codecs
Enter the order in which you want codecs to appear in the outgoing SDP offer. You can use the asterisk (*) as a wildcard in different positions of the order to directly reflect your configuration needs. The codecs that you enter here must have corresponding media profile configurations. This field accepts conditional codec policy syntax.

force-ptime
Enable or disable a forced ptime being used.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- enabled | disabled

packetization-time
Enter a preferred ptime when the **force-ptime** parameter is enabled.

- Default: 20
- Values: 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100

dtmf-in-audio
Select how the Oracle Communications Session Border Controller should support the conversion of signaling messages or RFC 2833 to DTMF Audio tones in the realm where this transcoding policy is active.

- Default: disabled
- Values:
  - disabled—Does not support DTMF audio tones as transcoded in this realm.
  - preferred—Supports DTMF audio tones as transcoded in this realm.
  - dual—Supports both transcoded DTMF audio tones and signaling-based DTMF indications if possible.

tone-detection
Enables FAX tone detection.

- fax-cng—Causes the system to start its FAX transcoding based on the detection of CNG or CED tone.
- fax-v21—Causes the system to start its FAX transcoding based on the receipt of V21 messages.

tone-detect-renegotiate-timer
Specifies the time after which the system sends a re-Invite if it does not receive a re-Invite from the endpoint. The system resets this timer whenever it receives a re-Invite from the endpoint.

- Default: 500
- Values: 50 - 32000

reverse-fax-tone-detection-reinvite
Allows you to force the SBC to send a ReInvite that includes T.38 in the SDP out a realm that does not have tone detection enabled.

- disabled—Does not force the system to send ReInvites out a different realm. (Default)
- enabled—Allows the system to send ReInvites out a different realm during applicable scenarios.

fax-single-m-line
Set this parameter to the preferred FAX media type for Re-INVITEs to endstations that do not support multiple m-lines. The SBC issues Re-INVITEs using the configured media type only. Should the negotiation fail, the SBC issues another Re-INVITE that offers the other media type.

- disabled—The single m-line function is disabled. (Default)
- image-first—Sends Re-INVITE with m=image as the only m-line in the SDP.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- audio-first—Sends Re-INVITE with m=audio as the only m-line in the SDP.

evrc-tty-baudot-transcode
Enables transcoding of EVRC TTY TDD to BAUDOT in EVRC-G.711

- Default: disabled
- Values: enabled | disabled

secure-dtmf-cancellation
Removes all Dual-Tone Multi-Frequency (DTMF) information that the SBC processes within the codec-policy from ingress. It also removes the residual signal energy (i.e. the leftover signaling from the media stream) at the beginning and ending of each DTMF digit so that an important piece of data is not detectable within the egress stream. But this option does not remove DTMF bleed unless transcoding is enabled for the call.

- Default: disabled
- Values: enabled | disabled

Path

codec-policy is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **media-manager**, and then **codec-policy**.

system-config > comm-monitor

The **comm-monitor** subelement configures the communication monitor/Palladion Mediation engine.

Parameters

state
The state of the Communication Monitor feature.

- Default: disabled
- Values: enabled | disabled

sbc-grp-id
Group ID in the Palladion Mediation engine.

- Default: 0
- Values: Min: 0 / Max: 999999999

tls-profile
tls-profile to use for connection to mediation engines for TLS Connections.

qos-enable
Enable/disable sending of QoS information to the mediation engine.

- Default: enabled
- Values: enabled | disabled

interim-qos-update
Enable/disable sending of periodic QoS update information for the duration of a call.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

monitor-collector
Enters the **monitor-collector** subelement to configure IP parameters of the Palladion Mediation engines.

Path

comm-monitor is a subelement under the system-config element. The full path from the topmost ACLI prompt is: **configure terminal**, and then **system**, and then **system-config**, and then **comm-monitor** .

system-config > comm-monitor > monitor-collector

The **monitor-collector** subelement configures the communication monitor/Palladion Mediation endpoints.

Parameters

address
IP address to push collected data to.

port
Port at which operations monitor server listens.

- Default:4739
- Min value: 1025
- Max value: 65535

network-interface
Local network-interface to use for the connection.

- Default: wancom0:0

> **Note**
>
> If configuring with a media interface, that interface must belong to a configured realm.

Path

monitor-collector is a subelement under the system-config element. The full path from the topmost ACLI prompt is: **configure terminal**, and then **system**, and then **system-config**, and then **comm-monitor**, and then **monitor-collector.**

data-flow

The data-flow configuration element specifies pass-through data-traffic processing when using IKE.

Parameters

name
Specify the name of this instance of the data-flow configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

realm-id
Specify the realm that supports the upstream (core side) data-flow.

group-size
Specify the maximum number of user elements grouped together by this data-flow instance. For maximum efficiency, this value should be set to a power of 2.

- Default: 128
- Values: 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256

> **Note**
>
> The optional group-size parameter specifies the divisor used by this data-flow instance to segment the total address pool into smaller, individually-policed segments.

upstream-rate
Specify the allocated upstream bandwidth.

- Default: 0 (allocates all available bandwidth)
- Values: Min: 0 / Max: 122070

downstream-rate
Specify the allocated downstream (access side) bandwidth.

- Default: 0 (unlimited, no bandwidth restrictions)
- Values: Min: 0 / Max: 122070

Path

Data-flow is a subelement under the ike element. The full path from the topmost ACLI prompt is.**configure terminal**, and then **security**, and then **ike**, and then **data-flow**.

> **Note**
>
> This is a multiple instance configuration element.

diameter-manipulation

The diameter-manipulation configuration element defines the message manipulation elements.

Constraints

This configuration element is not available for the Enterprise Session Border Controller or for the Subscriber-Aware Load Balancer.

Parameters

name
Configured name of this diameter manipulation. This is the key field.

- Default: empty

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: 24 character string, no special characters with the exception of the underscore and hyphen characters. Do not start name with numeric character.

description
Textual description of this diameter manipulation.

- Default: empty
- Values: 256 character string

diameter-manip-rule
Access the **diameter-manip-rule** subelement.

Path

diameter-manipulation is an element in the **session-router** path. The full path from the topmost ACLI prompt is: **session-router**, and then **diameter-manipulation**

diameter-manipulation > diameter-manip-rule

The diameter-manip-rule defines an individual step in creating REGEX type message manipulation object.

Constraints

This configuration element is not available for the Enterprise Session Border Controller or for the Subscriber-Aware Load Balancer.

Parameters

name
Configured name of this manipulation rule. This is the key field.

- Default: empty
- Values: Character string, no special characters with the exception of the underscore characters. Do not start name with numeric character.

avp-code
AVP in the Diameter message to be of manipulated by this rule. This parameter must be configured.

- Default: 0
- Values: Valid AVP code

descr-avp-code
Description of AVP code to be manipulated.

- Default: empty
- Values: 256 character string

avp-type
The data type of the content of the field the system PD is parsing to perform a manipulation on. This parameter must be configured with an enumerated value. Refer to the Diameter standards document for the encodings of individual AVPs.

- Default: none

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: none | octet-string | octet-hex | integer32 | unsignedint32 | address | diameteruri | enumerated

action
Type of manipulation action to perform on this AVP.

- Default: none
- Values: none | add | delete | store | diameter-manip | group-manip | find-replace-all | replace

comparison-type
Select the comparison type that the match-value uses.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | boolean

msg-type
The message type to which this Diameter manipulation rule applies.

- Default: any
- Values:
  - any—Both Requests and Reply messages
  - request—Request messages only
  - reply— Reply messages only

msg-cmd-code
The Diameter message code that this rule applies to. This parameter must be configured or the manipulation can not be applied to any message.

- Default: 0
- Values: Valid Diameter message code

match-value
Enter the exact value to be matched. The action you specify is only performed if the header value matches. The entered value must match the comparison type.

- Default: empty

new-value
The explicit value for a new element or replacement value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Default: empty

avp-header-rule
Access the **avp-header-rule** subelement.

Path

diameter-manip-rule is a subelement under the **diameter-manipulation** element in the session-router path. The full path from the topmost ACLI prompt is: **session-router**, and then **diameter-manipulation**, and then **diameter-manip-rule**

Copyright © 2024, 2026, Oracle and/or its affiliates.

diameter-manipulation > diameter-manip-rule > avp-header-rule

The avp-header-rule subelement defines how to manipulate an AVP's header.

Constraints

This configuration element is not available for the Enterprise Session Border Controller or for the Subscriber-Aware Load Balancer.

Parameters

name
Configured name of this AVP header rule. This is the key field.

- Default: empty
- Values: Character string, no special characters with the exception of the underscore characters. Do not start name with numeric character.

header-type
Type of AVP header to manipulate, as either the AVP flags or the Vendor ID.

- Default: avp-flags
- Values: avp-flags | avp-vendor-id

action
Type of manipulation action to perform on data range in the AVP header.

- Default: none
- Values: none | add | delete | replace

match-value
Value to be matched in the AVP flags or in the vendor ID bits. When manipulating AVP flags, the enumerated values are used to indicate which flag. When manipulating the vendor ID, an integer is entered.

- Default: empty
- Values: vendor | must | proxy

new-value
value to replace the match value with. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Default: empty

Path

avp-header-rule is a subelement under the **session-router** path. The full path from the topmost ACLI prompt is: **session-router**, and then **diameter-manipulation**, and then **diameter-manip-rule**, and then **avp-header-rule**

dnsalg-constraints

The dnsalg-constraints configuration element is used to provision various traffic constraints upon existing dns-config configurations.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

name
The name of the dnsalg constraint configuration element this value is applied in a dns-config configuration element.

state
State of this dnsalg-constraint.

- Default: enabled
- Values: enabled | disabled

max-burst-rate
Maximum number of messages, per second, that can pass through the system in the burst rate window before setting the element to Constraints Exceeded.

- Default: 0
- Values:
  - Min: 0
  - Max: 4294967295

max-sustain-rate
The maximum number od messages that can pass through the system in the sustained rate window before setting the element to Constraints Exceeded.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

max-inbound-burst-rate
Maximum number of inbound messages received by the referencing element within the burst rate window before setting the element to Constraint Exceeded.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

max-inbound-sustain-rate
The maximum number of inbound messages received by the referencing element within the sustained rate before setting the element to Constraints Exceeded.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

max-outbound-burst-rate
Maximum number of outbound messages forwarded from the referencing element within the burst rate window before setting the element to Constraints Exceeded.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

max-outbound-sustain-rate
The maximum number of outbound messages forwarded from the referencing element within the sustained rate window before setting the element to Constraints Exceeded.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

time-to-resume
The number of seconds that the referencing element stays in Constraints Exceeded state and rejects messages before it returns to service.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

burst-rate-window
Number of seconds during which to count messages toward a maximum burst rate.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

sustain-rate-window
The number of seconds during which to count messages toward a maximum sustained rate. a maximum sustained rate.

- Default: 0
- Values:
  - Min: 0
  - Max: 999999

max-latency
The maximum time in seconds a reply to a DNS request can take before considering that DNS server as out of service.

- Default: 0
- Values:
  - Min: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Max: 999999

Path

Path: **dnsalg-constraints**is a configuration element under the **media-manager**path. The full path from the topmost ACLI prompt is: full path from the topmost ACLI prompt is: **configure terminal > media-manager > dnsalg-constraints.**

dns-config

The dns-config configuration element configures the DNS-ALG on a per-client realm basis.

Parameters

client-realm
Enter the realm from which DNS queries are received. This value is the name of a configured realm.

description
Describe the dns-alg configuration element

extra-dnsalg-stats
Enables tracking of extra DNS ALG statistics.

- Default: disabled
- enabled | disabled

dns-max-ttl
Specifies the maximum DNS time to live value to support the DNS ALG feature.

- Default: 86400 seconds (24 hours)
- minimum: 30
- maximum: 2073600

server-dns-attributes
Enter the server-dns-attributes subelement .

constraint-name
Name of the **dnsalg-constraints** configuration element to apply to this **dns-config**.

client-address-list
Enter the IP client realm address(es) from which the Oracle Communications Session Border Controller can receive DNS queries. This field is required.

trap-on-status-change
Enables the system to issue SNMP traps when specific objects managed within any dns-config experience a change in their operating status.

- Default: disabled
- Values: enabled | disabled

Path

dns-config is a subelement under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **dns-config.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This is a multiple instance configuration element.

dns-config > server-dns-attributes

The server-dns-attributes subelement configures DNS servers.

Parameters

server-realm
Enter the realm from which DNS responses are sent. This value must be the name of a configured realm. This value is required.

domain-suffix
Enter the domain suffixes for which this DNS server attribute list is used. This field is required, and can start with an asterisk or a period.

server-address-list
Enter a list of DNS server IP addresses used for the specified domains. This field is required, and can include multiple entries.

source-address
Enter the source IP address from which the ALG sends queries to the DNS server (i.e., a layer 3/layer 4 source address). This field is required.

source-port
Enter the UDP port number from which the ALG sense queries to the DNS server (i.e., layer 3/layer 4 source address). This value is required.

- Default: 53
- Values: 1025-65535

transaction-timeout
Enter the number of seconds that the ALG maintains information to map a DNS server response to the appropriate client request. This value is required.

- Default: 10 seconds
- Values: Min: 0 / Max: 999999999

address-translation
Access the address-translation subelement

Path

server-dns-attributes is a subelement under the dns-config element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **dns-config** , and then **server-dns-attributes.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

dns-config > server-dns-attributes > address-translation

The address-translation subelement sets the list of IP address translations and determines how the NAT function for this feature occurs. Multiple entries in this field allow one DNS-ALG network entity to service multiple Oracle Communications Session Border Controllers or multiple sets of addresses.

Parameters

server-prefix
Enter the address/prefix returned by the DNS server. The server-prefix is an IP address and number of bits in slash notation.

client-prefix
Enter the address/prefix to which a response is returned. The client-prefix is an IP address and number of bits in slash notation.

Path

address-translation is a sub-subelement of the media-manager element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **dns-config** , and then **server-dns-attributes** , and then **address-translation**.

> **Note**
>
> Values specified for the number of bits dictates how much of the IP address will be matched. If the number of bits remains unspecified, then the Oracle Communications Session Border Controller will use all 32 bits for matching. Setting the bits portion after the slash to 0 is the same as omitting it. This is a multiple instance configuration element.

dpd-params

The dpd-params configuration element enables creation of one or more sets of DPD Protocol parameters.

Parameters

name
Enter a unique identifier for this instance of the dpd-params configuration element.

- Default: None
- Values: Valid configuration element name that is unique within the dpd-params namespace

max-loop
Set the maximum number of endpoints examined every dpd-time-interval.

- Default: 100
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> If CPU workload surpasses the threshold set by max-cpu-limit, the max-loop value is over-ridden by load-max-loop.

max-endpoints
Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is not under load (as specified by the max-cpu-limit property).

- Default: 25
- Values: An integer value, should be greater than load-max-endpoints

> **Note**
>
> If CPU workload surpasses the threshold set by max-cpu-limit, the max-endpoints value is over-ridden by load-max-endpoints.

max-cpu-limit
Set a threshold value (expressed as a percentage of CPU capacity) at which DPD protocol operations are minimized to conserve CPU resources.

- Default: 60 percent
- Values: An integer value, 0 (effectively disabling DPD) through 100

load-max-loop
Set the maximum number of endpoints examined every dpdtime-interval when the CPU is under load, as specified by the max-cpu-limit parameter.

- Default: 40
- Values: an integer value, should be less than max-loop

load-max-endpoints
Set the maximum number of simultaneous DPD Protocol negotiations supported when the CPU is under load, as specified by the max-cpulimit property.

- Default: 5
- Values: An integer value, should be less than max-endpoints

max-attempts
The maximum number of DPD attempts before an unresponsive peer is considered dead.

- Default: 1
- Range: 1 - 4

max-retrans
The maximum number of times to retransmit each DPD attempt.

- Default: 3
- Range: 1 - 4

Path

dpd-params is a subelement under the ike element. The full-path from the topmost ACLI prompt is: **configure-terminal**, and then **security**, and then **ike**, and then **dpd-params**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This is a multiple instance configuration element.

emergency-dscp-profile

You use the emergency-dscp-profile configuration element to define DSCP values to match within a SIP INVITE. The SBC drops matching INVITEs if they do not also include separate SIP designation as emergency traffic. If configured, the SBC sends the error code and message you set in this profile. If you do not configure an error code and text, the SBC sends the default SIP error code and message “403 Unauthorized attempt to use reserved resources”.

Parameters

name
Establishes a label for individual emergency-dscp-profiles. You use this label to apply these profiles to session-agents, sip-interfaces or the sip-config. This field supports a maximum of 128 characters.

tos-values
A space-separated string of decimal or hex numbers, that the SBC searches for within a packet. If it finds a value configured here, and the packet does not have any SIP information identifying the call as an emergency call, the system rejects the call.

- Values: string of decimal or hex numbers space separated (0x00 to 0xFF)

error-code
This optional field can include an integer that specifies the error code you send back to any endpoint that sends a non-emergency INVITE that includes a DSCP value you configured in this profile.

- Default: “403”
- Range: SIP error response codes 400 to 499

error-message
This optional field can include a string that specifies the error text that you send back to any endpoint that sends a non-emergency INVITE that includes a DSCP value you configured in this profile.

- Default: Unauthorized attempt to use reserved resources
- Values: String

Path

emergency-dscp-profile is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **emergency-dscp-profile**.

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

enforcement-profile

The enforcement-profile sets groups of SIP methods to apply in the global SIP configuration, a SIP interface, a SIP session agent, or a realm.

Parameters

name
Enter the name of the enforcement profile.

allowed-methods
Select a list of SIP methods that you want to allow in this set.

- Default: None
- Values: INVITE, REGISTER, PRACK, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH

sdp-address-check
Enable or disable SDP address checking on the Oracle Communications Session Border Controller.

- Default: disabled
- Values: enabled | disabled

allowed-elements-profile
Enter the name of the allowed elements profile.

add-certificate-info
List of one or more certificate attribute names to enable TLS certificate information caching and insertion of cached certificate information into customized SIP INVITEs. This list is entered enclosed in quotes with attributes separated by spaces.

certificate-ruri-check
Set the Oracle Communications Session Border Controller to cache TLS certificate information and validate Request-URIs.

- Default: disabled
- Values: enabled | disabled

verify-certificate-info-register
Adds certificate information for REGISTER messages and verifies Request-URIs against certificate attributes.

- Default: disabled
- Values: enabled | disabled

Path

enforcement-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > enforcement-profile**.

enforcement-profile > subscribe-event

The subscribe-event subelement defines subscription event limits for SIP per-user dialogs.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

event-type
Enter the SIP subscription event type for which to set up limits. You can wildcard this value (meaning that this limit is applied to all event types except the others specifically configured in this enforcement profile). To use the wildcard, enter an asterisk (*) for the parameter value.

max-subscriptions
Enter the maximum number of subscriptions allowed

- Default: 0
- Values: Min: 0 / Max: 65535

Path

subscribe-event is a subelement under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **enforcement-profile**, and then **subscribe-event**.

enum-config

The enum-config is used to configure ENUM functionality on your Oracle Communications Session Border Controller.

Parameters

name
Enter the name of the ENUM configuration

top-level-domain
Enter the domain extension used to query the ENUM servers for this configuration. The query name is a concatenation of the number and the domain.

realm-id
Enter the realm-id is used to determine on which network interface to issue an ENUM query.

enum-servers
Enter the name of an ENUM server and its corresponding redundant servers to be queried. In a query, separate each server address with a space and enclose list within parentheses.

service-type
Enter the ENUM service types you want supported in this ENUM configuration. Possible entries are E2U+sip and sip+E2U (the default), and the types outlines in RFCs 2916 and 3721. If you add to the pre-existing E2U+sip and sip+E2U list and want those values to remain, you must enter them with your new values.

- Default: E2U+sip,sip+E2U

query-method
Enter the ENUM query distribution strategy

- Default: hunt
- Values: hunt | round-robin

Copyright © 2024, 2026, Oracle and/or its affiliates.

timeout
Enter the total time, in seconds, that should elapse before a query sent to a server (and its retransmissions) will timeout. If the first query times out, the next server is queried and the same timeout is applied. This process continues until all the servers in the list have timed out or one of the servers responds. The retransmission of ENUM queries is controlled by three timers:

- Init-timer—The initial retransmission interval. The minimum value allowed for this timer is 250 milliseconds.
- Max-timer—The maximum retransmission interval. The interval is doubled after every retransmission. If the resulting retransmission interval is greater than the value of max-timer, it is set to the max-timer value.
- Expire-timer—The query expiration timer. If a response is not received for a query and its retransmissions within this interval, the server will be considered non-responsive and the next server in the list will be tried.
- Default: 11
- Values: Min: 0 / Max: 4294967295

cacheInactivityTimer
Enter the time interval, in seconds, after which you want cache entries created by ENUM requests deleted, if inactive for this interval. If the cache entry gets a hit, the timer restarts and the algorithm is continued until the cache entry reaches its actual time to live.

- Default: 3600
- Values: Min: 0 / Max: 4294967295

lookup-length
Specify the length of the ENUM query, starting from the most significant bit

- Default: 0
- Range: 0 - 255

max-response-size
Set the maximum size in bytes for UDP datagram responses.

- Default: 512
- Range: 512 - 65535

remote-recursion
Set the RD bit for the remote ENUM server to query recursively.

- Default: enabled
- Values: enabled / disabled

health-query-number
Enter the phone number for the ENUM server health query; when this parameter is blank the feature is disabled.

health-query-interval
Enter the interval in seconds at which you want to query ENUM server health.

- Default: 0
- Values: Min: 0 / Max: 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

failover-to
Enter the name of the enum-config to which you want to failover.

cache-addl-records
Set this parameter to enabled to add additional records received in an ENUM query to the local DNS cache.

- Default: enabled
- Values: enabled | disabled

include-source-info
Set this parameter to enabled to send source URI information to the ENUM server with any ENUM queries.

- Default: disabled
- Values: enabled | disabled

recursive-query
Enables the Oracle Communications Session Border Controller to query a DNS server for a hostname returned in an ENUM result.

- Default: disabled
- Values: enabled | disabled

retarget-requests
When set to enabled, the Oracle Communications Session Border Controller replaces the Request-URI in the outgoing request. When set to disabled, the Oracle Communications Session Border Controller routes the request by looking to the Route header to determine where to send the message.

- Default: enabled
- Values: enabled | disabled

Path

enum-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **enum-config**.

ext-policy-server

The ext-policy-server is used for configuring PDP/RACF or CLF functionality on the Oracle Communications Session Border Controller.

Parameters

name
Enter the name of this external policy server configuration

state
Enable or disable the operational state of this external policy server configuration

- Default: enabled
- Values: enabled | disabled

operation-type
Select the function this external policy server performs

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values:
  - disabled
  - admission-control—Oracle Communications Session Border Controllercommunicates with a CLF to obtain location string
  - bandwidth-mgmt— Oracle Communications Session Border Controller acts as a PEP in a PDP/RACF deployment

protocol
Select the external policy server communication protocol

- Default: C-SOAP
- Values:
  - COPS—Standard COPS implementation. COPS client type is 0x7929 for CLF, and 0x7926 for PDP/RACF usage as defined in the operation-type parameter.
  - A-COPS—Vendor specific protocol. COPS client type is 0x4AC0 for admission-control operation-type.
  - SOAP—Not used
  - C-SOAP—Not used
  - DIAMETER—Connects the Oracle Communications Session Border Controller to the policy-server

address
Enter the IP address or FQDN of an external policy server, or enter the name of a policy-group preceded by the **PSG:** prefix. IP addresses can by IPv4 or IPv6.

port
Enter the port on the external policy server to which you must connect. For example, the standard port for COPS is 3288. The system ignores this parameter if the address parameter is set to a policy-group or an FQDN.

- Default: 80
- Values: Valid Range: 0-65535

realm
Enter the realm where the external policy server exists. The system ignores this parameter if the address parameter is set to a policy-group, with the exception that it is used to populate all Origin-Realm and Origin-Host AVPs in diameter messages generated by traffic from the **policy-group**'s **policy-agent**s.

transport-protocol
Enter the transport protocol used to connect to this external policy server.

- Default: TCP
- Values: TCP / SCTP

local-multi-home-addrs
Applies to SCTP. Enter an IP address that is local to the SBC and can be used by this external policy server as an alternate connection point. This address must be the same type as the address parameter, either IPv4 or IPv6.

Copyright © 2024, 2026, Oracle and/or its affiliates.

remote-multi-home-addrs
Applies to SCTP. Enter an IP addresses that can be used by this SBC as an alternate connection point. This address must be the same type as the address parameter, either IPv4 or IPv6.

sctp-send-mode
Applies to SCTP. Specifies the SCTP delivery mode. The default value is **ordered**. Valid values are:

- ordered (Default)
- unordered

num-connections
Enter the number of TCP connections to external policy server

- Default: 1
- Values: Min: 0 / Max: 65535

reserve-incomplete
Enable or disable admission requests being made before all of the details of the call are known

- Default: enabled
- Values:
  - Enabled—Supports the usual behavior when the AAR is sent upon SDP offer as well as SDP answer. This mode ensures backwards compatibility with releases prior to Release S-C6.1.0.
  - Orig-realm-only—Allows calls originating from a realm with a policy server associated with it to send the AAR upon SDP offer; calls terminating at a realm with a policy server associated with it send the AAR post SDP exchange.
  - Disabled—Allows no bandwidth reservation for incomplete flows.

permit-conn-down
Enable or disable the Oracle Communications Session Border Controller's ability to permit calls if there is no connection to the external policy server.

- Default: disabled
- Values: enabled | disabled

permit-on-reject
Change this parameter to enabled if you want the Oracle Communications Session Border Controller to forward the session on at a "best-effort". Leave this parameter set to disabled (Default), if you want the Oracle Communications Session Border Controller to deny the session on attempts to revert to the previously-requested bandwidth

- Default: disabled
- Values: enabled | disabled

permit-on-reject
Change this parameter to enabled if you want the Oracle Communications Session Border Controller to forward the session on at a "best-effort". Leave this parameter set to disabled (default), if you want the Oracle Communications Session Border Controller to deny the session on attempts to revert to the previously-requested bandwidth.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

disconnect-on-timeout
Disable this parameter to prevent timeouts triggered by Gate-Set or Gate-Delete message sequences between the Oracle Communications Session Border Controller and a policy server from tearing down their connection. Retaining the default (enabled) allows all timeouts to tear down and re-establish the TCP connection.

- Default: enabled
- Values: enabled | disabled

product-name
Enter the vendor product name.

application-mode
Select the mode in which the policy server interface is operating.

- Default: none
- Values: Rq | Rx | Gq | e2 | pktmm3

application-id
Enter the application mode of this interface.

- Default: 0
- Values: Min: 0 / Max: 999999999

framed-ip-addr-encoding
Set the format of the Frame-IP-Address (AVP 8) value in Diameter messages.

- Default: octet-string
- Values: octet-string (i.e., 0xC0A80A01) | ascii-string (i.e., 192.168.10.1)

dest-realm-format
Set the format for the Destination-Realm AVP.

- Default: user_with_realm
- Values: user_with_realm | user_only | realm_only

ingress-realm-location
Set this parameter to configure the child realm or its parent for the Address-Realm in the Globally-Unique-Address AVL in DIAMETER UDR messages that the Oracle Communications Session Border Controller sends to the policy server.

- Default: realm-in
- Values:
  - realm-in—This setting means that the Oracle Communications Session Border Controller will use the same realm on which the REGISTRATION request arrived.
  - sip-interface—This setting means that the Oracle Communications Session Border Controller will use the realm associated with the SIP interface on which the REGISTRATION request arrived.

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - diam-address-realm - For the e2 interface, this value enables configurable Address-Realm AVPs. This setting points the Oracle Communications Session Border Controller to the associated realm from which it will learn Address-Realm AVP information.

user-name-mode
Determines how the User-Name AVP is constructed. Used primarily with e2 based CLF functionality.

- Default: none
- Values:
  - none—Oracle Communications Session Border Controller does not include the User-Name AVP in any UDRs
  - endpoint-ip—IP address of the registering endpoint is sent as the payload for the User-Name AVP
  - public-id—SIP-URI portion of the TO header from the register message is sent as the payload for the User-Name AVP
  - auth-user—Username attribute of the Authorization header from the register is sent as the payload for the User-Name AVP; if there is no authorization header, the Oracle Communications Session Border Controller will not consult the CLF and will forward the registration message.

domain-name-suffix
Sets the suffix for Origin-Realm and Origin-Host AVPs that have a payload string constructed as a domain name. If your entry does not include the dot, the system prepends one.

- Default: .com

gate-spec-mask
With this parameter, you can configure the Oracle Communications Session Border Controller to use a mask comprised entirely of zeros (0). The default value is 255. This parameter sets the value to use for the COPs pkt-mm-3 interface. This interface maintains a persistent TCP connection to the external policy server, even without repsonses to requests for bandwidth. This permits calls to traverse the Oracle Communications Session Border Controller even though the external policy server either fails to respond, or rejects the session.

- Default: 255
- Values: Min: 0 / Max: 255

allow-srv-proxy
Enable this parameter if you want to include the proxy bit in the header. The presense of the proxy bit allows the Oracle Communications Session Border Controller to tell the external policy server whether it wants the main server to handle the Diameter message, or if it is okay to proxy it to another server on the network (disabled)

- Default: enabled
- Values: enabled | disabled

wildcard-trans-protocol
Set this parameter from enabled if you want to use transport protocol wildcarding for Rx/Rq Flow-Description AVP (507) generation. Enabled sends a flow description of “ip”. Set this parameter to disabled if you want to use the specific media stream transport protocol.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

watchdog-ka-timer
Enter the number of seconds to define the interval for watchdog/keep-alive messages; this is the time in which the Oracle Communications Session Border Controller must receive a COPS-KA message from the policy server to ensure collection is still valid.

- Default: 0
- Values: Min: 0 / Max: 65535

include-rtcp-in-request
Change this parameter from disabled (default), to enabled so the Oracle Communications Session Border Controller will include RTCP information in AARs.

- Default: disabled
- Values: enabled | disabled

provision-signaling-flow
Enables the Oracle Communications Session Border Controller to send AARs to PCRFs after registration that includes the grouped Media-Component-Description AVP as described in 3GPP TS 29.213 section B1b [1], and the procedures specified in TS 29.214 section 4.4.5a.

- Default: disabled
- Values: enabled | disabled

max-timeouts
max number of request timeouts before the Oracle Communications Session Border Controller sets this external policy server to inactive.

- Default: 0
- Values: Min: 0 / Max: 200

max-connections
Number of external policy servers to be monitored as a server cluster

- Default: 1

srv-selection-strategy
Strategy used to select an external policy server from the cluster.

- Default: Failover

optimize-aar
Reduces the number of ARRs sent to the PCRF.

- Default: disabled
- Values: enabled | disabled

emergency-epc-level-identities
Enable or disable the ability of the Oracle Communications Session Border Controller to request EPC level identities within the context of an emergency call.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

use-epc-level-msisdn
Enable or disable the Oracle Communications Session Border Controller's ability to insert an EPC-level MSISDN into the PAI of the egress INVITE. This parameter is relevant only when you have also enabled emergency-epc-level-identities.

- Default: disabled
- Values: enabled | disabled

operator-config-local-mcc-mnc
Specifies the MNC value and, by means of the entry, the number of digits the Oracle Communications Session Border Controller uses to build the host part of the outgoing PAI derived during EPC level identity retrieved when emergency-epc-level-identities is enabled.

- Default: 999999
- Range: 10000 - 999999

cache-dest-host
Used to enable the Diameter Multi-tiered Policy Server Support feature.

- Default: disabled
- Values: enabled | disabled

specific-action-subscription
Populates the Specific-Action AVP in an AAR message to indicate the subscription types it supports. When unconfigured, no Specific-Action AVP is sent.

- Default: blank
- Values:
  - loss-of-bearer
  - recovery-of-bearer
  - release-of-bearer

> **Note**
>
> Use this setting to support an Abort-Session-Request (ASR) via the PCRF to close a user session when they return to their home-network from a roaming network.

  - ip-can-change
  - out-of-credit
  - successful-resources-allocation
  - failed-resources-allocation
  - access-network-info-report

specific-action-sig-flow-subscription
subscribes for signaling flow status change notifications

diameter-in-manip
Configure this parameter with the **name** of a **diameter-manipulation** to be applied on traffic inbound to the Oracle Communications Session Border Controller.

Copyright © 2024, 2026, Oracle and/or its affiliates.

diameter-out-manip
Configure this parameter with the **name** of a **diameter-manipulation** to be applied to outbound traffic from this Oracle Communications Session Border Controller.

asynchronous-mode
Identifies whether to use the asynchronous mode of signaling on the external policy server interface rather than the default synchronous mode.

- Default: disabled
- Values: enabled | disabled

media-release
For scenarios wherein the SBC releases media, enabling this parameter allows the policy server request to include flow descriptions that accurately represent the IP addresses of the two endpoints instead of that of the Oracle Communications Session Border Controller.

- Default: disabled
- Values: enabled | disabled

options
Enter any customer-specific features and/or parameters for this external policy server. This parameter is optional.

Path

ext-policy-server is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **ext-policy-server**.

filter-config

The **filter-config** element is used for configuring a filter object for SIP Monitor and Trace functionality.

Parameters

name
Enter the name of this filter-config configuration element.

address
IP Address to apply to this filter. The netmask is optional.

- Default: 0.0.0.0
- <addr-prefix><ipv4|ipv6> [/<num-bits>]

user
Phone number or user-part to apply to this filter.

Path

filter-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **session-router**, and then **filter-config.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

factory-accounts

Use the factory-accounts command to enable or disable the default admin and user accounts.

Arguments

enable
Re-enable the default admin and user accounts.

disable
Disable the default admin and user accounts.

Mode

Superuser

Example

```
factory-accounts disable
```

fraud-protection

Use **fraud-protection** to enable fraud protection and specify the fraud protection source file.

Constraints

Enable the Fraud Protection entitlement to access this configuration element.

Path

The **fraud-protection** configuration element is in the **system** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# fraud-protection
ORACLE(fraud-protection)#
```

Parameters

The **fraud-protection** configuration element contains the following parameters:

mode
Set the fraud protection mode.

- Default: disabled
- Values: disabled | local | comm-monitor
- local—Use the SBC as the source of the fraud protection file.
- comm-monitor—Not supported.

file-name
Enter the name of the fraud protection file.
Syntax: `/code/fpe/<filename>`.

Copyright © 2024, 2026, Oracle and/or its affiliates.

options
Add fraud protection options.

allow-remote-call-terminate
Not currently supported.

- Default: disabled
- Values: enabled | disabled

fxo-profile

Use **fxo-profile** to add up to four Foreign Exchange Office (FXO) profiles to support different attributes at different endpoints. For example, you might create profiles based on username, department, or location.

Constraints

Only platforms with Digium analog cards support **fxo-profile**.

Path

The **fxo-profile** configuration element is in the **tdm-config** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# tdm-config
ORACLE(tdm-config)# fxo-profile
ORACLE(fxo-profile)#
```

Parameters

The **fxo-profile** configuration element contains the following parameters:

name
Enter a name for this profile.

channels
Enter the channels that apply to this profile. You can enter any combination of the four (5, 6, 7, 8) that apply to the FXO card.

- Default: 5,6,7,8

rx-gain
Set the TDM receive volume in decibels.

- Default: 0.0
- Values: 0.0 - 9.9

tx-gain
Set the TDM transmit volume in decibels.

- Default: 0.0
- Values: 0.0 - 9.9

echo-cancellation
Enable or disable echo cancellation.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- Values: enabled | disabled

fax-detect
Set the fax-detect.

- Default: both
- Values: incoming | outgoing | both | no

route-group
Enter the number of the route-group for this profile.

- Default: 0
- Min: 0 | Max: 63

signalling
Set the signaling type.

- Default: fxs_ks
- Values: fxs_ls | fxs_gs | fxs_ks

phone-number
Enter the caller's number. Required.

fullname
Enter the caller's name.

cid-signalling
Set the caller ID signaling type.

- Default: bell
- Values: bell | v23

options
Configure FXO options.

voice-codec
Set the voice codec.
This attribute is only available on platforms that have the Wanpipe driver installed.

- Default: MULAW
- Values: MULAW | ALAW

fxs-profile

Use **fxs-profile** when your deployment requires a Foreign Exchange Service (FXS) profile for Time Division Multiplexing (TDM). You can add up to four FXS profiles to support different attributes at different endpoints. For example, you might create profiles based on user name, department, and location. Note that you must also configure **tdm-config**.

Constraints

Only platforms with Digium analog cards support **fxs-profile**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

The **fxs-profile** configuration element is in the **tdm-config** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# tdm-config
ORACLE(tdm-config)# fxs-profile
ORACLE(fxs-profile)#
```

Parameters

The **fxs-profile** configuration element contains the following parameters:

name
Enter the fxs profile name.

channels
Enter the channels that apply to this profile. You can enter any combination of the four (1, 2, 3, 4) that apply to the FXS card.

- Default: 1,2,3,4

rx-gain
Set the TDM receive volume in decibels.

- Default: 0.0
- Values: 0.0 - 9.9

tx-gain
Set the TDM transmit volume in decibels.

- Default: 0.0
- Values: 0.0 - 9.9

echo-cancellation
Enable or disable echo cancellation.

- Default: enabled
- Values: enabled | disabled

fax-detect
Set the fax-detect.

- Default: both
- Values: incoming | outgoing | both | no

route-group
Enter the number of the route-group for this profile.

- Default: 0
- Min: 0 | Max: 63

signalling
Set the signaling type.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: fxo_ks
- Values: fxo_ls | fxo_gs | fxo_ks

phone-number
The caller's number.

fullname
The caller's name.

cid-signalling
Set the caller ID signaling type.

- Default: bell
- Values: bell | v23

options
Configure additional FXS options.

voice-codec
Set the voice codec.
This attribute is only available on platforms that have the Wanpipe driver installed.

- Default: MULAW
- Values: MULAW | ALAW

h323

The h323 configuration element is the top level of the H.323 configuration, and it contains h323 parameters that apply globally.

Parameters

state
Enable or disable H.323 functionality.

- Default: enabled
- Values: enabled | disabled

log-level
Select the log level for monitoring H.323 functionality. This parameter overrides the process-log level field value set in the system-config element only for H.323 functionality. If the state parameter in this element is set to disabled, this parameter still overrides the process-log-level field from the system-config element for H.323.

- Default: INFO
- Values: EMERGENCY | CRITICAL | MAJOR | MINOR | WARNING | NOTICE | INFO | TRACE | DEBUG | DETAIL

response-tmo
Set the number of seconds Oracle Communications Session Border Controller waits between sending a SETUP message and receiving no response before the call is torn down

- Default: 4
- Values: Min: 0 / Max: 999999999

Copyright © 2024, 2026, Oracle and/or its affiliates.

connect-tmo
Set the number of seconds Oracle Communications Session Border Controller waits between sending out a SETUP message and failing to receive a CONNECT message before the call is torn down. If the Oracle Communications Session Border Controller receives a PROCEEDING or ALERT message from the endpoint, it will tear down the session after this timer elapses if a CONNECT message is not received.

- Default: 32
- Values: Min: 0 / Max: 999999999

options
Enter customer-specific features and/or parameters that affect H.323 behavior globally. This parameter sets a comma-separated list of “feature=value” or “feature” parameters.

h323-stacks
Enter the h323-stacks subelement.

rfc2833-payload
Enter the payload type used by the H.323 stack in preferred rfc2833-mode

- Default: 101
- Values: Valid Range: 96-127

alternate-routing
Choose between pre-4.1 or 4.1 behavior:

- Pre-4.0 behavior—Alternate routing is disabled, and the Oracle Communications Session Border Controller sends a release complete message back to the caller, proxy
- 4.1 behavior—The Oracle Communications Session Border Controller performs alternate routing, recur
  - Default: proxy
  - Values: proxy | recur

codec-fallback
Enable or disable slow start to fast start codec negotiation.

- Default: disabled
- Values: enabled | disabled

enum-sag-match
Enable or disable matching against the hostnames in ENUM/LRT lookup responses and session agent groups

- Default: disabled
- Values: enabled | disabled

remove-t38
Enable or disable the removal of t38 fax capabilities received in a SIP call’s SDP, from the TCS of the outgoing IWF call.

- Default: disabled
- Values: enabled | disabled

Path

h323 is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **h323**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Unlike other single-instance configuration elements, the h323 element does not have to be selected before it can be viewed. The options field does not appear in the output for the show command within the h323 element or for running-config subcommand unless it contains configured values.
> This is a single instance configuration element.

h323 > h323-stacks

The h323-stack subelement supports the SFIWF, FSIWF, H.323<—>SIP traffic, and general H.323 functionality.

Parameters

name
Enter the name of H.323 stack. This value is required and must be unique. The value you enter in this parameter for your H.323 interface (stack) configuration cannot start with a number; it must start with a letter. The Oracle Communications Session Border Controller considers names that start with numbers to be invalid.

description
Provide a brief description of the h323-config configuration element

state
Enable or disable this h323-stack

- Default: enabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

isgateway
Enable or disable H.323 stack functionality as a Gateway. When this field is set to enabled, the H.323 stack runs as a Gateway. When this field is set to disabled, the H.323 stack runs as a Gatekeeper proxy.

- Default: enabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

realm-id
Enter the realm served by this H.323 stack. This value must be a valid identifier for a realm configuration.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not RTC supported

assoc-stack
Enter the name of associated outbound H.323 stack for this h323-stack instance. If not configured, the Oracle Communications Session Border Controller will use policy-based stack selection based on a local policy (configured in a local-policy element). If you wish to use static stack selection, then each configured h323-stack subelement must have an associated outbound stack. This parameter must correspond to a valid name field value in another instance of the h323-stack subelement.

> **Note**
>
> This parameter is not RTC supported.

local-ip
Enter the IP address H.323 stack uses when opening sockets. This field value is the default H.323 stack address.

- Default: 0.0.0.0

> **Note**
>
> This command is not RTC supported

max-calls
Enter the maximum number of calls allowed for the network associated with this H.323 stack

- Default: 200
- Values: Min: 1 / Max: 2147483647

> **Note**
>
> This command is not RTC supported.

max-channels
Enter the maximum number of concurrent channels (or pathways used between nodes) allowed for each call associated with this H.323 stack

- Default: 6
- Values: Min: 1 / Max: 2147483647

> **Note**
>
> This command is not RTC supported.

Copyright © 2024, 2026, Oracle and/or its affiliates.

registration-ttl
Enter the TTL in seconds before a registration becomes invalid. During the initial registration process, after a registration is confirmed, the TTL value set by the Gatekeeper in the RCF message will override this field value. This field is only applicable when the h323-stack: isgateway field is set to enabled.

- Default: 120
- Values: Min: 1 / Max: 2147483647

> **Note**
> This command is not RTC supported.

terminal-alias
Enter a list of alias addresses that identify the H.323 stack terminal. This field value must be entered as a space-separated type=value string (e.g., h323-ID=acme01). This field is only applicable when the isgateway field is set to enabled.

- Values: h323-ID | e164 | url | email | ipAddress

> **Note**
> This command is not RTC supported.

ras-port
Select a listening port number for RAS requests. When this field value is 0, H.323 stack uses port assigned by the operating system and not the well-known port 1719.

- Default: 1719
- Values: Min: 1, Max: 65535

> **Note**
> This command is not RTC supported.

auto-gk-discovery
Enable or disable Automatic Gatekeeper discovery feature upon start-up. This field is applicable only when h323-stack:isgateway field is enabled.

- Default: disabled
- Values: enabled | disabled

> **Note**
> This parameter is not RTC supported.

multicast
Enter the multicast address and port of the RAS Multicast IP Group used for automatic gatekeeper discovery. In order to clear this field, you must enter an empty string by typing a space. 224.0.1.41:1718 is the well known value used to discover the Gatekeeper.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0.0.0.0:0

> **Note**
>
> This parameter is not RTC supported.

gatekeeper
Enter the IP address and RAS port of the Gatekeeper. In order to clear this field, you must enter an empty string.

- Default: 0.0.0.0:0

> **Note**
>
> This parameter is not RTC supported.

gk-identifier
Enter the gatekeeper identifier with which the H.323 stack registers

- Values: 1 to 128 characters

> **Note**
>
> This parameter is not RTC supported.

q931-port
Enter the Q.931 call signaling port. This is the port for the h323-stack: local-ip address set above.

- Default: 1720
- Values: Min: 1 / Max: 65535

> **Note**
>
> This parameter is not RTC supported.

alternate-transport
Enter the alternate transport addresses and ports (i.e., the Annex E address(es) and port(s)). If this field is left empty, the H.323 stack will not listen for incoming Annex E requests.

> **Note**
>
> This parameter is not RTC supported.

q931-max-calls
Set the maximum number of concurrent, active calls allowed on the Oracle Communications Session Border Controller If this field value is exceeded, the H.323 stack returns a state of “busy.”

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 200
- Values: Min: 1 / Max: 2147483647

> **Note**
>
> This parameter is not RTC supported.

h245-tunneling
Enable or disable H.245 tunneling supported by this H.323 stack

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

fs-in-first-msg
Enable or disable Fast Start fields sent in the first message in response to a SETUP message that contains Fast Start fields

- Default: disabled
- Values: enabled | disabled

call-start-fast
Enable or disable conversion of an incoming Slow Start call into a Fast Start call. This H.323 stack must be the outgoing stack for conversion to work. If this field is set to disabled, the outgoing call will be set up with the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-slow parameter.

- Default: enabled
- Values: enabled | disabled

call-start-slow
Enable or disable conversion of an incoming Fast Start call into a Slow Start call. This H.323 stack must be the outgoing stack for this conversion to work. If this field is set to disabled, the outgoing call will be set up to have the same starting mode as the incoming call. This parameter must take the opposite value as the call-start-slow parameter.

- Default: disabled
- Values: enabled | disabled

media-profiles
Enter a list of media profile names used for the logical channels of the outgoing call. These names are configured in the media-profile element. The media-profiles field value must correspond to a valid name field entry in a media-profile element that has already been configured.

prefixes
Enter a list of supported prefixes for this particular H.323 stack

- Values: e164 | url | h323-ID | ipAddress

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not RTC supported.

process-registration
Enable or disable registration request processing for this H.323 stack . Oracle Communications Session Border Controller will process any RRQs that arrive on this H.323 stack if enabled. Oracle Communications Session Border Controller will not acknowledge any requests and drop all RRQ if disabled.

- Default: disabled
- Values: enabled | disabled

allow-anonymous
Enter the admission control of anonymous connections accepted and processed by this H.323 stack

- Default: all
- Values:
  - all—allow all anonymous connections
  - agents-only—only requests from session agents allowed
  - realm-prefix—session agents and address matching realm prefix

options
Enter customer-specific features and/or parameters on a per-stack basis. This parameter sets a comma-separated list of “feature=value” or “feature” parameters. This options field affects H.323 behavior for this particular h323 stack whereas the options field in the main h323 element affects H.323 behavior globally.

> **Note**
>
> This command is not RTC supported.

proxy-mode
Select the proxy functionality for signaling only operation

- Values: H225 | H245

> **Note**
>
> This command is not RTC supported.

h245-stage
Select the H.245 stage at which the Oracle Communications Session Border Controller allows either of the following:

- Transfer of the H.245 address to remote side of the call
- Acting on the H.245 address sent by the remote side
- Default: connect

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: setup | proceeding | alerting | connect | early | facility | noh245 | dynamic

q931-start-port
Set the starting port number for Q.931 port range used for Q.931 call signalling

- Default: 0
- Values: 0 - 32768 (multiples of 1024)
  For example: 1024 | 2048 | 4096 | 8192 | 16384 | 32768

> **Note**
> This parameter is not RTC supported.

q931-number-ports
Set the number of ports in Q.931 port range used for the H.323 registration proxy feature

- Default: 0
- Values: 0 - 32768 (multiples of 1024)
  For example: 1024 | 2048 | 4096 | 8192 | 16384 | 32768

> **Note**
> This parameter is not RTC supported.

dynamic-start-port
Set the starting port number for Q.931 port range used for the H.323 registration proxy feature

- Default: 0
- Values: 0 - 32768 (multiples of 1024)
  For example: 1024 | 2048 | 4096 | 8192 | 16384 | 32768

> **Note**
> This parameter is not RTC supported.

dynamic-number-ports
Enter the number of ports in port range used for dynamic TCP connections the H.323 registration proxy feature

- Default: 0
- Values: 0 - 32768 (multiples of 1024)
  For example: 1024 | 2048 | 4096 | 8192 | 16384 | 32768

> **Note**
> This parameter is not RTC supported.

Copyright © 2024, 2026, Oracle and/or its affiliates.

filename
Enter the name of the configuration file used to override the default configuration. H.323 stack configuration is read from the file specified by this field value. The configuration file does not override manually configured values; the configuration uses the values you have configured plus the information that resides in the file. This file resides in <default-dir>/H323CfgFile, where <defaultdir> is usually /ramdrv.

> **Note**
>
> This parameter is not RTC supported.

tcp-keepalive
Enable or disable TCP keepalive processing on call-signaling port

- Default: disabled
- Values: enabled | disabled

rfc2833-mode
Select whether 2833/UII negotiation will be transparent to the Oracle Communications Session Border Controller (pre-4.1 behavior), or use 2833 for DTMF and signal it in its TCS

- Default: transparent
- Values: transparent | preferred

alarm-threshold
Access the alarm-threshold subelement.

Path

h323-stacks is a subelement under the h323 element. The full path from the topmost ACLI prompt is: **configure terminal** , **session-router** , **h323** , **h323-stacks**.

> **Note**
>
> This is a multiple instance configuration subelement.

h323 > h323-stacks > alarm-threshold

The alarm-threshold subelement allows you to set a threshold for sending an alarm when the Oracle Communications Session Border Controller approaches the max-calls limit.

Parameters

severity
Enter the level of alarm to be configured per port.

- Default: minor
- Values: minor | major | critical

value
Set the percentage of the value defined in the max-calls parameter to determine when the Oracle Communications Session Border Controller issues an alarm

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 1 | Max: 100

Path

alarm-threshold is a subelement under the h323-stacks subelement. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **h323** , and then **h323-stacks**, and then **alarm-threshold**.

http-client

This element is reserved for future use. The http-client configuration element provides a way for the Oracle Communications Session Border Controller (SBC) to communicate with a remote server.

Parameters

name
Set the name of the HTTP client.

state
Enable or disable the connection to the HTTP client.

- Default: enabled

realm
Set the name of the realm on which to send requests. The SBC uses management when you do not specify a realm.

ip-address
Set the local Host Identity Protocol (HIP) IP address to use as the source address.

tls-profile
Set the name of the TLS profile you want the SBC to use.

auth-profile
Set the name of the authenticaton profile you want to use for this client interface.

Path

http-client is an element under the System path. The full path from the topmost ACLI prompt is:**configure terminal > system > http-client**.

> **Note**
>
> This is a multi-instance element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

http-server

Use the **http-server** configuration element to provision the HTTP server of the SBC.

Parameters

name
Set the name of this HTTP server.

> **Note**
>
> The http-server name should match the common-name or alternative-name of the certificate-record when using TLS.

state
Enable or disable this HTTP server.

- Default: enabled
- Values: enabled | disabled

realm
Set the name of the realm on which to listen.
Do not specify a realm when listening on the management interface.

ip-address
Set the local Host IP address on which to listen.
Use this parameter when listening on a media interface. Do not specify an IP address when listening on the management interface.
This IP address must be listed in the **hip-ip-list** attribute under **network-interface**.

http-state
Enable or disable the HTTP connection.

- Default: enabled
- Values: enabled | disabled

http-port
Set the port number to use for the HTTP connection.

- Default: 80
- Min value: 1
- Max value: 65535

http-strict-transport-security-policy
Enable to make the browser access only HTTPS rather than HTTP.

- Default: disabled
- Values: disabled | enabled

https-state
Enable or disable the HTTPS connection.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

https-port
Set the port number to use for the HTTP connection.

- Default: 443
- Min value: 1
- Max value: 65535

http-interface-list
List the applications that will listen for HTTP/HTTPS requests.

- Default: REST,GUI
- Values: REST | GUI | REST,GUI

http-file-upload-size
The maximum size in MB of a file that is uploaded over HTTP/HTTPS.

- Default: 0
- Min value: 0
- Max value: 999

tls-profile
The name of the **tls-profile** to use for HTTPS connections.

auth-profile
Set the **authentication-profile** you want this server to use if your SPL packages require a bearer token. You may leave this parameter blank if this **http-server** instance is going to be used only for the REST API or the web interface.

Path

http-server is an element under the System path. The full path from the topmost ACLI prompt is:**configure terminal**, and then **system**, and then **http-server**.

> **Note**
>
> This is a multi-instance element.

home-subscriber-server

The **home-subscriber-server** element allows you to configure an HSS configuration element with which to exchange information over the Diameter Cx interface.

Parameters

name
Name of this home-subscriber-server configuration element.

state
Running state of this home-subscriber-server configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

address
IP address of this HSS.

port
Port to connect to on this HSS.

- Default: 3868
- Range: 0 - 65535

realm
Realm name in which this HSS exists.

watchdog-ka-timer
Period of time in seconds that DWRs are sent to this HSS.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 65535

add-lookup-parameter
Inserts a P-Acme-Serving header into a message sent into the network. The sender of this message must have been verified by this HSS.

- Default: disabled
- Values: enabled | disabled

value
Set the percentage of the value defined in the max-calls parameter to determine when the SBC issues an alarm.

Path

home-subscriber-server is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **session-router**, and then **home-subscriber-server.**

host-route

The host-route configuration element establishes routing exceptions on the Oracle Communications Session Border Controller for management traffic.

Parameters

dest-network
Enter the IP address of the destination network for this host route. No two host-route elements can have the same dest-network field value.

An IPV6 address is valid for this parameter.

Values: <IPV4> | <IPV6>

netmask
Enter the destination network subnet mask. The network-interface element will not function properly unless this field value is valid.

An IPV6 address is valid for this parameter.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Values: <IPV4> | <IPV6>

gateway
Enter the gateway used to leave the local network. The gateway field identifies the next hop to use when forwarding a packet out of the originator's LAN.

> **Note**
>
> The gateway entered must already be defined as a gateway for an existing network interface.

An IPV6 address is valid for this parameter.

Values: <IPV4> | <IPV6>

description
Provide a brief description of this host-route configuration.

Path

host-route is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **host-route**.

> **Note**
>
> For IPV4, you need to configure netmask.

> **Note**
>
> This is a multiple instance configuration element.

ice-profile

Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE-STUN lite mode) enables a WebRTC client to perform connectivity checks, and can provide several STUN servers to the browser.

Parameters

Name
Set a unique name for this ice profile. Default: Empty.

stun-conn-timeout
Set the maximum time interval, in seconds, between the first STUN binding request received in a media session and the time when a valid STUN binding request containing the USE-CANDIDATE attribute is received. 0 indicates no timeout.

- Default: 10
- Range: 0 - 9999

Copyright © 2024, 2026, Oracle and/or its affiliates.

stun-keepalive-interval
Set the interval, in seconds, since the last media packet or STUN binding request response after which a STUN keep alive message is sent. Zero means do not send keep-alive messages. The value must be less than the value set for subsq-guard-timer.

- Default: 15
- Range: 0 - 300

stun-rate-limit
Set the number of STUN binding requests that you want the SBC to process per minute. Zero means impose no limit.

- Default: 100
- Range: 0 - 99999

mode
Specify the SBC functionality as Downstream or Proxy for media path optimization in Teams. The default, None, avoids this specification.

- Default: None
- Values: DOWNSTREAM | None | PROXY

rtcp-stun
Enable or disable the use of a STUN candidate for RTCP in the SDP of an INVITE that includes ICE in addition to RTP.

- Default: disabled
- Values: enabled | disabled

Path

The **ice-profile** element is located under the **media-manager** group.

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
SBC920(media-manager)# ice-profile
ORACLE(ice-profile)#
```

ike-access-control

The ike-access-control configuration element defines the allowlist, blocklist, and DDoS parameters to be used by the ike-interface to which it is applied.

Syntax

name
Establishes the name of this ike-access-control object.

state
Enables or disables this ike-access-control object.

identifiers
Specifies a list of allowlist identifier prefixes (^ used as a wildcard for a single hexadecimal digit, + or - used for adding or removing prefix.

Copyright © 2024, 2026, Oracle and/or its affiliates.

blocklisted-identifiers
Specifies a list of blocklist identifier prefixes (^ used as a wildcard for a single hexadecimal digit, + or - used for adding or removing prefix.

deny-period
Specifies the quarantine period imposed on an endpoint that transitions to the deny state. During the quarantine period, the endpoint is denied all access to the IKEv2 interface. **deny-period** and **tolerance-window** must both be set to non-zero values to enable IKEv2 DDoS protection.

- Default: 30
- Values: Min: 0 / Max: 999999999 (seconds)

tolerance-window
Specifies the interval (in seconds) between checks of endpoint-specific traffic counters.

- Default: 0 (IKEv2 DDoS disabled)
- Values: Min: 0 / Max: 999999999 (seconds)

pre-ipsec-invalid-threshold
Enables protection against a DDoS attack that consists of malformed, or otherwise invalid, packets during the IKEv2 SA negotiation process by specifying the maximum number of malformed IKEv2 SA packets tolerated from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks can attempt to consume system resources in a futile effort to complete negotiation of IKEv2 SAs.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 999999999 (packets)

pre-ipsec-maximum-threshold
Specifies the maximum number of valid IKEv2 SA packets tolerated from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks can attempt to prolong the IKEv2 negotiation by persistently renegotiating the IKEv2 SA.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 999999999 (packets)

after-ipsec-invalid-threshold
Enables protection against a DDoS attack that consists of malformed, or otherwise invalid, packets after SA setup by specifying the maximum number of malformed packets tolerated from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks can attempt to consume system resources in a futile effort to complete negotiation of IKEv2 SAs.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 999999999 (packets)

Copyright © 2024, 2026, Oracle and/or its affiliates.

after-ipsec-maximum-threshold
Specifies the maximum number of valid IKEv2 packets tolerated after SA setup from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks can attempt to prolong the IKEv2 negotiation by persistently renegotiating the IKEv2 SA.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 999999999 (packets)

auth-failure-threshold
Specifies the maximum number of unsuccessful authentication messages tolerated from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks attempt to consume system resources by persistently presenting invalid credentials during the endpoint authentication process.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 999999999 (authentication attempts)

auth-critical-failure-threshold
Specifies the maximum number of authentication critical failures tolerated from a specific endpoint within the interval set by the **tolerance-window** parameter. These attacks attempt to consume system resources by persistently presenting invalid credentials during the endpoint authentication process.
If this threshold value is reached, the endpoint is quarantined for an interval defined by the **deny-period** parameter.

- Disable: 0
- Default: 1
- Values: Min: 0 / Max: 999999999 (authentication attempts)

auth-failure-report
Specifies how failed authentications are reported. Used in conjunction with the **auth-failure-threshold**

- no-reporting—(the default), authentication failures are not reported
- snmp-trap-only—authentication failures are reported by generating an SNMP trap (refer to "SNMP Trap" for information of trap structure)
- syslog-only—authentication failures are reported by sending a syslog message
- snmp-trap-and-syslog—authentication failures are reported with both an SNMP trap and a syslog message

Path

ike-access-control is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure terminal**, **security**, **ike**, **ike-access-control.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ike-accounting-param

The ike-sainfo configuration element enables negotiation and establishment of IPsec tunnels. To configure this element, install your platform-specific IPsec license.

Parameters

name
Specifies the unique name of this instance of the ike-accounting-param configuration element. You use this name to assign the IPsec accounting parameter list to an IKEv2 interface

- Default: None
- Values: A valid configuration element name, that is unique within the ike-sainfo namespace

radius-accounting-events
Specifies IPsec events that trigger an IPsec accounting transaction. Supported values include:

- Default:
- Values:
- none—disables RADIUS-based IPsec Accounting.
- early-start—triggers an Accounting Request Start packet on initiation of IKEv2 SA negotiation.
- start—triggers an Accounting Request Start packet on tunnel establishment.
- stop—triggers an Accounting Request Stop packet on tunnel tear-down.
- interim-ipsec-rekey—triggers an Accounting Request Interim-Update packet on IPsec tunnel re-keying.
- interim-ike-rekey—triggers an Accounting Request Interim-Update packet on IKEv2 Security Association rekeying.

The early-start and start events are mutually exclusive; you can select only one start event. If early-start is selected, the Security Gateway schedules two accounting transactions. The first transaction is an Accounting Request Start packet triggered by the start of IKEv2 SA negotiation. The second transaction depends on the success or failure of tunnel establishment. Successful tunnel establishment triggers an Interim-Update packet that provides the tunnel details usually found in the standard Accounting Request Start packet. Tunnel failure triggers an Accounting Request Stop packet.
Use double quotes to bracket parameter arguments if multiple events trigger accounting transaction; leave a space between event names.
This command triggers an accounting transaction for four reportable events.

diameter-accounting-events
Specifies specific IPsec events that trigger an IPsec accounting exchange. Supported values include:

- none—disables DIAMETER-based IPsec Accounting
- start—triggers an Accounting Request Start packet on tunnel establishment
- stop—triggers an Accounting Request Stop packet on tunnel tear-down
- interim-ipsec-rekey—not supported in this current release. Support scheduled for inclusion in a subsequent release.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- interim-ike-rekey—not supported in this current release. Support scheduled for inclusion in a subsequent release

Use double quotes to bracket parameter arguments if multiple events trigger accounting transaction; leave a space between event names.
This command triggers an accounting transaction for four reportable events.

intermediate-period
For RADIUS-based IPsec accounting only, use the intermediate-period parameter to specify the interval at which the Security Gateway generates Accounting Request Interim-Update packets.
Supported values are integers within the range 0 (the default) through 65535. The default value (0) disables the generation of interim packets. Any non-default value, within the allowable range, specifies the frequency, in seconds, of interim updates.
Any value less than 60 generates a warning that such frequent transactions can impact system performance.

Path

ike-accounting-param is a subelement under the ike element. The full path from the topmost ACLI prompt is: **security > ike > ike-accounting-param**.

> **Note**
>
> This is a multiple instance configuration element.

ike-certificate-profile

The ike-certificate-profile subelement references a public certificate that authenticates a specific IKEv2 identity, as well as one of more CA certificates used to validate a certificate offered by a remote peer.

Parameters

identity
Enter the local IKEv2 entity that using the authentication and validation credentials provided by this ike-certificate-profile instance.

- Default: None
- Values: An IP address or fully-qualified domain name (FQDN) that uniquely identifies the user of resources provided by this ike-certificate-profile instance

end-entity-certificate
Enter the unique name of a certificate-record configuration element referencing the identification credential (specifically, an X509.v3 certificate) offered by a local IKEv2 entity in support of its asserted identity.

- Default: None
- Values: Name of an existing certificate-record configuration element

trusted-ca-certificates
Enter the unique names of one or more certificate-record configuration elements referencing Certification Authority (CA) certificates used to authenticate a remote IKEv2 peer.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: None
- Values: A comma separated list of existing CA certificate-record configuration elements.

verify-depth
Enter the maximum number of chained certificates that will be processed while authenticating the IKEv2 peer.

- Default: 3
- Values: Min: 1 | Max: 10

Path

ike-certificate-profile is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **configure-terminal**, and then **security**, and then **ike**, and then **ike-certificate-profile**.

> **Note**
>
> This is a multiple instance configuration element.

ike-config

The ike-config subelement defines a single, global Internet Key Exchange (IKE) configuration object.

Parameters

state
Enter the state (enabled or disabled) of the ike-config configuration element.

- Default: enabled
- Values: disabled | disabled

ike-version
Enter an integer value that specifies IKE version.

Select 1 for IKEV1 protocol implementation.

Select 2 for IKEV2 protocol implementation.

- Default: 2
- Values: 1 | 2

log-level
Enter the IKE log level; events of this level and other events deemed more critical are written to the system log.

- Default: info
- Values: emergency | critical | major | minor | warning | notice | info | trace | debug | detail

udp-port
Enter the UDP port used for IKEv1 protocol traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 500
- Values: Min: 1025 / Max: 65535

negotiation-timeout
Enter the maximum interval between Diffie-Hellman message exchanges.

- Default: 15 (seconds)
- Values: Min: 0 / Max:4294967295 (seconds)

> **Note**
>
> In the event of timer expiration, the IKE initiator must restart the Diffie-Hellman exchange.

event-timeout
Enter the maximum time allowed for the duration of an IKEv1 event, defined as the successful establishment of an IKE or IPsec Security Association (SA).

- Default: 60 (seconds)
- Values: Min: 0 / Max:4294967295 (seconds)

> **Note**
>
> In the event of timer expiration, the IKE initiator must restart the Phase 1 (IKE SA) or Phase 2 (IPsec SA) process.

phase1-mode
Enter the IKE phase 1 exchange mode: aggressive or main.

- Default: main
- Values:
  - aggressive—is less verbose (requiring only three messages), but less secure in providing no identity protection, and less flexible in IKE SA negotiation
  - main—is more verbose, but provides greater security in that it does not reveal the identity of the IKE peers. Main mode requires six messages (3 requests and corresponding responses) to (1) negotiate the IKE SA, (2) perform a Diffie-Hellman exchange of cryptographic material, and (3) authenticate the remote peer

phase1-dh-mode
Enter the Diffie-Hellman group used during IKE phase 1 negotiation.

- Default: first-supported
- Values:
  - first-supported — as responder, use the first supported Diffie-Hellman group proposed by initiator

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.

  - dh-group5 — as initiator, propose Diffie-Hellman group 5 (1536-bit)
  - dh-group14 — as initiator, propose Diffie-Hellman group 14 (2048-bit)
  - dh-group15 — as initiator, propose Diffie-Hellman group 15 (3072-bit)
  - dh-group16 — as initiator, propose Diffie-Hellman group 16 (4096-bit)
  - dh-group17 — as initiator, propose Diffie-Hellman group 17 (6144-bit)
  - dh-group18 — as initiator, propose Diffie-Hellman group 18 (8192-bit)

> **Note**
>
> When you enable the FIPS entitlement, you cannot select **dh-group5**.

phase2-exchange-mode
Enter the Diffie-Hellman group used during IKE Phase 2 negotiation.

- Default: phase1-group
- Values:
  - phase1-group — use the same group as in phase1
  - no-forward-secrecy — use the same key as used during Phase 1 negotiation

> **Note**
>
> During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.
>
> Diffie-Hellman groups determine the lengths of the prime numbers exchanged during the symmetric key generation process.

  - dh-group5 — as initiator, propose Diffie-Hellman group 5 (1536-bit)
  - dh-group14 — as initiator, propose Diffie-Hellman group 14 (2048-bit)
  - dh-group15 — as initiator, propose Diffie-Hellman group 15 (3072-bit)
  - dh-group16 — as initiator, propose Diffie-Hellman group 16 (4096-bit)
  - dh-group17 — as initiator, propose Diffie-Hellman group 17 (6144-bit)
  - dh-group18 — as initiator, propose Diffie-Hellman group 18 (8192-bit)

> **Note**
>
> When you enable the FIPS entitlement, you cannot select **dh-group5**.

v2-ike-life-secs
Enter the default IKEv2 SA lifetime in seconds.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 86400 (24 hours)
- Values: Min: 1800 / Max: 999999999 (seconds)

> **Note**
>
> This global default can be over-ridden at the IKEv2 interface level.

v2-ipsec-life-secs
Enter the default IPsec SA lifetime in seconds.

- Default: 28800 (8 hours)
- Values: Min: 1 / Max:4294967295 (seconds)

> **Note**
>
> This global default can be over-ridden at the IKEv2 interface level.

v2-rekey
Enable to initiate new negotiations to restore expired IKEv2 or IPsec SAs. The SBC makes a maximum of three retransmission attempts before abandoning the re-keying effort.

anti-replay
Enable anti-replay protection on IPsec SAs.

phase1-life-seconds
Set the time (in seconds) proposed for IKE SA expiration during IKE Phase 1 negotiations.

- Default: 3600 (1 hour)
- Values: Min: 0 / Max: 4294967295 (seconds)

> **Note**
>
> Relevant only when the SBC is acting in the IKE initiator role.

phase1-life-secs-max
Set the maximum time (in seconds) accepted for IPsec SA expiration during IKE Phase 1 negotiations.

- Default: 86400 (24 hours)
- Values: Min: 0 / Max: 4294967295 (seconds)

> **Note**
>
> Relevant only when the SBC is acting in the IKE responder role.

phase2-life-seconds
relevant only when the SBC is acting in the IKE initiator role, contains the time proposed (in seconds) for IPsec SA expiration during IKE Phase 2 negotiations.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 28800 (8 hours)
- Values: Min: 0 / Max:4294967295 (seconds)

> **Note**
>
> During IKE Phase 2, the IKE initiator and responder establish the IPsec SA.

phase2-life-secs-max
Set the maximum time (in seconds) accepted for IPsec SA expiration during IKE Phase 2 negotiations.

- Default: 86400 (24 hours)
- Values: Min: 0 / Max: 4294967295 (seconds)

> **Note**
>
> Relevant only when the SBC is acting in the IKE responder role.

shared-password
Enter the default PSK used during IKE SA authentication.

This global default can be over-ridden at the IKE interface level.

- Default: None
- Values: A string of ACSII-printable characters no longer than 255 characters (not displayed by the ACLI)

eap-protocol
Enter the EAP protocol used with IKEv2.

- Default: eap-radius-passthru
- Values: eap-tls | eap-leap | eap-sim | eap-srp | eap-ttls | eap-aka | eap-peap | eap-mschapv2 | eap-fast | eap-psk | eap-radius-passthru

> **Note**
>
> The current software performs EAP operations by a designated RADIUS server or server group; retain the default value.

eap-bypass-identity
Contains a value specifying whether or not to bypass the EAP (Extensible Authentication Protocol) identity phase

EAP, defined in RFC 3748, provides an authentication framework widely used in wireless networks.

An Identity exchange is optional within the EAP protocol exchange. Therefore, it is possible to omit the Identity exchange entirely, or to use a method-specific identity exchange once a protected channel has been established.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled (requires an identity exchange)
- Values: disabled | enabled

red-port
Enter the port number monitored for IKEv2 synchronization messages; used in high-availability environments.

The default value (0) disables redundant high-availability configurations. Select port 1995 to enable high-availability operations.

- Default: 0
- Values: 0 | 1995

red-max-trans
For HA nodes, set the maximum number of retained IKEv2 synchronization message.

- Default: 10000 (messages)
- Values: Min: 0 / Max: 50000 (messages)

red-sync-start-time
For HA nodes, set the timer value for transitioning from standby to active role — the amount of time (in milliseconds) that a standby device waits for a heartbeat signal from the active device before transitioning to the active role.

- Default: 5000 (milliseconds)
- Values: Min: 0 / Max:4294967295 (milliseconds)

red-sync-comp-time
For HA nodes, set the interval between synchronization attempts after the completion of an IKEv2 redundancy check.

- Default: 1000 (milliseconds)
- Values: Min: 0 / Max:4294967295 (milliseconds)

dpd-time-interval
Set the maximum period of inactivity (in seconds) before the Dead Peer Detection (DPD) protocol is initiated on a specific endpoint.

The default value, 0, disables the DPD protocol; setting this parameter to a non-zero value globally enables the protocol and sets the inactivity timer.

- Default: 0 (DPD disabled)
- Values: Min: 0 / Max:4294967295 (seconds)

overload-threshold
Set the percentage of CPU usage that triggers an overload state.

- Default: 100 (disabling overload processing)
- Values: Min: 10 / Max: 100

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> The value of **overload-threshold** must be less than the value of **overload-critical-threshold**.

overload-interval
Set the interval (in seconds) between CPU load measurements while in the overload state.

- Default: 1
- Values: Min: 1 / Max: 60

overload-action
Select the action to take when the SBC (as a SG) CPU enters an overload state. The overload state is reached when CPU usage exceeds the percentage threshold specified by the overload-threshold

- Default: none
- Values:
  - drop-new-connection—use to implement call rejection
  - none—use to retain default behavior (no action)

overload-critical-threshold
Set the percentage of CPU usage that triggers a critical overload state. This value must be greater than the value of overload-threshold.

- Default: 100 (disabling overload processing)
- Values: Min: 10 / Max: 100

overload-critical-interval
Set the interval (in seconds) between CPU load measurements while in the critical overload state.

- Default: shared-password
- Values: Min: 1 / Max: 60

sd-authentication-method
Select the method used to authenticate the IKEv2 SA. Two authentication methods are supported.

This global default can be over-ridden at the IKEv2 interface level.

- Default: shared-password
- Values:
  - certificate—uses an X.509 certificate to digitally sign a block of data
  - shared-password—uses a PSK that is used to calculate a hash over a block of data

certificate-profile-id
When sd-authentication-method is certificate , identifies the default ike-certificate-profile configuration element that contains identification and validation credentials required for certificate-based IKEv2 authentication.

- This parameter can be over-ridden at the IKEv2 interface level.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: None
- Values: Name of an existing ike-certificate-profile configuration element.

id-auth-type
(Optional) Specify that the PSK used while authenticating the remote IKEv2 peer is associated with the asserted identity contained within an IKEv2 Identification payload.

- idi—use IDi KEY_ID for authentication
- idr—use IDr KEY_ID for authentication

Path

ike-config is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal**, and then **security**, and then **ike**, and then **ike-config.**

> **Note**
>
> This is a single instance configuration element.

ike-interface

The ike-interface configuration element enables creation of multiple IKE-enabled interfaces.

Syntax

state
Enable or disable this IKE interface.

ike-version
Set the IKEv1 version for this IKE interface.

- Default: 0—Use the IKE version set in the ike-config,
- Values: 1
- Values: 2

address
Enter the IPv4 address of a specified IKEv1 interface.

- Default: none
- Values: Any valid IPv4 address

realm-id
Enter the name of the realm that contains the IP address assigned to this IKEv1 interface.

- Default: none
- Values: Name of an existing realm configuration element.

ike-mode
Select the IKE operational mode.

- Default: responder
- Values: initiator | responder

Copyright © 2024, 2026, Oracle and/or its affiliates.

local-address-pool-id-list
Select a list local address pool from a list of configured local-address-pools.

dpd-params-name
Enter the specific set of DPD operational parameters assigned to this IKEv1 interface (relevant only if the Dead Peer Detection (DPD) Protocol is enabled).

- Default: None
- Values: Name of an existing dpd-params configuration element.

v2-ike-life-secs
Enter the default IKEv2 SA lifetime in seconds

- Default: 86400 (24hours)
- Values: Min: 1 / Max: 999999999 (seconds)

> **Note**
>
> The global default can be over-ridden at the IKEv2 interface level.

v2-ipsec-life-secs
Enter the default IPsec SA lifetime in seconds.

- Default: 28800 (8 hours)
- Values: Min:1 / Max: 999999999 (seconds)

> **Note**
>
> This global default can be over-ridden at the IKEv2 interface level.

v2-rekey
Enable to initiate new negotiations to restore expired IKEv2 or IPsec SAs. The SBC makes a maximum of three retransmission attempts before abandoning the re-keying effort.

esnSupport
Enable to support Extended Sequence Number (ESN) per RFC 4304.

shared-password
Enter the interface-specific PSK used during IKE SA authentication. This IKEv1-specific value over-rides the global default value set at the IKE configuration level.

- Default: none
- Values: a string of ACSII printable characters no longer than 255 characters (not displayed by the ACLI).

eap-protocol
Enter the EAP protocol used with IKEv2.

- Default: eap-radius-pssthru
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- eap-md5
- eap-tls
- eap-leap
- eap-sim
- eap-srp
- eap-ttls
- eap-aka
- eap-peap
- eap-mschapv2
- eap-fast
- eap-psk
- eap-radius-passthru

> **Note**
>
> The current software performs EAP operations by a designated RADIUS server or server group; retain the default value.

addr-assignment
(Optional) Specify the method used to assign addresses in response to an IKEv2 Configuration Payload request.

- Default: no-assign—No assignment of local address
- radius-only—Use the radius server for the local address
- radius-local—Use the radius server first and then try the local address pool
- local—Use the local address pool to assign the local address

sd-authentication-method
Enter the allowed Oracle Communications Session Border Controller authentication methods

- Default: none
- Values: none-Use the authentication method defined in ike-config for this interface | shared-password - Endpoints authenticate the Oracle Communications Session Border Controller using a shared password | certificate-Endpoints authenticate the Oracle Communications Session Border Controller using a certificate

certificate-profile-id-list
Select an IKE certificate profile from a list of configured **ike-certificate-profiles**.

cert-status-check
(Optional) Enable certificate status checking using either Online Certificate Status Profile (OCSP) or a local copy of a Certificate Revocation List.

cert-status-profile-list
(Optional) Assign one or more **cert-status-profile** configuration elements to this IKEv2 interface.

Copyright © 2024, 2026, Oracle and/or its affiliates.

access-control-name
Specifies the ike-access-control list to use on this IKE interface. The list assignment applies the IKEv2 DDOS, allowlist and blocklist protection configured within the ike-access-control object to the interface.

tunnel-orig-name-list
Specifies the name the tunnel-origin-params element to be applied to this IKE interface.

Path

ike-interface is a subelement under the ike element. The full path from the topmost ACLI prompt is: configure terminal, security, ike, ike-interface.

> **Note**
>
> This is a multiple instance configuration element.

ike-key-id

If authentication between IKEv2 peers is based on a PSK associated with an identity asserted in the IKE Identification Payload, associate received asserted identities with a specified PSK.

Parameters

name
Specifies the unique name of this instance of the ike-key-id configuration element. You can assign this object by entering the name of this element to the local-id-profile or the remote-id-profile of an ike-sainfo object.

key-id
Specifies the identity, similar to a user name, to associate an asserted identity with a PSK. Valid values include IPv4 or IPv6 addressing, or a keyid string.

presharedkey
Specifies the PSK for the applicable security association. The system encrypts and never displays a presharedkey in ACLI or in configuration output.

id-type
Specifies the user Identity type to be used in the IDi or IDr for authentication. Values include:

- ipv4—Specifies that this keyid parameter is in the IPv4 format
- ipv6—Specifies that this keyid parameter is in the IPv6 format
- key—Specifies that this keyid parameter is a string

Path

ike-key-id is a subelement under the **ike** element. The full path from the topmost ACLI prompt is: **security > ike > ike-key-id.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ike-sainfo

The ike-sainfo configuration element enables negotiation and establishment of IPsec tunnels. To configure this element, install your platform-specific IPsec license.

Parameters

name
Enter the unique name of this instance of the ike-sainfo configuration element.

- Default: None
- Values: A valid configuration element name, that is unique within the ike-sainfo namespace

security-protocol
Enter the IPsec security (authentication and encryption) protocols supported by this SA.

- Default: esp-auth
- Values:
  - ah—RFC 4302 authentication services
  - esp—RFC 4303 encryption services
  - esp-auth—RFC 4303 encryption and authentication services

> **Note**
> On virtual platforms, only the default setting is supported.

auth-algo
Set the authentication algorithms supported by this SA.

- Default: sha2-512
- Values: any | sha2-256 | sha2-384 | sha2-512

> **Note**
> On virtual platforms, only the default setting is supported.

encryption-algo
Set the allowed encryption algorithms.

- Default: aes
- Values: any | aes | aes-ctr

> **Note**
> On virtual platforms, only the default setting is supported.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> When you enable the FIPS entitlement, you cannot select **any**.

ipsec-mode
Select the IPSec operational mode. Transport mode provides a secure end-to-end connection between two IP hosts. Tunnel mode provides VPN service where entire IP packets are encapsulated within an outer IP envelope and delivered from source (an IP host) to destination (generally a secure gateway) across an untrusted internet.

- Default: transport
- Values: transport | tunnel

tunnel-local-addr
Enter the IP address of the local IP interface that terminates the IPsec tunnel (relevant only if the ipsec-mode is tunnel, and otherwise is ignored).

- Default: None
- Values: Any valid local IP address

tunnel-remote-addr
Enter the IP address of the remote peer or host (relevant only if the ipsec-mode is tunnel, and is otherwise ignored).

- Default: * (matches all IP addresses)
- Values: Any valid IP address

local-id-profile
Applies the applicable local (SBC) **ike-key-id** for this **ike-sainfo** element. That **ike-key-id** element contains information needed to associate an asserted identity with a PSK.

remote-id-profile
Applies the applicable remote (remote station) **ike-key-id** element for this **ike-sainfo** element when configured with the **ike-key-id** name. That **ike-key-id** element contains information needed to associate an asserted identity with a PSK.

Path

ike-sainfo is a subelement under the ike element. The full path from the topmost ACLI prompt is: **security > ike > ike-sainfo.**

> **Note**
>
> This is a multiple instance configuration element.
> Configures an **ike-sainfo** instance named star.
>
> The default value for tunnel-remote-address (*) matches all IPv4 addresses.
>
> Non-default values specify IPsec tunnel mode running ESP, and identify the local tunnel endpoint.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ikev2-ipsec-wancom0-params

Parameters

The **ikev2-ipsec-wancom0-params** configuration element contains the following parameters:

name
A user-supplied name.

state
The state of this connection.

- Default: enabled
- Values: enabled | disabled

remoteip
The IPv4 or IPv6 address of the remote peer.

remotesubnet
The private subnet behind the remote participant. For example, 10.0.0.1/24 or 2001:DB8:0:56::/64. Defaults to a /32 for IPv4 or /128 for IPv6.

remoteproto
The transport protocol or protocols of the remote peer that will be protected within the tunnel.

- Default: ALL
- Values: TCP | UDP | ICMP | SCTP | IPV6-ICMP | ALL

remoteport
The port that the remote peer will use to communicate within the tunnel. For example, 1812 or 49. Use 0 to match any port.

- Default: 0
- Min: 0 | Max: 65535

localip
The IPv4 or IPv6 address of the local participant's public-network interface. The only accepted value is the IP address of wancom0.

localsubnet
The private subnet behind the local participant. The only accepted value is the wancom0 IP address with a /32 for IPv4 or /128 for IPv6.

localproto
The transport protocol or protocols of the local peer that will be protected within the tunnel.

- Default: ALL
- Values: TCP | UDP | ICMP | SCTP | IPV6-ICMP | ALL

localport
The port that the local peer will use to communicate within the tunnel. Use 0 to match any port.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Min: 0 | Max: 65535

auto
The action taken on IPsec startup. The 'start' action adds and establishes an IPsec connection. The 'ondemand' action establishes an IPsec connection only when an ingressing or egressing packet matches the connection's traffic parameters. The 'ignore' action causes no automatic IPsec startup operation.

- Default: ondemand
- Values: start | ondemand | ignore

ike-algorithms
The IKE algorithm used for IKE security association connections (phase 1). The format is `<cipher>-<hash>;<dhgroup>`. For example: `aes256-sha256;dh14`. Using the correct separator is required.

- Default: aes256-sha256;dh14
- Allowed ciphers: aes128, aes192, aes256, aes_ctr128, aes_ctr192, aes_ctr256, aes_gcm128, aes_gcm192, aes_gcm256
- Allowed hash: sha256, sha512
- Allowed DH: dh14, dh15, dh16, dh17, dh18

ipsec-protocol
The type of IPsec security association.

- Default: esp
- Values: ah | esp

ipsec-algorithms
The IPsec algorithms offered and accepted during phase 2 negotiation. The format is `<cipher>-<hash>[;<DH-group>]`. For example: `aes256-sha256;modp2048`. Using the correct separator is required.

- Default: aes256-sha256;modp2048
- Allowed ciphers: aes128, aes192, aes256, aes_ctr128, aes_ctr192, aes_ctr256
- Allowed hash: sha256, sha512, aes_xcbc
- Allowed DH: modp2048

pfs
Whether perfect forward secrecy is used.

- Default: yes
- Values: yes | no

authby
How the two endpoints authenticate each other. Use 'secret' for a pre-shared key; use 'never' if negotiation is never to be attempted or accepted; and use 'rsasig' for RSA authentication with SHA-1.

- Default: rsasig
- Values: secret | never | rsasig

ipsec-mode
The mode of the IPsec connection.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: tunnel
- Values:
  - tunnel—A host-to-host, host-to-subnet, or subnet-to-subnet tunnel
  - transport—A host-to-host tunnel.
  - passthrough—no IPsec processing
  - drop—Discard the packets.
  - reject—The packets are discarded and a diagnostic ICMP returned.

esn
Whether to enable extended sequence numbers for the IPsec SA. If 'either' is specified, the responder decides. If the SBC is the responder and 'either' is selected, the SBC picks 'no'.

- Default: no
- Values: yes | no | either

rekey
Whether a connection should be renegotiated when it is about to expire.

- Default: yes
- Values: no | yes

ipsec-sa-life-secs
The number of seconds an IPsec SA connection lasts.

- Default: 28800
- Min: 1 | Max: 86400

ike-sa-life-secs
The number of seconds an IKEv2 SA connection lasts.

- Default: 3600
- Min: 1 | Max: 86400

rekeymargin
The number of seconds before an SA expires during which to negotiate a new connection.

- Default: 10
- Min: 1 | Max: 86400

rekeyfuzz
The maximum percentage by which the rekeymargin should be randomly increased to randomize rekeying intervals.

- Default: 0
- Min: 0 | Max: 8640000

shared-password
The password for IKE PSK authentication.

local-certificate-profile-identity
Specify the identity of the **ike-certificate-profile** to use for the local peer. This string should match the Subject Alernative Name of the local **end-entity-certificate** attribute in the **ike-certificate-profile** element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

remote-certificate-identity
Specify the identity of the **ike-certificate-profile** to use for the remote peer. This string should match the Subject Alternative Name of the peer's certificate.

dpddelay
The number of seconds between DPD keepalive messages.

- Default: 0 (disabled)
- Min: 0 | Max: 999999999

dpdtimeout
The number of seconds to idle without hearing back from the peer.

- Default: 0
- Min: 0 | Max: 999999999

dpdaction
The action to be taken once a peer is declared dead.

- Default: hold
- Values: hold | clear | restart

Path

The **ikev2-ipsec-wancom0-params** configuration element is in the **security** element.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# ikev2-ipsec-wancom0-params
ORACLE(ikev2-ipsec-wancom0-params)#
```

ims-aka-profile

The ims-aka-profile configuration element establishes supports IP Media Subsystem-Authentication and Key Agreement, defined in 3GPPr7 (specifications in TS 33.203 and call flows in TS 24.228).

Parameters

name
Enter the name for this IMS-AKA profile

start-protected-client-port
Start value for the pool of port numbers available following a successful re-authentication. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system’s host processor.

- Default: 0
- Values: Min: 1025 | Max: 65535

end-protected-client-port
End value for the pool of port numbers available following a successful re-authentication. Ensure that this value is greater than the value assigned to start-protected-client-port. Note

Copyright © 2024, 2026, Oracle and/or its affiliates.

that the maximum supported pool contains 5 entries. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

- Default: 0
- Values: Min: 1025 | Max: 65535

protected-server-port
Enter the port number on which the Oracle Communications Session Border Controller receives protected messages; 0 disables the function. The protected server port should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

- Default: 0
- Values: Min: 1025 | Max: 65535

encr-alg-list
Enter the list of encryption algorithms

- Values: aes-cbc | null

auth-alg-list
Enter the list of authentication algorithms

- Default: hmac-sha-1-96

Path

ims-aka-profile is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **security** , and then **ims-aka-profile**.

> **Note**
>
> This is a multiple instance configuration element.

ipsec

The ipsec configuration element allows you to configure security policies and security associations on your Oracle Communications Session Border Controller.

Parameters

security-policy
Enter the security-policy configuration element.

security-association
Enter the security-association configuration element.

ipsec-global-config
Access the ipsec-global-config subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

ipsec is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal > security> ipsec.**

ipsec > ipsec-global-config

The ipsec-global-config subelement allows you to configure establish the parameters governing system-wide IPSec functions and behavior, including IPSec redundancy.

Parameters

red-ipsec-port
Enter the port on which the SBC should listen for redundancy IPSec synchronization messages

- Default: 0
- Values: 0 | 1994

red-max-trans
Enter the maximum number of redundancy transactions to retain on the active

- Default: 10000
- Values: Min: 0 / Max: 50000

red-sync-start-time
Enter the time in milliseconds before the system starts to send redundancy synchronization requests

- Default: 5000
- Min: 0 | Max: 999999999

red-sync-comp-time
Enter the time in milliseconds to define the timeout for subsequent synchronization requests once redundancy synchronization has completed

- Default: 1000
- Min: 0 | Max: 999999999

options
Enter the appropriate option name for the behavior you want to configure

Path

security-association is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: configure terminal > security> ipsec>security-association.

> **Note**
>
> This is a single instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ipsec > security-association

The security-association subelement allows you to configure a security association (SA), the set of rules that define the association between two endpoints or entities that create the secured communication.

Parameters

manual
Enter the manual subelement where you can manually configure a security association

Path

security-association is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **ipsec**, and then **security-association**.

ipsec > security-association > manual

The manual subelement is where you manually configure a security association on the Oracle Communications Session Border Controller.

Parameters

name
Enter the name for this security policy

spi
Set the security parameter index

- Default: 256
- Values: Min: 256 / Max: 4294967295

network-interface
Enter the network interface and VLAN where this security association applies in the form of: interface_name:VLAN

local-ip-address
Enter the local IP address to match for traffic selectors for this SA

remote-ip-addr
Enter the remote IP address to match for traffic selectors for this SA

local-port
Enter the local port to match for traffic selectors for this SA

remote-port
Enter the remote port to match for traffic selectors for this SA

- Default: 0
- Values: Min: 0 (disabled) | Max: 65535

trans-protocol
Select the transport protocol to match for traffic selectors for this SA

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: ALL
- Values: UDP | TCP | ALL | ICMP

ipsec-protocol
Select the IPsec protocol used for this SA

- Default: esp
- Values: esp | ah

direction
Set the direction of traffic this security association can apply to

- Default: both
- Values: in | out | both

ipsec-mode
Select the IPsec mode of this SA

- Default: transport
- Values: tunnel | transport

auth-algo
Select the IPsec authentication algorithm for this SA

- Default: hmac-sha-512
- Values: hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | null

enrc-algo
Enter the IPsec encryption algorithm for this SA

- Default: null
- Values: null | aes-128-cbc | aes-256-cbc | aes-128-ctr | aes-256-ctr

auth-key
Enter the authentication key for the previously chosen authentication algorithm for this SA

encr-key
Enter the encryption key for the previously chosen encryption algorithm for this SA

aes-ctr-nonce
Enter the AES nounce. This only applies if aes-128-ctr or aes-256-ctr are chosen as your encryption algorithm.

- Default: 0

tunnel-mode
Enter the tunnel-mode subelement

Path

security-association is a subelement under the ipsec element. The full path from the topmost ACLI prompt is:**configure-terminal > security > ipsec > security-association**

Copyright © 2024, 2026, Oracle and/or its affiliates.

ipsec > security-association > tunnel-mode

This configuration element allows you to configure the addresses in the security-association. These addresses represent the external, public addresses of the termination points for the IPSEC tunnel.

Parameters

local-ip-addr
Enter the local IP address of this tunnel mode profile

remote-ip-addr
Enter the remote IP address of this tunnel mode profile

Path

tunnel-mode is a subelement under the **ipsec>security-association** The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-association>tunnel-mode.** configure-terminal > security > ipsec > security-association>tunnel-mode.

ipsec > security-policy

This configuration element defines multiple policy instances with each policy defining match criteria and an operational action performed on matching traffic flows.

Parameters

name
Enter a unique identifier for this security-policy instance.

- Default: none
- Value: A valid configuration element name that is unique within the security-policy namespace.

network-interface
Enter the unique name of the network-interface supported by this security-policy instance. Identify the network interface by providing the interface name and VLAN ID separated by a colon; for example access:10.

- Default: None
- Values: Name and VLAN ID of an existing network-interface configuration element.

priority
Set the priority of this security-policy instance, where 0 is the highest priority.

- Highest priority: 0
- Lowest priority: 3071

local-ip-addr-match
Enter an IPv4 or IPv6 address; in conjunction with local-ip-mask and local-port-match, this parameter specifies address-based matching criteria for inbound traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Specifically, local-ip-addr-match works with local-ip-mask to define a range of inbound IP address subject t this security-policy instance. Using default values for both properties, the security-policy instance matches all applicable addresses.

- Default: 0.0.0.0
- Values: A valid IPv4 or IPv6 address; the special address value, 0.0.0.0 matches all IPv4 addresses.

remote-ip-addr-match
Enter an IPv4 or IPv6 address; in conjunction with remote-ip-mask and remote-port-match specifies address-based matching criteria for outbound traffic.

> **Note**
>
> Specifically, remote-ip-addr-match works with remote-ip-mask to define a range of outbound IP addresses subject to this security-policy instance. Using default values for both properties, the security-policy instance matches all applicable addresses.
>
> - Default: 0.0.0.0
> - Values: A valid IPV4 or IPv6 address; the special address value, 0.0.0.0 matches all IPv4 addresses.

local-port-match
Enter a port number, or the special value 0; in conjunction with local-ip-addr-match and local-ip-mask, the parameter specifies address-based matching criteria for inbound traffic.
The default value disables port-based matching, meaning port numbers are ignored in the default state.

- Default: 0 (disables port-based matching)
- Values: Min: 0 / Max: 65535

local-port-match-max
Enter a port number that specifies the maximum value for the local port to which the IPsec Security applies.

- Default: 65535
- Values: Min: 0 / Max: 65535

remote-port-match
Enter a port number, or the special value 0; in conjunction with remote-ip-addr-match and remote-ip-mask, this parameter specifies address-based matching criteria for outbound traffic.
The default value disables port-based matching, meaning port numbers are ignored in the default state.

- Default: 0 (disables port-based matching)
- Values: Min: 0 / Max: 65535

remote-port-match-max
Enter a port number that specifies the maximum value for the remote port to which the IPsec Security applies.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 65535
- Values: Min: 0 / Max: 65535

trans-protocol-match
Select a specified protocol or the special value all that specifies transport-protocol-based matching criteria for inbound and outbound traffic.
The default value all matches all supported transport layer protocols

- Default: all
- Values: all | ICMP | SCTP | TCP | UDP

direction
Select an indicator of the directionality of this security-policy instance.

- Default: both
- Values: both - the policy applies to all traffic. | in - the policy applies only to inbound traffic. | out - the policy applies only to outbound traffic.

local-ip-mask
Enter am IPv4 address; in conjunction with local-ipaddr-match and local-port-match, this parameter specifies address-based matching criteria for inbound traffic.
Specifically, local-ip-addr-match works with local-ip-mask to define a range of inbound IP addresses subject to this security-policy instance matches all IPv4 addresses.

- Default: 255.255.255.255
- Values: A dotted decimal IP address mask.

remote-ip-mask
Enter an IPv4 address; in conjunction with remote-ip-addr-match and remote-port-match, this parameter specifies address-based matching criteria for outbound traffic.
Specifically, remote-ipaddr-match works with remote-ip-mask to define a range of out IP addresses subject to this security-policy instance matches all IPv4 addresses.

- Default: 255.255.255.255
- Values: A valid IPv4 address mask

action
Select the process of trafficking that conforms to the match criteria specified by this security-policy instance.

- Default: ipsec
- Values: allow-forwards matching traffic but performs no security processing. | discard-discards matching traffic | ipsec-processes matching traffic per configured IPsec properties.

> **Note**
>
> srtp is not a supported value

outbound-sa-fine-grained-mask
not used for IKE operation.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ike-sainfo-name
Enter the name of the **ike-sainfo** configuration element assigned to this security-policy instance.

- Default: None
- Values: A valid configuration element name that is unique within the ike-sainfo namespace.

> **Note**
>
> The **ike-sainfo** configuration element identifies the algorithms and protocols available for the establishment if IP sec Security Associations (SA).

pre-fragmentation
Select, when the value of **action** is **ipsec**, whether to enable IPSec packet fragmentation before encryption. When enabled, the MSG fragments outbound jumbo packets before they can be transmitted and then encrypts the fragments so that each transmitted encrypted fragment packet has a valid Encapsulating Security Payload (ESP) header.

- Default: disabled
- Values: disabled | enabled

Path

security-policy is a subelement of the ipsec path. The full path from the topmost ACLI prompt is: configure terminal > security> ipsec>security-policy.

ipsec > security-policy > outbound-sa-fine-grained-mask

This configuration element allows you to configure a fine grained security policy.

Parameters

local-ip-mask
Enter the local IP address mask

- Default: 255.255.255.255

remote-ip-mask
Enter the remote IP address mask.

- Default: 255.255.255.255

local-port-mask
Enter the local port mask for this security policy.

- Default: 0
- Values: Min: 0 / Max: 65535

remote-port-mask
Enter the remote port mask for this security policy.

- Default: 0
- Values: Min: 0 / Max: 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

trans-protocol-mask
Enter the transport protocol mask for this security policy

- Default: 0
- Values: Min: 0 | Max: 65535

vlan-mask
Enter the VLAN ID mask

- Default: 0x000
- Values: 0x000 (disabled)-0xFFF

Path

outbound-sa-fine-grained-mask is a subelement under the ipsec>security-policy element. The full path from the topmost ACLI prompt is: **configure-terminal > security > ipsec > security-policy > outbound-sa-fine-grained-mask.**

iwf-config

The iwf-config element enables the H.323—SIP interworking (IWF) and provides a list of media profiles to use when IWF translations occur.

Parameters

state
Enable or disable the Oracle Communications Session Border Controller's IWF

- Default: disabled
- Values: enabled | disabled

media-profiles
Set the default media SDP profiles that Oracle Communications Session Border Controller uses for Slow Start IWF calls. This field does not have a relationship with the media-profiles field found in the h323-stack subelement, as the values configured there affect calls that take place entirely in H.323. This list must be populated with the SDP codec names.

- Values: • PCMU | PCMA | G722 | G723 | G726-32 | G728 | G729 | H261 | H263

logging
Enable or disable IWF-related SIP messages logging

- Default: disabled
- Values: enabled | disabled

add-reason-hdr
Enable or disable adding the Reason header to IWF calls

- Default: disabled
- Values: enabled | disabled

Path

iwf-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **iwf-config**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This is a single instance configuration element.

ldap-cfg-attributes

Use the **ldap-cfg-attributes** configuration element to set up the Active Directory attribute name, next hop for routing SIP requests, the realm for the next hop, a regular expression pattern, and a format for the attribute value.

Path

The **ldap-cfg-attributes** configuration element is in the **ldap-transactions** element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# ldap-config
ORACLE(ldap-config)# ldap-transactions
ORACLE(ldap-transactions)# ldap-cfg-attributes
ORACLE(ldap-cfg-attributes)#
```

Parameters

The **ldap-cfg-attributes** configuration element contains the following parameters:

name
Enter the Active Directory attribute name.

next-hop
Enter the Active Directory's next hop when routing SIP requests

realm
Enter the name of the realm associated with the next hop.

extraction-regex
Enter the regular expression pattern used to break down the string of digits in the phone number extracted from the request URI of the SIP request.

- Default: ^\\+?1?(\\d{3})(\\d{3})(\\d{4})$

value-format
Enter the format for the attribute value.

- Default: tel:+1$1$2$3

These format values are extracted from the phone number using the **extraction-regex** parameter. The default parameter is "tel:+1$1$2$3". This value assumes that the phone number is a North American phone number specified in the E.164 format, and it recreates the phone number in E.164 format.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ldap-transactions

Use the **ldap-transactions** configuration element to set up the application transaction type for LDAP, determine route priority in the route list, and specify the LDAP search queries in call routing.

Path

The **ldap-transactions** configuration element is in the **ldap-config** element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# ldap-config
ORACLE(ldap-config)# ldap-transactions
ORACLE(ldap-transactions)#
```

Parameters

The **ldap-transactions** configuration element contains the following parameters:

app-trans-type
Enter the application transaction type.

- Default: ad-call-routing
- Values: ad-call-routing

route-mode
Specify the route priority that the SBC uses in the route list.

- Default: exact-match-only
- Values: exact-match-only | attribute-order-only | exact-match-first
- exact-match-only—Create routes only for attributes with exact match.
- attribute-order-only—Create routes with route priority based on attribute order.
- exact-match-first—Create routes with route priority based on exact match first and then attribute order.

operation-type
Enter the LDAP attribute operation type.

- Default: or
- Values: and | or

ldap-cfg-attributes
Access the **ldap-cfg-attributes** configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

license

The license configuration element is used for configuring Oracle Communications Session Border Controller licenses.

Parameters

add
Add a license by entering a key obtained from your service representative.

no
Delete licenses by feature. You are prompted to choose a license for deletion based on license features.

Path

licenses is an element under the system-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **license**.

local-address-pool

The local-address-pool configuration element enables creation of local address pools, which can be used to provide a local (internal) address in response to remote requests for IP addresses.

Parameters

name
Enter a unique identifier for this local-address-pool instance.

- Default None
- Values A valid configuration element name that is unique within the local-address-pool namespace.

address-range
Access the address-range subelement.

dns-realm-id
Enter a DNS realm that supports this local-address-pool instance.

- Default: None
- Values: Name of an existing dns-realm configuration element.

data-flow-list
Enter a data-flow configuration element assaigned to this local-address-pool instance. This parameter specifies bandwidth availible to the pool of addresses specified by this local-address-pool instance.

- Default: None
- Values: Name of an existing data-flow configuration element local-address-pool is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure>terminal>security>ike>local-address-pool.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

local-address-pool is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure terminal > security > ike > local-address-pool**

> **Note**
>
> This is a multiple instance configuration element.

local-address-pool > address-range

The address-range configuration element specifies a single range of contiguous IPv4 addresses that are available to fulfill remote requests for a local address.

Parameters

network-address
In conjunction with this parameter defines a range of IPv4 addresses available for dynamic assignment.

- Default: Nome
- Values: A valid IPv4 network address.

subnet-mask
In conjunction with network-address, the parameter defines a range of IPv4 addresses available for dynamic assignment.

- Default: None
- Values: A valid IPv4 subnet mask

> **Note**
>
> The range of IPv4 addresses support only Class-B and Class-C subnet masks.

Path

local-address-pool, and then **address-range** is a subelement under the ike element. The full path from the topmost ACLI prompt: **configure-terminal**, and then **security**, and then **ike**, and then **local-address-pool**, and then **address-range**.

> **Note**
>
> This is a multiple instance configuration.

local-policy

The local-policy configuration element determines where session signaling messages are routed and/or forwarded.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

from-address
Enter the source IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded, or entered with a DS: prefix (dialed string).

An IPv6 address is valid for this parameter.

> **Note**
>
> This field adheres to the standard ACLI character limit of 1024, as documented herein.

to-address
Enter the destination IP address, POTS number, E.164 number, or hostname for the local-policy element. At least one address must be set within this list, but it can include as many addresses as necessary. This parameter may be wildcarded.

An IPv6 address is valid for this parameter.

> **Note**
>
> This field adheres to the standard ACLI character limit of 1024, as documented herein.

source-realm
Enter the realms used to determine how to route traffic. This list identifies incoming traffic on a realm and is used for routing by ingress realm via the local policy element. Source-realm entries must be a valid realm.

- Default: *

description
Provide a brief description of the local-policy configuration element

activate-time
Set the time when selected local-policy becomes valid

activate-time yyyy-mm-dd-hh:mm:ss

y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second

deactivate-time
Set the time when selected local-policy becomes invalid

activate-time yyyy-mm-dd-hh:mm:ss

y=year; m=month; d=day h=hour (24-hour clock) m=minute; s=second

state
Enable or disable the local-policy element

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- Values: enabled | disabled

parallel-forking
Enable or disable parallel forking on this local-policy.

- Default: disabled
- Values: enabled | disabled

policy-priority
Set the policy priority parameter for this local policy. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a SIP interface configuration element.

- Default: none
- Values: none | normal | non-urgent | urgent | emergency

next-hop

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Enter the next signaling host IP address, SAG, hostname, or ENUM config; ENUM is also an accepted value. You can use the following as next-hops:

- IPv4 address or IPv6 address of a specific endpoint
- Hostname or IPv4 address or IPv6 address of a configured session agent
- Group name of a configured session agent group

The group name of a configured session agent group must be prefixed with SAG: For example:

- policy-attribute: next-hop SAG:appserver
- policy-attribute: next-hop lrt:routetable
- policy-attribute: next-hop enum:lerg

realm

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Enter the egress realm, or the realm of the next hop. If traffic is routed using the local policy, and the selected route entry identifies an egress realm, then this realm field value will take precedence. This value must be a valid entry in a realm configuration.

Copyright © 2024, 2026, Oracle and/or its affiliates.

action

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Set this parameter to redirect if you want to send a redirect next-hop message back to the calling party with the information in the Contact. The calling party then needs to send an INVITE using that information.

- Default: none
- Values:
  - none—No specific action requested
  - replace-uri—To replace the Request-URI with the next hop
  - redirect—To send a redirect response with this next hop as contact

terminate-recursion

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Terminate route recursion with this next hop

- Default: disabled
- Values: enabled | disabled

app-protocol

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Select the signaling protocol used when sending messages to the configured next-hop. When the SBC receives an ingress signaling message and uses local policy to determine the message's destination, it will interwork the signaling between protocols (H.323<—>SIP or SIP<—>H.323) if the signaling type does not match the value configured in the app-protocol field.

- Default: ""
- Values: "" | SIP | H323 | MGCP | H248 | BGF | BFD | SCF | RTSP | DD | DIAMETER | IKE | NONE

Copyright © 2024, 2026, Oracle and/or its affiliates.

methods

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Enter the SIP methods you want to use for matching this set of policy attributes. Use a double-quoted string with space-separated items.

- Values: INVITE | REGISTER | PRACK | OPTIONS | INFO | SUBSCRIBE | NOTIFY | REFER | UPDATE | MESSAGE | PUBLISH

lookup

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Enable multistage local policy routing, or leave the parameter at the default single for single stage local policy routing.

- Default: single
- Values: single | multi

next-key

> **Note**
>
> This attribute is only present when the Routing entitlement is disabled.

Select the key to use for the next stage of local policy look-up.

- Values: $TO | $FROM | $PAI

Path

local-policy is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **local-policy**.

> **Note**
>
> This is a multiple instance configuration element.

local-policy > policy-attributes

The policy-attributes subelement in conjunction with local-policy make routing decisions for the session based on the next-hop field value.

Constraints

This element is only available when the Routing entitlement is enabled.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

next-hop
Enter the next signaling host IP address, SAG, hostname, or ENUM config; ENUM is also an accepted value. You can use the following as next-hops:

- IPv4 address or IPv6 address of a specific endpoint
- Hostname or IPv4 address or IPv6 address of a configured session agent
- Group name of a configured session agent group

The group name of a configured session agent group must be prefixed with SAG: For example:

- policy-attribute: next-hop SAG:appserver
- policy-attribute: next-hop lrt:routetable
- policy-attribute: next-hop enum:lerg

> **Note**
>
> The **next-hop** parameter does not accept values starting with *.

realm
Enter the egress realm, or the realm of the next hop. If traffic is routed using the local policy, and the selected route entry identifies an egress realm, then this realm field value will take precedence. This value must be a valid entry in a realm configuration.

action
Set this parameter to redirect if you want to send a redirect next-hop message back to the calling party with the information in the Contact. The calling party then needs to send an INVITE using that information.

- Default: none
- Values:
  - none—No specific action requested
  - replace-uri—To replace the Request-URI with the next hop
  - redirect—To send a redirect response with this next hop as contact

carrier
Enter the carrier for this local-policy. Carrier names are arbitrary names used to affect the routing of SIP signaling messages based on their being specified in the local-policy, session-agent, and the sip-config. These carrier names are global in scope, especially if they are exchanged in TRIP.

start-time
Set the time of day these policy attributes considered for preference determination

- Default: 0000
- Values: Min: 0000 | Max: 2400

end-time
Set the time of day these policy attributes cease to be considered for preference determination

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 2400
- Values: Min: 0000 | Max: 2400

days-of-week
Enter the combination of days of the week plus holidays that policy attributes can be considered for preference determination. A holiday entry coincides with a configured holiday. At least one day or holiday must be specified in this field.

- Default: U-S
- Values:
  - U—Sunday
  - M—Monday
  - T—Tuesday
  - W—Wednesday
  - R—Thursday
  - F—Friday
  - S—Saturday
  - H—Holiday

cost
Enter the cost configured for local policy to rank policy attributes. This field represents the cost of a route relative to other routes reaching the same destination address.

- Default: 0
- Values: Min: 0 | Max: 999999999

state
Enable or disable these policy attributes as part of the local-policy element

- Default: enabled
- Values: enabled | disabled

app-protocol
Select the signaling protocol used when sending messages to the configured next-hop. When the Oracle Communications Session Border Controller receives an ingress signaling message and uses local policy to determine the message's destination, it will interwork the signaling between protocols (H.323<—>SIP or SIP<—>H.323) if the signaling type does not match the value configured in the app-protocol field.

- Values: H323 | SIP

media-profiles
Enter the names of media-profile elements related to the policy attribute. Media profiles define a set of media formats that the Oracle Communications Session Border Controller can recognize in SDP. This list does not have to be configured. However, if this list is configured, there can be as many entries within it as necessary.

terminate-recursion
Terminate route recursion with this next hop

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

methods
Enter the SIP methods you want to use for matching this set of policy attributes

lookup
Enable multistage local policy routing, or leave the parameter at the default single for single stage local policy routing.

- Default: single
- Values: single | multi

next-key
Select the key to use for the next stage of local policy look-up.

- Values: $TO | $FROM | $PAI

auth-user-lookup
Enter the name of the auth-attributes in your target realm.

eloc-str-lkup
Set this parameter to enabled for the Oracle Communications Session Border Controller to parse the emergency location string, as received in a CLF Line Identifyier AVP, for emergency LRT lookup.

- Default: enabled
- Values: enabled | disabled

eloc-str-match
Set this parameter to the attribute name found in thelocation-string whose value will be used as a lookup key in the LRT named in the next-hop parameter.

- Values: <string> string used as key for emergency LRT lookup

move
Change the order in which policy-attributes are processed.
The command syntax:

```
move <from-position> <to-position>
```

Path

policy-attributes is a subelement under the local-policy element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **local-policy** , and then **policy-attributes**.

> **Note**
>
> You must select a local-policy element to which you want to add policy attributes before you enter those elements. If you do not select a local-policy element prior to entering configurations for the policy attributes, your information will be lost. This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

local-response-map

The local-response-map configuration element is used for RFC3326 support.

Parameters

entries
Enter the entries configuration subelement.

delete
Remove the specified response map entry type.

edit
This parameter is unsupported.

Path

local-response-map is an element under the session router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **local-response-map**.

local-response-map > entries

Use the entries subelement to add a local response map entry for RFC3326 support. Each entry into the map allows for the configuration of a unique SIP response code and description in the **sip-status** and **sip-reason** fields, which will appear in the “Status-line” of the SIP response. The **q850-cause** and **q850-reason** fields are part of the optional “Reason Header” which is added to the SIP response if enabled through the **sip-config** configuration element.

Parameters

local-error
Enter the local error condition. When not specified, the sip-reason field in the SIP response defaults to "Service Unavailable".

Value	Description
`invalid-message`	Maps responses for locally rejected invalid SIP messages, including malformed requests or failed trunk group URI validation.
`cpu-overload`	Maps responses when the SBC rejects a request because CPU overload protection is active.
`media-released`	Maps Reason-header behavior for locally generated BYE requests when media or the dialog is released by the SBC.
`media-not-allocated`	Maps responses when media allocation fails and no more specific media error applies.
`enum-void-route`	Maps responses when ENUM or local routing returns no usable route for the request.
`monthly-minutes-exceed`	Maps responses when monthly minutes admission control rejects an INVITE.
`next-hop-sa-oos`	Maps responses when the selected next-hop session agent is out of service, standby, disabled, or otherwise unavailable.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Value	Description
recv-sa-exc-constraints	Maps ingress rejections when the previous-hop session agent exceeds configured session constraints.
recv-sip-int-exc-constraints	Maps ingress rejections when the receiving SIP interface exceeds configured session constraints.
next-hop-sa-exc-constraints	Maps egress rejections when the next-hop session agent exceeds configured session constraints.
next-hop-sip-int-exc-constraints	Maps egress rejections when the next-hop SIP interface exceeds configured session constraints.
realm-bw-exc-poly-serv-reject	Maps responses when realm bandwidth CAC fails or the external bandwidth policy server rejects the request.
no-steering-pool-ports-available	Maps media failures where the media manager cannot allocate a steering-pool port.
no-media-flow-found	Maps media failures where the requested media flow cannot be found.
no-media-interface-found-for-realm	Maps media failures where no media interface is available for the realm.
media-recording-failure	Maps media allocation failures caused by call recording setup problems.
allow-anonymous-rejection	Maps responses when anonymous endpoint policy rejects the previous hop or request.
sdp-address-mismatch	Maps responses when SDP address correlation rejects a non-HNT request because the SDP address does not match the source address.
request-method-throttled	Maps responses when method-based constraints or throttling reject the request.
reg-cache-full	Maps REGISTER responses when the registration cache limit is exceeded; the code also adds Retry-After when configured.
per-user-cac-exc-sessions	Maps responses when per-user CAC rejects a non-priority call because the user session count limit is exceeded.
per-user-nsep-exc-rate	Maps responses when NS/EP or MPS per-user CAC session-rate limits are exceeded.
recv-conditional-cac-reject	Maps responses when conditional CAC rejects the request, including conditional bandwidth failure cases.
ldap-unavailable	Maps responses when LDAP lookup processing reports the LDAP server unavailable and LDAP failure mapping is enabled.
allowed-elements-profile-rejection	Maps responses when allowlist or allowed-elements-profile rules reject the SIP request.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Value	Description
recording-required	Maps responses when recording is mandatory but a recording target or recording session cannot be established.
hss-lir-timeout	Maps responses when an HSS Cx Location-Info-Request times out during routing.
hss-lir-failure	Maps responses when an HSS Cx Location-Info-Request fails for a non-timeout reason.
transcoding-licensed-session-capacity-reached	Maps responses when transcoding is needed but the licensed transcoding session capacity is exhausted.
dsp-resource-limit-reached	Maps responses when transcoding or media service setup fails because no DSP resources are available.
licensed-session-capacity-reached	Maps responses when the SBC licensed session capacity is reached.
fraud-protection-reject-call	Maps responses when the Fraud Protection Engine tags the user and instructs the SBC to drop the call.
rx-rar-loss-of-bearer	Maps Diameter Rx RAR Specific-Action: indication of loss of bearer; default SIP mapping is 503 if no local entry exists.
rx-rar-release-of-bearer	Maps Diameter Rx RAR Specific-Action: indication of release of bearer; default SIP mapping is 503 if no local entry exists.
rx-rar-out-of-credit	Maps Diameter Rx RAR Specific-Action: out of credit; default SIP mapping is 503 if no local entry exists.
rx-rar-failed-resources-allocation	Maps Diameter Rx RAR Specific-Action: failed resource allocation; default SIP mapping is 503 if no local entry exists.
rx-rar-access-network-info-reporting_failure	Maps Diameter Rx RAR Specific-Action: access network information reporting failure; default SIP mapping is 503 if no local entry exists.
rx-asr-bearer-released	Maps Diameter Rx ASR Abort-Cause: bearer released; default SIP mapping is 503 if no local entry exists.
rx-asr-insufficient-server-resources	Maps Diameter Rx ASR Abort-Cause: insufficient server resources; default SIP mapping is 503 if no local entry exists.
rx-asr-insufficient-bearer-resources	Maps Diameter Rx ASR Abort-Cause: insufficient bearer resources; default SIP mapping is 503 if no local entry exists.
rx-asr-ps-to-cs-handover	Maps Diameter Rx ASR Abort-Cause: packet-switched to circuit-switched handover; default SIP mapping is 503 if no local entry exists.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Value	Description
rx-asr-sponsored-data-connectivity-disallowed	Maps Diameter Rx ASR Abort-Cause: sponsored data connectivity disallowed; default SIP mapping is 503 if no local entry exists.
bad-request-400	Maps locally generated SIP 400 Bad Request responses to configured SIP/Q.850 values and Reason-header text.
unauthorized-401	Maps locally generated SIP 401 Unauthorized responses to configured SIP/Q.850 values and Reason-header text.
payment-required-402	Maps locally generated SIP 402 Payment Required responses to configured SIP/Q.850 values and Reason-header text.
forbidden-403	Maps locally generated SIP 403 Forbidden responses to configured SIP/Q.850 values and Reason-header text.
not-found-404	Maps locally generated SIP 404 Not Found responses to configured SIP/Q.850 values and Reason-header text.
method-not-allowed-405	Maps locally generated SIP 405 Method Not Allowed responses to configured SIP/Q.850 values and Reason-header text.
not-acceptable-406	Maps locally generated SIP 406 Not Acceptable responses to configured SIP/Q.850 values and Reason-header text.
proxy-authentication-required-407	Maps locally generated SIP 407 Proxy Authentication Required responses to configured SIP/Q.850 values and Reason-header text.
request-timeout-408	Maps locally generated SIP 408 Request Timeout responses to configured SIP/Q.850 values and Reason-header text.
conflict-409	Maps locally generated SIP 409 Conflict responses to configured SIP/Q.850 values and Reason-header text.
gone-410	Maps locally generated SIP 410 Gone responses to configured SIP/Q.850 values and Reason-header text.
length-required-411	Maps locally generated SIP 411 Length Required responses to configured SIP/Q.850 values and Reason-header text.
request-entity-too-large-413	Maps locally generated SIP 413 Request Entity Too Large responses to configured SIP/Q.850 values and Reason-header text.
request-uri-too-large-414	Maps locally generated SIP 414 Request-URI Too Large responses to configured SIP/Q.850 values and Reason-header text.
unsupported-media-type-415	Maps locally generated SIP 415 Unsupported Media Type responses to configured SIP/Q.850 values and Reason-header text.
unsupported-uri-scheme-416	Maps locally generated SIP 416 Unsupported URI Scheme responses to configured SIP/Q.850 values and Reason-header text.
unknown-resource-priority-417	Maps locally generated SIP 417 Unknown Resource-Priority responses to configured SIP/Q.850 values and Reason-header text.
bad-extension-420	Maps locally generated SIP 420 Bad Extension responses to configured SIP/Q.850 values and Reason-header text.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Value	Description
extension-required-421	Maps locally generated SIP 421 Extension Required responses to configured SIP/Q.850 values and Reason-header text.
session-interval-too-small-422	Maps locally generated SIP 422 Session Interval Too Small responses to configured SIP/Q.850 values and Reason-header text.
interval-too-brief-423	Maps locally generated SIP 423 Interval Too Brief responses to configured SIP/Q.850 values and Reason-header text.
temporarily-unavailable-480	Maps locally generated SIP 480 Temporarily Unavailable responses to configured SIP/Q.850 values and Reason-header text.
call/transaction-does-not-exist-481	Maps locally generated SIP 481 Call/Transaction Does Not Exist responses to configured SIP/Q.850 values and Reason-header text.
loop-detected-482	Maps locally generated SIP 482 Loop Detected responses to configured SIP/Q.850 values and Reason-header text.
too-many-hops-483	Maps locally generated SIP 483 Too Many Hops responses to configured SIP/Q.850 values and Reason-header text.
address-incomplete-484	Maps locally generated SIP 484 Address Incomplete responses to configured SIP/Q.850 values and Reason-header text.
ambiguous-485	Maps locally generated SIP 485 Ambiguous responses to configured SIP/Q.850 values and Reason-header text.
busy-here-486	Maps locally generated SIP 486 Busy Here responses to configured SIP/Q.850 values and Reason-header text.
request-terminated-487	Maps locally generated SIP 487 Request Terminated responses to configured SIP/Q.850 values and Reason-header text.
not-acceptable-here-488	Maps locally generated SIP 488 Not Acceptable Here responses to configured SIP/Q.850 values and Reason-header text.
bad-event-489	Maps locally generated SIP 489 Bad Event responses to configured SIP/Q.850 values and Reason-header text.
request-pending-491	Maps locally generated SIP 491 Request Pending responses to configured SIP/Q.850 values and Reason-header text.
undecipherable-493	Maps locally generated SIP 493 Undecipherable responses to configured SIP/Q.850 values and Reason-header text.
security-agreement-required-494	Maps locally generated SIP 494 Security Agreement Required responses to configured SIP/Q.850 values and Reason-header text.
internal-server-error-500	Maps locally generated SIP 500 Internal Server Error responses to configured SIP/Q.850 values and Reason-header text.
not-implemented-501	Maps locally generated SIP 501 Not Implemented responses to configured SIP/Q.850 values and Reason-header text.
bad-gateway-502	Maps locally generated SIP 502 Bad Gateway responses to configured SIP/Q.850 values and Reason-header text.
service-unavailable-503	Maps locally generated SIP 503 Service Unavailable responses to configured SIP/Q.850 values and Reason-header text.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Value	Description
gateway-timeout-504	Maps locally generated SIP 504 Gateway Timeout responses to configured SIP/Q.850 values and Reason-header text.
version-not-supported-505	Maps locally generated SIP 505 Version Not Supported responses to configured SIP/Q.850 values and Reason-header text.
message-too-large-513	Maps locally generated SIP 513 Message Too Large responses to configured SIP/Q.850 values and Reason-header text.
precondition-failure-580	Maps locally generated SIP 580 Precondition Failure responses to configured SIP/Q.850 values and Reason-header text.
busy-everywhere-600	Maps locally generated SIP 600 Busy Everywhere responses to configured SIP/Q.850 values and Reason-header text.
decline-603	Maps locally generated SIP 603 Decline responses to configured SIP/Q.850 values and Reason-header text.
does-not-exist-anywhere-604	Maps locally generated SIP 604 Does Not Exist Anywhere responses to configured SIP/Q.850 values and Reason-header text.
not-acceptable-606	Maps locally generated SIP 606 Not Acceptable responses to configured SIP/Q.850 values and Reason-header text.
unwanted-607	Maps locally generated SIP 607 Unwanted responses to configured SIP/Q.850 values and Reason-header text.
rejected-608	Maps locally generated SIP 608 Rejected responses to configured SIP/Q.850 values and Reason-header text.
sip-locally-generated-bye	Maps Reason-header behavior for BYE requests originating from the SBC when no more specific media-release mapping is configured.
sip-locally-generated-cancel	Maps Reason-header behavior for CANCEL requests originating from the SBC, which have no response status of their own.
sip-locally-generated-cancel-for-parallel-fork	Maps Reason-header behavior for CANCEL requests originating from the SBC that clear other legs after a parallel-forked call completes elsewhere.

sip-status
Enter the SIP response code to use for this error.

- Default: 0
- Values: Min: 100 / Max: 699

q850-cause
Enter the Q.850 cause code.

- Default: 0
- Values: Min: 0 / Max: 2147483647

sip-reason
Enter the SIP response code description.

q850-reason
Enter the Q850 cause code description.

Copyright © 2024, 2026, Oracle and/or its affiliates.

method
Enter the name of the locally generated SIP failure response message you want to map to a 200 OK. When this parameter is left blank, the SIP registration response mapping feature is turned off.

register-response-expires
Enter the time, in seconds, you want to use for the expires time when mapping the SIP method you identified in the method parameter.

- Values: Min: 0 | Max: 999999999

Path

local-response-map-entries is an subelement under the local-response-map configuration element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **local-response-map** , and then **entries**.

local-routing-config

The local-routing-config element allows you to configure local route tables, giving the Oracle Communications Session Border Controller the ability to determine nest hops and map E.164 to SIP URIs locally, providing extensive flexibility for routing.

Note: Entering XML comments on the same line as LRT XML data is not currently supported.

Parameters

name
Enter a unique identifier for the local route table. This is the name you use to refer to this local route table when you configure policy attributes, This is a required parameter.

file-name
Enter the name for the file from which the database corresponding to this local route table is created. You should use the **.gz**format, and the file should be placed in the **/code/lrt/**directory. This is a required parameter.

prefix-length
Enter the number of significant digits/bits to be used for lookup and cache storage.

- Default: 0
- Value: Min:0 | Max 999999999

string-lookup
Sets the Oracle Communications Session Border Controller to perform LRT lookups on table keys of a string data type. Leave this parameter to its default as disabled to continue using E.164 type lookups.

- Default: disabled
- Values: enabled | disabled

retarget-requests
When set to enabled, the Oracle Communications Session Border Controller replaces the Request-URI in the outgoing request. When set to disabled, the Oracle Communications Session Border Controller routes the request by looking to the Route header to determine where to send the message.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- Values: enabled | disabled

match-mode
Determines how the Oracle Communications Session Border Controller makes amongst LRT entries.

- Default: exact
- Values:
  - exact-When searching the applicable LRT, the search and table keys must be an exact match.
  - best-The longest matching table key in the LRT is the chosen match.
  - all-The all mode makes partial matches where the table's key value is a prefix of the lookup key. For example, a lookup in the following table with a key of 123456 returns entries 1, 2, and 4. The 'all' mode incurs a performance penalty because it performs multiple searches of the tables with continually shortened lookup keys to find all matching entries. This mode also returns any exact matches too.

Path

local-routing-configis an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > local-routing-config.**

media-manager-config

This media-manager-config element defines parameters used in the media steering functions performed by the SBC including the flow timers.

Parameters

state
Enable or disable media management functionality

- Default: enabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

latching
Enable or disable the SBC obtaining the source of the first packet received for a dynamic flow. This parameter is only applicable to dynamic flows. If packet source is unresolved, but SBC expects a packet, it will use newly arrived packet’s source address if latching is enabled. All subsequent packets for the dynamic flow must come from the “latched” source address; otherwise, the packets are dropped.

- Default: enabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

flow-time-limit
Enter the total time limit in seconds for the flow. The SBC notifies the signaling application when this time limit is exceeded. This field is only applicable to dynamic flows. A value of 0 seconds disables this function and allows the flow to continue indefinitely.

- Default: 86400
- Values: Min: 0 / Max: 999999999

initial-guard-timer
Enter the time in seconds allowed to elapse before first packet of a flow arrives. If first packet does not arrive within this time limit, SBC notifies the signaling application. This field is only applicable to dynamic flows. A value of 0 seconds indicates that no flow guard processing is required for the flow and disables this function.

- Default: 300
- Values: Min: 0 / Max: 999999999

subsq-guard-timer
Enter the maximum time in seconds allowed to elapse between packets in a flow. The SBC notifies the signaling application if this timer is exceeded. This field is only applicable to dynamic flows. A field value of zero seconds means that no flow guard processing is required for the flow and disables this function.

- Default: 300
- Values: Min: 0 / Max: 999999999

tcp-flow-time-limit
Enter the maximum time in seconds that a media-over-TCP flow can last

- Default: 86400
- Values: Min: 0 / Max: 999999999

tcp-initial-guard-timer
Enter the maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow

- Default: 300
- Values: Min: 0 / Max: 999999999

tcp-subsq-guard-timer
Enter the maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets

- Default: 300
- Values: Min: 0 / Max: 999999999

tcp-number-of-ports-per-flow
Enter the number of ports, inclusive of the server port, to use for media over TCP. The total number of supported flows is this value minus one.

- Default: 2
- Values: Min: 2 / Max: 5

Copyright © 2024, 2026, Oracle and/or its affiliates.

hnt-rtcp
Enable or disable support of RTCP when the SBC performs HNT. If disabled, the SBC will only do RTP for endpoints behind a NAT. If enabled, the SBC will add a separate CAM entry for the RTCP flow so that it can send the RTCP back to the endpoint behind the NAT.

- Default: disabled
- Values: enabled | disabled

algd-log-level
Select the log level for the appropriate process

- Default: notice
- Values:
  - emergency
  - critical
  - major
  - minor
  - warning
  - notice
  - info
  - trace
  - debug
  - detail

mbcd-log-level
Select the log level for the MBCD process

- Default: notice
- Values:
  - notice
  - emergency
  - critical
  - major
  - minor
  - warning
  - notice
  - info
  - trace
  - debug
  - detail

red-flow-port
Enter the number of the port for checkpointing media flows associated with the HA interface. Setting the red-flow-port value to 0 disables media flow HA.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 1985
- Values: Min: 1025 / Max: 65535

> **Note**
>
> This parameter is not RTC supported.

red-mgcp-port
Enter the number of the port on which the system listens for redundancy mgcp sync messages. Setting the red-mgcp-port value to 0 disables MGCP flow HA.

- Default: 1986
- Values: 0 is disabled - Min: 1025 / Max: 65535

red-max-trans
Enter the maximum number of redundancy sync transactions to keep on active.
Default: 10000

- Default: 10000
- Min: 0 / Max: 50000

red-sync-start-time
Timeout in milleseconds that the system uses to check the transition from standby to active. After this interval starts sending redundancy sync requests.

- Default: 5000
- Min: 0 / Max: 4294967295

red-sync-comp-time
Timeout in milleseconds that the system waits after a redundancy sync has finished before it issues subsequent sync requests.

- Default: 1000
- Min: 0 / Max: 4294967295

media-policing
Enable or disable the media policing feature

- Default: enabled
- Values: enabled | disabled

max-arp-rate
Specifies the maximum percentage of bandwidth the system may use for ARP traffic.

- Default: 10
- Min: 0 / Max: 100

max-untrusted-signaling
Specifies the maximum percentage of signaling bandwidth the system can use for untrusted hosts.

- Default: 100
- Min: 0 / Max: 100

Copyright © 2024, 2026, Oracle and/or its affiliates.

min-untrusted-signaling
Specifies the minimum percentage of signaling bandwidth the system can use for untrusted hosts.

- Default: 30
- Min: 0 / Max: 100

max-signaling-bandwidth
Enter the maximum signaling bandwidth allowed to the host-path in bytes per second

- On the AP3820, AP4500, and AP4600:
  - Default: 1000000
  - Values: Min: 71000 / Max: 10000000
- On the AP6300:
  - Default: 4000000
  - Values: Min: 71000 / Max: 40000000

app-signaling-bandwidth
Select the percentage of the untrusted bandwidth reserved for specific application messages. Currently the only supported application message is NCS.

- Default: 0
- Values: Min: 1 / Max: 100

tolerance-window
Enter the tolerance window size in seconds used to measure host access limits.

- Default: 30
- Values: Min: 0 / Max: 999999999

untrusted-drop-threshold
Percent drop count threshold for untrusted hosts at which the system generates an alarm.

- Default: 0 (Disabled)
- Values: Min: 0 / Max: 100

trusted-drop-threshold
Percent drop count threshold for trusted and dynamic trusted hosts at which the system generates an alarm and, assuming associated configuration, an SNMP trap.

- Default: 0 (Disabled)
- Values: Min: 0 / Max: 100

acl-monitor-window
The time window, after which the system resets its ACL drop counters, and generates a trap if trusted or untrusted ACLs have exceeded their configured drop threshold.

- Default: 30
- Values: Min: 5 / Max: 3600 seconds

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not real-time configurable. Reboot after setting this parameter.

trap-on-demote-to-deny
Enable or disable the SBC to send a trap in the event of an endpoint demption from untrusted to deny.

- Default disabled
- Values enabled | disabled

trap-on-demote-to-untrusted
Enable for the SBC to send a trap in the event of an endpoint demption from trusted to untrusted.

- Default: disabled
- Values: enabled | disabled

syslog-on-demote-to-deny
Enable or disable the SBC to send a message to the syslog when an endpoint is demoted from untrusted to deny.

- Default: disabled
- Values: enabled | disabled

syslog-on-demote-to-untrusted
Enable or disable the SBC to send a message to the syslog when an endpoint is demoted from trusted to untrusted.

- Default: disabled
- Values: enabled | disabled

rtcp-rate-limit
Enter the maximum speed in bytes per second for RTCP traffic

- Default: 0
- Values: Min: 0 | Max: 125000000

syslog-on-call-reject
Enables generation of a syslog message in response to the rejection of a SIP call.

- Default: disabled
- Values: enabled | disabled

anonymous-sdp
Enable or disable username and session name fields anonymous in SDP

- Default: disabled
- Values: enabled | disabled

arp-msg-bandwidth
Enter the maximum bandwidth that can be used by an ARP message

- Default: 32000

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 8192 | Max: 200000

fragment-msg-bandwidth
(Only available on the Acme Packet 3820 and Acme Packet 4500)
Enter the maximum bandwidth that can be used by IP fragment messages

- Default: 0
- Values: Min: 0 (fragment packets are treated as untrusted bandwidth); 2000 | Max: 10000000

rfc2833-timestamp
Enable or disable use of a timestamp value calculated using the actual time elapsed since the last RTP packet for H.245 to 2833 DTMF interworking

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> Timestamp and duration changes will not take effect when the 2833 timestamp (rfc-2833-timestamp) and default-2833-duration parameter is altered in the media manager configuration during a SIP INFO to DTMF Interworking scenario.

default-2833-duration
Enter the time in milliseconds for the SBC to use when receiving an alphanumeric UII or SIP INFO with no specified duration.

- Default: 100
- Values: Min: 50 | Max: 5000

> **Note**
>
> Timestamp and duration changes will not take effect when the 2833 timestamp (rfc-2833-timestamp) and default-2833-duration parameter is altered in the media manager configuration during a SIP INFO to DTMF Interworking scenario.

rfc2833-end-pkts-only-for-non-sig
Enable this parameter if you want only the last three end 2833 packets used for non-signaled digit events. Disable this parameter if you want the entire start-interim-end RFC 2833 packet sequence for non-signaled digit events.

- Default: enabled
- Values: enabled | disabled

translate-non-rfc2833-event
Enable or disable the SBC's ability to translate non-rfc2833 events.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

media-supervision-traps
The SBC will send the following trap when the media supervision timer has expired:

```
apSysMgmtMediaSupervisionTimerExpTrap NOTIFICATION-TYPE
OBJECTS { apSysMgmtCallId }
STATUS current
```

- Default: disabled
- Values: enabled | disabled

dnsalg-server-failover
Enable or disable allowing DNS queries to be sent to the next configured server, even when contacting the SBC's DNS ALG on a single IP address; uses the transaction timeout value set in the dns-server-attributes configuration (part of the dns-config).

- Default: disabled
- Values: enabled | disabled

reactive-transcoding
Enable or disable SBC's ability to pre-book a transcoding resource during the SDP offer.

- Default: disabled
- Values: enabled | disabled

dos-guard-window
Set the number of seconds that define the window of time for measuring traffic volume within which the DoS alert thresholds may be triggered. When the window expires, the threshold counters revert to zero.

- Default: 5 seconds
- Values: Min: 1 / Max: 30

untrusted-minor-threshold
Set the percentage of the untrusted bandwidth that triggers a minor alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

untrusted-major-threshold
Set the percentage of the untrusted bandwidth that triggers a major alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

untrusted-critical-threshold
Set the percentage of the untrusted bandwidth that triggers a critical alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 / Max: 100

trusted-minor-threshold
Set the percentage of the trusted bandwidth that triggers a minor alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

trusted-major-threshold
Set the percentage of the trusted bandwidth that triggers a major alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

trusted-critical-threshold
Set the percentage of the trusted bandwidth that triggers a critical alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

arp-minor-threshold
Set the percentage of the arp bandwidth that triggers a minor alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

arp-major-threshold
Set the percentage of the arp bandwidth that triggers a major alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

arp-critical-threshold
Set the percentage of the arp bandwidth that triggers a critical alert for this threshold. When triggered, the system sends an alarm and a trap. Set the value to zero to disarm this threshold for alert events.

- Default: 0
- Values: Min: 0 / Max: 100

xcode-fax-max-rate
Specifies the maximum supported fax rate in bits per second.

- Default: 14400
- unlimited

Copyright © 2024, 2026, Oracle and/or its affiliates.

- 2400
- 4800
- 7200
- 9600
- 12000
- 14400

home-realm-id
This parameter has been deprecated

percent-sub
This parameter has been deprecated

pss-wd-key
This parameter has been deprecated

Path

Path: **media-manager-config** is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , **media-manager**, **media-manager**.

> **Note**
>
> This is a single instance configuration element.

Options

Refer to Option Configuration in Chapter 1, *How to use the ACLI* for instructions on how to configure options.

unique-sdp-id
Enables or disables codec negotiation by updating the SDP session ID and version number. When enabled, the SBC will hash the session ID and IP address of the incoming SDP with the current date/time of the SBC in order to generate a unique session ID.

active-arp
When enabled, this option causes all ARP entries to get refreshed every 20 minutes.

> **Note**
>
> As a security measure, in order to mitigate the effect of the ARP table reaching its capacity, configuring active-arp is advised.

use-rtp-marker-bit
When enabled, if the RTP sequence number in an ingress packet is either a duplicate number or increments more than one from the previous RTP sequence number, the SBC checks the ingress RTP packet for a marker bit. If a marker bit is set, the packet is treated as the first packet in a new media sequence, and QoS reporting does not record the sequence number change as RTP packet loss in the CDR.

Copyright © 2024, 2026, Oracle and/or its affiliates.

If a marker bit is not set, or the option is disabled, QoS reporting records jumps in RTP sequence number of less than 3000 as packet loss in the CDR. QoS reporting cannot accurately calculate packet loss for duplicates or jumps of 3000 or more without a marker bit.

media-policy

The media-policy element sets the TOS/DiffServ values that define an individual type or class of service.

Parameters

name
Name of this media policy.

tos-settings
Enter into the tos-values subelement.

rtp-ttl
Specifies the number of hops the packet can traverse before being dropped.

- Default: zero (disabled)
- Values: 0 - 255

Path

media-policy is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **media-policy**.

> **Note**
>
> This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Oracle Communications Session Border Controller. Media policies can be chosen on a per-realm basis.
> This is a multiple instance configuration element.

media-policy > tos-settings

The tos-settings configuration subelement bases media classification on type and subtype to create any media type combination allowed by IANA standards.

Parameters

media-type
Enter the type of media to use for this set of TOS settings

- Default: None
- Values: Any IANA-defined media type, such as: audio, image, model

media-sub-type
Enter the media sub-type to use for the specified media type

- Default: None

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Any of the media sub-types IANA defines for the selected media type

media-attribute
Enter a list of one or more media attributes that will match in the SDP

- Default: None

tos-values
Enter the TOS value to apply to matching traffic

- Default: 0x00 (must be a decimal or hexadecimal value)
- Values: Range from 0 - 255 or 0x00 to 0xFF

Path

tos-settings is a subelement under the media-policy element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **media-policy**>**tos-settings**.

> **Note**
>
> This configuration element sets the Packet Marking for Media features and defines an individual type or class of service for the Oracle Communications Session Border Controller. Media policies can be chosen on a per-realm basis.
> This is a multiple instance configuration element.

media-profile

Parameters

name
Enter the encoding name used in the SDP rtpmap attribute. This is a required field. No two media-profile elements can have the same name field value. SILK and opus are supported values as of S-CZ7.3.0.

media-type
Select the type of media used in SDP m lines

- Values:
  - audio
  - video
  - application
  - data
  - image
  - text

payload-type
Enter the format in SDP m lines. No payload type number is assigned for newer, dynamic codecs. For RTP/AVP media-profile elements, this field should only be configured when there is a standard payload type number that corresponds to the encoding name. Otherwise, this field should be left blank. This field is used by the system to determine the encoding type

Copyright © 2024, 2026, Oracle and/or its affiliates.

when the SDP included with a session identifies the standard payload type on the m line, but does not include an a-rtpmap entry.

transport
Select the type of transport protocol used in the SDP rtpmap attribute

- Default: RTP/AVP
- Values: " UDP | RTP/AVP

clock-rate
The clock rate in Hz for the SDP/RTP map. Use 8000 for narrowband codecs and 16000 for wideband codecs. If set to 0, the default clock rate for the codec will be used.

- Default: 0
- Values: Min: 0 | Max: 4294967295

req-bandwidth
Enter the total bandwidth in kilobits that the media requires

- Default: 0
- Values: Min: 0 | Max: 999999999

frames-per-packet
Enter the number of frames per RTP packet. This field is used to specify a media profile to facilitate Slow Start translations to Fast Start. A value of 0 means that this field is not being used.

- Default: 0
- Values: Min: 0 / Max: 256

parameters
Enter any additional information for codecs

average-rate-limit
Enter the maximum speed in bytes per second for a flow that this media profile applies to

- Default: 0
- Values: Min: 0 / Max: 125000000

peak-rate-limit
Enter the flowspec parameter r (bucket rate) / p (peak rate) value to insert into COPS message for RACF/PDP configuration

- Default: 0
- Values: Min: 0 / Max: 125000000
- Values: Min: 8192 / Max: 125000000 - Applicable only for SD5 platforms - 4600/6300/6350

max-burst-size
Enter the flowspec parameter b (bucket depth) / m (minimum policed unit) / M (maximum datagram size) value to insert into COPS message for RACF/PDP configuration

- Default: 0
- Values: Min: 0 / Max: 125000000

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 8192 / Max: 125000000 - Applicable only for SD5 platforms - 4600/6300/6350

sdp-rate-limit-headroom
Specify the percentage of headroom to be added while using the AS bandwidth parameter while calculating the average-rate-limit (rate limit for the RTP flow)

- Default: 0
- Values: Min: 0 / Max: 100

sdp-bandwidth
Enable or disable the use of the AS modifier in the SDP if the req-bandwidth and sdp-rate-limit-headroom parameters are not set to valid values in the corresponding media profile.

- Default: disabled
- Values: enabled | disabled

as-bandwidth
Specifies the value of the AS modifier in the SDP, in kbps, to support bandwidth requirement variation in transcoding scenarios.

- Default: 0
- Values: Min: 0 / Max: 4294967295

police-rate
Enter the rate at which the Oracle Communications Session Border Controller polices media for external bandwidth

- Default: 0
- Values: Min: 0 | Max: 999999999

subname
Enter a subname to create multiple media profiles with the same codec name; using a bandwidth value is convenient. For example, you might set a subname of 64k for a media-profile with a name value of PCMU.

standard-pkt-rate
When ptime isn't available in received SDP for this codec, the SBC uses this default packetization rate baseline to make bandwidth allocations when communicating with an external policy server.

- Default: 0
- Values: Min: 0 | Max: 125000000

Path

media-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **media-profile**.

> **Note**
>
> This element supports new SDP formats when they are defined. This element is used to associate bandwidth requirements with SDP requirements from information passed during the establishment of sessions. The names established in the media-profile elements are used to populate the corresponding fields in other elements. This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

media-security

The media-security element lets you access configuration elements concerning media security configuration.

Parameters

dtls-srtp-profile
Access the **dtls-srtp-profile** configuration element.

media-sec-policy
Access the **media-sec-policy** configuration element.

sdes-profile
Access the **sdes-profile** configuration element.

sipura-profile
Access the **sipura-profile** configuration element.

Path

The **media-security** element is under the **security** path.

```
ORACLE(sipura-profile)# quit
ORACLE# conf terminal
ORACLE(configure)# security
ORACLE(security)# media-security
ORACLE(media-security)#
```

media-security > dtls-srtp-profile

The dtls-srtp-profile element allows you to use DTLS-SRTP to secure media and the signaling used to establish DTLS-SRTP flows. You apply a configured dtls-srtp-profile profile to a realm.

Parameters

name
Enter a unique identifier for this DTLS SRTP profile. Use this name when you apply the profile to realms.

tls-profile
Enter the name of the tls-profile you want to apply to traffic under this dtls-srtp-profile.

dtls-completion-timeout
Specify the number of seconds the system waits for a DLTS handshake to finish before terminating the session.

- Range: 0 (default) to 9999

preferred-setup-role
Specify the role the system takes within the client-server context of the DTLS handshake.

- Default: passive—The system acts as the server.

Copyright © 2024, 2026, Oracle and/or its affiliates.

crypto-suite
Specifies the cryptography suite the system proposes during the DTLS handshake for encrypting media and authentication.

- Default: SRTP_AES128_CM_HMAC_SHA1_80
- Values:
  - SRTP_AES128_CM_HMAC_SHA1_80—Enables support for the AES/128 bit key for encryption and HMAC/SHA-1 80-bit digest for authentication.
  - SRTP_AES128_CM_HMAC_SHA1_32—Enables support for the AES/128 bit key for encryption and HMAC/SHA-1 32-bit digest for authentication.
  - SRTP_AEAD_256_GCM

Path

dtls-srtp-profile is an element under the security path. The full path from the topmost ACLI prompt is: configure terminal > security > media-security > dtls-srtp-profile.

> **Note**
>
> This is a multiple instance configuration element.

media-sec-policy

The media-sec-policy configuration element lets you access configuration elements concerning media security configuration. The media-sec-policy element does not apply to hairpin call flows.

Parameters

name
Name of this media-sec-policy object.

pass-through
Enable or disable pass-through mode. When enabled, the User Agent (UA) endpoints negotiate security parameters between each other; consequently, the Oracle Communications Session Border Controller simply passes SRTP traffic between the two endpoints.
With pass-thru mode disabled (the default state), the Oracle Communications Session Border Controller disallows end-to-end negotiation — rather the Oracle Communications Session Border Controller initiates and terminates SRTP tunnels with both endpoints.

- Default: disabled
- Values: enabled | disabled

options
Options configured on this media security policy

outbound
Enter this subelement to configure the policy parameters when this policy applies to outbound traffic.

Copyright © 2024, 2026, Oracle and/or its affiliates.

inbound
Enter this subelement to configure the policy parameters when this policy applies to inbound traffic.

Path

media-sec-policy is a configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **media-security**, and then **media-sec-policy**.

media-sec-policy > inbound

The media-sec-policy > inbound configuration element lets you configure the inbound media security policy.

Parameters

profile
Indicates the name of the corresponding security profile that's active on the call leg that this policy direction specifies.

mode
Selects the real time transport protocol.

- Default: rtp
- Values: rtp | srtp

protocol
This sets the key exchange protocol

- Default: none
- Values: none | sdes

hide-egress-media-update
Enables or disables the hide media update function for this inbound policy

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> You must reboot the system when you change this parameter. This parameter is not RTC supported.

Path

inbound is a subelement in the media-sec-policy configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **media-security**, and then **media-sec-policy**, and then **inbound**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

media-sec-policy > outbound

The media-sec-policy > inbound configuration element lets you configure the outbound media security policy.

Parameters

profile
Indicates the name of the corresponding security profile that's active on the call leg that this policy direction specifies.

mode
Selects the real time transport protocol.

- Default: rtp
- Values: rtp | srtp

protocol
This sets the key exchange protocol

- Default: none
- Values: none | sdes

Path

outbound is a subelement in the media-sec-policy configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **media-security**, and then **media-sec-policy**, and then **outbound**.

msrp-config

The msrp-config element is used to configure global MSRP functionality.

Parameters

state
Enables MSRP operations.

- Default: enabled
- enabled | disabled

uri-translation
Enables or disables NAT of URIs found in the From-Path and To- Path headers of MSRP requests and responses, and in a=path attributes found in SDP offers.

- Default: enabled
- enabled | disabled

session-inactivity-timer
This parameter is configured in connection with the sipconfig > msrp-delayed-bye-timer parameter to implement the delayed transmission of SIP BYE requests. The session-inactivity-timer parameter specifies the maximum inactivity interval (defined as the absence of transmitted data) tolerated before the MSRP connection is terminated.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 5
- Min: 0 / Range: 5 - 10

conn-setup-delay-timer
This parameter specifies the maximum time before the system sets up a session with the UA even though it has not received any input or response from that UA in milleseconds.

- Default: 0
- Min: 0 / Max: 1500

msrp-kpi
Enable or disable MSRP KPI statistics.

- Default: disabled
- Values: enabled | disabled

double-port-allocation
Enable allocating 2 steering pool ports for MSRP calls.

- Default: disabled
- Values: enabled | disabled

Path

msrp-config is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **media-manager**, and then **msrp-config**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

5

ACLI Configuration Elements N-Z

net-management-control

The net-management-control configuration element allows you to control multimedia traffic, specifically for static call gapping and 911 exception handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed-number prefixes.

Parameters

name
Enter the name of this network management control rule.

state
Select the state of this network management control rule.

- Default: enabled
- Values: enabled | disabled

type
Enter the control type you want to use.

- Values: GAP-RATE | GAP-PERCENT | PRIORITY

value
Enter the control value of the net management control. This parameter applies only when you set the control type to either GAP-RATE or GAP-PERCENT.

- Default: 0
- Values: GAP-RATE: 0-2147483647 | GAP-PERCENTAGE: 0-100

treatment
Enter the treatment method you want to use or leave this parameter empty

- Values: reject | divert | apply-local-policy

next-hop
Enter the next hop for the Oracle Communications Session Border Controller to use when the treatment method is DIVERT. This value should contain one of the following:

- hostname(:port) or IPv4 address or IPv6 address of a configured session agent.
- IPv4 address (:port) or IPv6 address (:port) of a specific endpoint

Group name of a configured session agent group. The group name of a configured session agent group must be prefixed with SAG: For example:

- policy-attribute: next-hop SAG:appserver
- policy-attribute: next-hop lrt:routetable

Copyright © 2024, 2026, Oracle and/or its affiliates.

- policy-attribute: next-hop enum:lerg

realm-next-hop
Enter the realm identifier to designate the realm of the next hop when the treatment type is DIVERT

protocol-next-hop
Enter the signaling protocol for the next hop when the treatment type is DIVERT

status-code
Enter the SIP response code that you want the Oracle Communications Session Border Controller to use when the treatment method is REJECT

- Default: 503
- Values: Min: 1 / Max: 699

cause-code
Enter the Q.850 cause code that you want the Oracle Communications Session Border Controller to use when the treatment method is REJECT

- Default: 63
- Values: Min: 1 / Max: 999999999

gap-rate-max-count
Enter the maximum token counter value for gapping rate

- Default: 0
- Values: Min: 0 / Max: 999999999

gap-rate-window-size
Enter the window size (in seconds) for gapping rate calculation

- Default: 0
- Values: Min: 0 / Max: 999999999

destination-identifier
Enter the classification key. This parameter specifies information about the destination, which can be an IP address, an FQDN, and destination (called) number, or destination prefix. You can wildcard characters in the classification key using the carat symbol (^).
This parameter can accommodate a list of entries so that, if necessary, you can specify multiple classification keys.

add-destination-identifier
Add a destination identifier

remove-destination-identifier
Remove a destination identifier

rph-feature
Set the state of NSEP support for this NMC rule

- Default: disabled
- Values: enabled | disabled

rph-profile
Enter the name of the RPH profile to apply to this NMC rule

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: None
- Values: Name of an rph-profile

rph-policy
Enter the name of the RPH policy to apply to this NMC rule

- Default: None
- Values: Name of an rph-policy

sip-380-reason
Adds configurable reason for IR.92 Multiple Emergency Numbers feature

- Default: None
- Values: Enter a reason phrase enclosed in quotes

:

Path

net-management-control is an element of the session-router path. The full path from the topmost ACLI prompt is:**configure terminal**, and then **session-router**, and then **net-management-control**

phy-interface > network-alarm-threshold

Use the **network-alarm-threshold** configuration element to set utilization thresholds for media interfaces.

Path

The **network-alarm-threshold** configuration element is in the **phy-interface** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# phy-interface
ORACLE(phy-interface)# network-alarm-threshold
ORACLE(network-alarm-threshold)#
```

Parameters

The **network-alarm-threshold** configuration element contains the following parameters:

severity
Enter the severity for the alarm you want to create for this interface.

- Default: minor
- Values: minor | major | critical

value
Enter the utilization percentage (transmitting and receiving) that triggers an alarm for this interface.

- Default: 0
- Min: 1 | Max: 100

For example, you might define a minor alarm with a utilization percentage of 50.

Copyright © 2024, 2026, Oracle and/or its affiliates.

network-interface

The network-interface element creates and configures a logical network interface.

> **Note**
>
> This configuration element is not RTC supported.

Parameters

name
Enter the name of the physical interface with which this network-interface element is linked. Network-interface elements that correspond to phy-interface elements with an operation type of Control or Maintenance must start with “wancom.”

sub-port-id
Enter the identification of a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is only required if the operation type is Media.

- Default: 0
- Values: Min: 0 | Max: 4095

description
Enter a brief description of this network interface.

hostname
Enter the hostname of this network interface. This is an optional entry that must follow FQDN Format or IP Address Format.
An IPV6 address is valid for this parameter.

ip-address
Enter the IP address of this network interface. This is a required entry that must follow the IP Address Format.
An IPV6 address is valid for this parameter.

pri-utility-addr
Enter the utility IP address for the primary HA peer in an HA architecture.
An IPV6 address is valid for this parameter.

sec-utility-addr
Enter the utility IP address for the secondary Oracle Communications Session Border Controller peer in an HA architecture.
An IPV6 address is valid for this parameter.

netmask
Enter the netmask portion of the IP address for this network interface entered in IP address format. The network-interface element will not function properly unless this field value is valid.
An IPV6 address is valid for this parameter.

gateway
Enter the gateway this network interface uses to forward packets. Entries in this field must follow the IP Address Format. No packets are forwarded if this value is 0.0.0.0.

Copyright © 2024, 2026, Oracle and/or its affiliates.

An IPV6 address is valid for this parameter.
Oracle recommends, as a best-practice, that you always configure a **gateway** for the media interfaces. If the only trigger to learn a gateway or a directly connected endpoint is ingress media packets, then the SBC typically drops initial packets of a first call until the gateway or the endpoint L2 MAC address is resolved.

sec-gateway
Enter the gateway to use on the secondary Oracle Communications Session Border Controller in an HA pair. Entries in this field must follow the IP address format.
An IPV6 address is valid for this parameter.

gw-heartbeat
Access the gateway-heartbeat subelement.

dns-ip-primary
Enter the IP address of the primary DNS to be used for this interface.
An IPV6 address is valid for this parameter.

dns-ip-backup1
Enter the IP address of the first backup DNS to be used for this interface.
An IPV6 address is valid for this parameter.

dns-ip-backup2
Enter the IP address of the second backup DNS to be used for this interface.
An IPV6 address is valid for this parameter.

dns-domain
Set the default domain name used to populate incomplete hostnames that do not include a domain. Entries must follow the Name Format.

dns-timeout
Enter the total time in seconds you want to elapse before a query (and its retransmissions) sent to a DNS server timeout.

- Default: 11
- Values: Min: 1/ Max: 999999999

dns-max-ttl
Specifies the maximum DNS time to live value for this network interface.

- Default: 86400 seconds (24 hours)
- minimum: 30
- maximum: 2073600

add-hip-ip
Enter a list of IP addresses allowed to access signaling and maintenance protocol stacks via this front interface using the HIP feature.
An IPV6 address is valid for this parameter.

remove-hip-ip
Remove an IP address added using the add-hip-ip parameter.

add-icmp-ip
Enter a list of IP addresses from which ICMP traffic can be received and acted upon by a front media interface.

An IPV6 address is valid for this parameter.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> IP address changes to the add-icmp-ip parameter during traffic hours may impact established calls.

remove-icmp-ip
Remove an IP address added using the add-icmp-ip parameter.
An IPV6 address is valid for this parameter.

> **Note**
>
> IP address changes to the remove-icmp-ip parameter during traffic hours may impact established calls.

add-snmp-ip
Enter an IP address from which SNMP traffic can be received and acted upon by a front media interface.

remove-snmp-ip
Remove an IP address added using the add-snmp-ip parameter.

add-ssh-ip
Enter the IP address from which SSH traffic can be received and acted upon by a front media interface.

- Default: None
- Values: A valid IPv4 network address

remove-ssh-ip
Remove an IP address added using the add-ssh-ip parameter.

signaling-mtu
MTU size for packets leaving this interface.

- Default: 0 - When the default value is zero, the network-interface inherits this value from the system configuration (ipv6-signaling-mtu and ipv4-signaling-mtu).
- Values:
  - IPv4: <0, 576-4096>
  - IPv6: <0, 1280-4096

Path

The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **network-interface**

> **Note**
>
> This is a multiple instance configuration subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

network-interface > gw-heartbeat

The gw-heartbeat subelement supports the front interface link failure detection and polling feature.

Parameters

state
Enable or disable front interface link detection and polling functionality on the Oracle Communications Session Border Controller for this network-interface element

- Default: disabled
- Values: enabled | disabled

heartbeat
Enter the time interval in seconds between heartbeats for the front interface gateway

- Default: 0
- Values: Min: 0 | Max: 65535

retry-count
Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable

- Default: 0
- Values: Min: 0 | Max: 65535

retry-timeout
Enter the heartbeat retry timeout value in seconds

- Default: 1
- Values: Min: 1 | Max: 65535

health-score
Enter the amount to subtract from the health score if the front interface gateway heartbeat fails (i.e., expires). The health score will be decremented by the amount set in this field if the timeout value set in the gw-heartbeat: retry-timeout field is exceeded without the front interface gateway sending a response.

- Default: 0
- Values: Min: 0 | Max: 100

Path

gw-heartbeat is a subelement of the network-interface element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **network-interface** , and then **gw-heartbeat**

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> The values configured in the fields of a gw-heartbeat subelement apply to the Oracle Communications Session Border Controller on a per-network-interface basis, and can override the values configured in the redundancy element's corresponding front interface link detection and polling fields.
> This is a single instance configuration subelement.

network-parameters

The network-parameters element enables and configures the TCP keepalive feature used for keeping H.323 connections open. This is also used for global SCTP configuration.

Parameters

tcp-keepalive-count
Enter the number of outstanding keepalives before connection is torn down

- Default: 4
- Values: Min: 1 | Max: 4294967295

tcp-keepalive-idle-timer
Enter the idle time in seconds before triggering keepalive processing. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated.

- Default: 400
- Values: Min: 30 | Max: 7200

tcp-keepalive-mode
Enter the TCP keepalive mode

- Default: 0
- Values:
  - 0—The sequence number is sent un-incremented
  - 1—The sequence number is sent incremented
  - 2—No packets are sent
  - 3—Send RST (normal TCP operation)

tcp-keepinit-timer
Enter the TCP connection timeout period if a TCP connection cannot be established. If you have upgraded the release you are running and a value outside of the acceptable range was configured in an earlier release, the default value is used and a log message is generated.

- Default: 75
- Values: 0 - 999999999

tcp-keepalive-interval-timer
Enter the TCP retransmission time if a TCP connection probe has been idle for some amount of time

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 75
- Values: Min: 15 / Max: 75

sctp-send-mode
Leave this parameter set to its default (unordered) so data delivery can occur without regard to stream sequence numbering. If data delivery must follow stream sequence number, change this parameter to ordered.

- Default: unordered
- Values: ordered | unordered

sctp-rto-initial
Sets the initial value of the SCTP retransmit timeout (RTO).

- Default: 3000 msec (value recommended by RFC 4960)
- Values: 0 - 4294967295

sctp-rto-max
Sets the maximum value of the SCTP retransmit timeout (RTO).

- Default: 60000 msec (value recommended by RFC 4960)
- Values: 0 - 4294967295

sctp-rto-min
Sets the maximum value of the SCTP retransmit timeout (RTO).

- Default: 1000 msec (value recommended by RFC 4960)
- Values: 0 - 4294967295

sctp-hb-interval
Sets the initial value of the SCTP Heartbeat Interval timer.

- Default: 30000 msec (value recommended by RFC 4960)
- Values: 0 - 4294967295

sctp-max-burst
Sets the maximum number of DATA chunks contained in a single SCTP packet.

- Default: 4 DATA chunks (value recommended by RFC 4960)
- Values: 0 - 4294967295

sctp-sack-timeout
Sets the initial value of the SACK (Selective Acknowledgement) Delay timer.

- Default: 200 msec (value recommended by RFC 4960)
- Values: 0 - 500

sctp-assoc-max-retrans
Specifies the maximum number of consecutive unacknowledged retransmissions to a specific SCTP endpoint. Should this value be exceeded, the endpoint is considered to be unreachable, and the SCTP association is placed in the CLOSED state.

- Default: 10 retries (value recommended by RFC 4960)
- Values: 0 - 4294967295

Copyright © 2024, 2026, Oracle and/or its affiliates.

sctp-path-max-retrans
Specifies the maximum number of RTO expirations/unacknowledged HEARTBEATS to a specific SCTP transport address. Should this value be exceeded, the endpoint is considered to be inactive, and an alternate transport address, if available, will be used for subsequent transmissions.

- Default: 5
- Values: 0 - 4294967295

options
Enter any optional features or parameters

Path

network-parameters is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **network-parameters**

> **Note**
>
> This is a single instance configuration subelement.

npli-profile

The npli-profile configuration element defines the system's behavior with respect to NPLI on the object to which it is applied.

Parameters

name
Configured name of this NPLI profile. This is the key field.

- Default: empty
- Values: 24 character string, no special characters with the exception of the underscore and hyphen characters. Do not start name with numeric character.

add-ue-location-in-pani
Enable this parameter to add UE Location string in the PANI header when the location is available.

- Default: disabled
- Values: enabled | disabled

hold-emergency-calls-for-loc-info
Timer to hold emergency calls until the system receives location information from the PCRF.

- Default: 0
- Values: 0-4294969295

hold-invite-calls-for-loc-info
The time the systems waits for the location information from the PCRF in a RAR over the Rx interface, assuming it is greater than 0, and reserve-incomplete is enabled.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: 0-4294969295

cache-loc-info-expire
Maximum number of seconds after which the system drops network location information for the NPLI for the Short Message feature, unless the **keep-cached-loc-info-after-timeout** parameter is enabled.

- Default: 32
- Values: 0 - 4294967295

msg-hold-for-loc-info
Maximum number of seconds that the system holds MESSAGEs for location information for the NPLI for the Short Message feature.

- Default: 0—disabled
- Values: 0 - 30

npli-upon-register
This adds the ability to capture Network Provided Location Information during the Registration process.

- Default: disabled
- Values: enabled | disabled

allow-pani-for-trusted-only
Allow PANI header only for trusted domains.

- Default: disabled
- Values enabled | disabled

default-location-string-VoWifi
Default location information string to be populated when no other NPLI is provided and the AAA includes a RAT type of WLAN.

- Default: empty
- Values: 24 character string, no special characters with the exception of the underscore and hyphen characters. Do not start name with numeric character.

Path

npli-profile is an element in the **session-config** path. The full path from the topmost ACLI prompt is: **session-config**, and then **npli-profile**.

nsep-stats-profile

The nsep-stats-profile defines the NSEP statistics the system collects for the realms on which you have enabled the nsep-stats parameter.

Parameters

state
Enables or disables this profile.

- Default: disabled
- enabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

rvalues
Lists the rvalues to be considered for per realm statistics.

- Default: empty
- Single or list of rvalues

feature-code
The country code STD to be used to with the dialed numbers on which you want to collect realm-based statistics. This is to be pre-pended to all configured dialed numbers. This value must be configured if any dialed number is configured. You can configure only one feature code. A list of values is not permitted.

- Default: empty
- The country code STD to prepend to your dialed number entry or entries.

dialed-numbers
Specifies the dialed numbers to be considered for per realm statistics. Use of this parameter also requires that the feature-code parameter be configured.

- Default: empty
- Single or list of dialed numbers on which you want to collect realm statistics

Path

nsep-stats-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **nsep-stats-profile**.

ntp-sync

The ntp-sync element defines the ntp server for time synchronization.

Parameters

add-server
Adds IP address or FQDN of the NTP server. IP entries must follow the IP Address Format. An IPv4 or IPv6 address is valid for this parameter.
This parameter accepts a single FQDN or one or more IP addresses. There cannot be more than one FQDN. The parameter does not allow an FQDN and any IP address(es).

del-server
Removes a previously entered NTP server. Entries must follow the IP Address Format or FQDN used to add the server. An IPv4 address, IPv6 address or FQDN is valid for this parameter.

dns-realm
When using an FQDN in the add-server parameter, this parameter becomes required and specifies the realm on which your target NTP server resides.

auth-servers
This parameter provides access to the auth-servers sub-element.

Path

ntp-sync is a top-level element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **ntp-sync**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ntp-sync > auth-servers

The auth-servers subelement is used to configure authenticated NTP

Parameters

ip-address
IP address of the NTP server that supports authentication. An IPv4 or IPv6 address is valid for this parameter.

key-id
Key ID of the key parameter.

- Values: 0 - 999999999
- Default: 0

key
Key used to secure the NTP requests. The key is a string 1 - 28 characters in length.

Path

auth-servers is a configuration element. The full path from the topmost ACLI prompt is: **configure terminal**, and then **ntp-sync**, and then **auth-servers**

password-policy

The **password-policy** element configures password rules. The Oracle Communications Session Border Controller (SBC) uses password secure mode by default. This setting cannot be changed by users and cannot be disabled through the CLI.

Parameters

min-secure-pwd-len
Enter the minimum password length to use when system is in secure password mode. The maximum allowable length for any password is 64 characters.

- Default: 8
- Values: 8-64

> **Note**
>
> The password using this minimum length value must contain at least one punctuation mark and two out of these three requirements: upper case letter, lower case letter, number. No special characters are allowed, for example: #, &, @.

> **Note**
>
> This parameter is ignored when the **password-policy-strength** parameter is used (the Admin Security and/or Admin Security ACP license is active).

Copyright © 2024, 2026, Oracle and/or its affiliates.

expiry-interval
Specifies the maximum password lifetime in days.

- Default: 90
- Min: 1 / Max: 65535

password-change-interval
Specifies the minimum password lifetime.

- Default: 24 hours
- Min: 1 hour / Max: 24 hours

expiry-notify-period
Specifies the number of days prior to expiration that users begin to receive password expiration notifications.

- Default: 30 days
- Min: 1 day / Max: 90 days

grace-period
Time after password expiration user has until forced to change password.

- Default: 30 days
- Min: 1 day / Max: 90 days

grace-logins
Number of logins after password expiration the user has until forced to change password.

- Default: 3
- Min: 1 / Max: 10

password-history-count
Specifies the number of previously used passwords retained in encrypted format in the password history cache.

- Default: 3
- Supported values are integers within the range 3 through 24 (retained passwords). Each system's actual support, however, is dependent on enabled license:
  - Admin Security alone—Password history count ranges between 3 and 10
  - JITC—Password history count ranges between 8 and 24

> **Note**
>
> If your configuration violates either of the licenses above, the system displays an error message that states the applicable range.

password-policy-strength
Enables the enhanced password strength requirements provided by the Admin Security and/or Admin Security ACP license.

- Default: disabled
- enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

password-policy is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **password-policy**.

paste-config

This command is unsupported.

Path

paste-config is a command within the top-level configure terminal path. The full path from the topmost ACLI prompt is **configure terminal** > **paste-config**.

phy-interface

The phy-interface element is used to configure physical interfaces.

> **Note**
>
> The phy-interface element is not RTC supported. Reboot the SBC to apply your settings.

Parameters

name
Enter the name for this physical interface. Physical interfaces with an operation-type of Control or Maintenance must begin with “wancom.” This is a required field. Entries in this field must follow the Name Format. Name values for the phy-interface must be unique.

operation-type
Select the type of physical interface connection

- Default: Control
- Values:
  - Media—Front-panel interfaces only. Port: 0-3 Slot: 0 or 1
  - Control—Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0
  - Maintenance —Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0

port
Select the physical port number on an interface of the phy-interface being configured

- Default: 0
- Values:
  - 0-2 for rear-panel interfaces
  - 0-1 for two possible GigE ports on front of Oracle Communications Session Border Controller chassis

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - 0-3 for four possible FastE ports on front of Oracle Communications Session Border Controller chassis

slot
Select the physical slot number on the Oracle Communications Session Border Controller chassis

- Default: 0
- Values:
  - 0 is the motherboard (rear-panel interface) if the name begins with “wancom”
  - 0 is the left Phy media slot on front of Oracle Communications Session Border Controller chassis
  - 1 is the right Phy media slot on front of Oracle Communications Session Border Controller chassis

virtual-mac
Enter the MAC address identifying a front-panel interface when the Oracle Communications Session Border Controller is in the Active state. This field value should be generated from the unused MAC addresses assigned to a Oracle Communications Session Border Controller. The virtual-mac field is only applicable for front interfaces.

admin-state
Enable or disable the Oracle Communications Session Border Controller to allow incoming and outgoing traffic to be processed using the front physical interface cards

- Default: enabled
- Values: enabled | disabled

auto-negotiation
Enable or disable auto negotiation on front Phy card interfaces taking place before either end begins sending packets over the Ethernet link. The auto-negotiation field is only applicable for front interfaces. The value configured in this field does not change the Oracle Communications Session Border Controller status at runtime.

- Default: enabled
- Values: enabled | disabled

> **Note**
>
> For fiber interfaces, auto-negotiation should be enabled (default) because fiber interfaces do not allow for manual configuration of the speed and duplex.

duplex-mode
Set whether the 10/100 Phy card interfaces located on the front panel of Oracle Communications Session Border Controller operate in full-duplex mode or half-duplex mode

- Default: full
- Values: full | half

speed
Set the speed in Mbps of the front-panel 10/100 Phy interfaces; this field is only used if the auto-negotiation field is set to disabled for 10/100 Phy cards

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 100
- Values: "" | 10 | 100 | 1000

wancom-health-score
Enter the amount to subtract from the Oracle Communications Session Border Controller's health score if a rear interface link goes down

- Default: 50
- Values: Min: 0 | Max: 100

This parameter has no effect on a phy-interface set to Media as its operation-type.

network-alarm-threshold
Access the network-alarm-threshold subelement.

overload-protection
Enable this parameter to turn graceful call control on. Disable (default) if you do not want to use this feature.

- Default: disabled
- Values: enabled | disabled

This parameter is not RTC supported
.

options
Enter any optional features or parameters.

Path

phy-interface is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **phy-interface**.

> **Note**
>
> Certain fields are visible based on the setting of the operation-type parameter. This is a multiple instance configuration subelement.

phy-interface > network-alarm-threshold

The network-alarm-threshold subelement enables the Oracle Communications Session Border Controller to monitor network utilization of its media interfaces and send alarms when configured thresholds are exceeded.

Parameters

severity
Enter the level of alarm to be configured per port.

- Default: minor
- Values: minor | major | critical

value
Set the threshold percentage of network utilization that triggers an SNMP trap and alarm for each severity value.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

network-alarm-threshold is a subelement under the **system** path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **phy-interface**.

policy-group > policy-agent

The policy-agent is used for configuring the members of the associated policy-group, which provides load balancing for Rx interface traffic within the RACF context on the Oracle Communications Session Border Controller.

Parameters

name
Specifies the name of this policy agent configuration.

state
Enables or disables the operational state of this policy agent configuration.

- Default: enabled
- Values: enabled | disabled

address
Specifies the IP address or FQDN of the policy agent.

port
Specifies the port on which the policy agent connects.

- Default: 3868
- Range: 0 - 65535

realm
Specifies the realm where the policy-agent exists.

watch-dog-ka-timer
Specifies the watchdog timer interval for this agent in seconds.

- Default: 0
- Values: Valid Range: 0-65535

transport-protocol
Specifies the transport protocol used to connect to this policy-agent.

- Default: TCP
- Values: TCP / SCTP

local-multi-home-addrs
Applies to SCTP. Enter an IP address that is local to the SBC and can be used by this external policy server as an alternate connection point. This address must be the same type as the address parameter, either IPv4 or IPv6.

remote-multi-home-addrs
Applies to SCTP. Enter an IP addresses that can be used by this SBC as an alternate connection point. This address must be the same type as the address parameter, either IPv4 or IPv6.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sctp-send-mode
Applies to SCTP. Specifies the SCTP delivery mode. The default value is **ordered**. Valid values are:

- ordered (Default)
- unordered

Path

policy-agent is a sub-element under the policy-group . The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **policy-group**, and then **policy-agent**.

policy-group

The policy-group is used for configuring load balancing for Rx interface traffic on the Oracle Communications Session Border Controller.

Parameters

group-name
Enter the name of this policy-group configuration.

description
Enter a description of this group name. Multi-word descriptions must be enclosed in quotes.

state
Enable or disable the operational state of this policy-group configuration.

- Default: enabled
- Values: enabled | disabled

policy-agent
Enter the policy-agent sub-element to configure one or more policy-agents for this group. There is no limit to the number of agents you can configure.

strategy
Enter the policy allocation strategy you want to use. The strategy you choose defines the order the SBC uses to try **policy-agent**s. The default and only value is **RoundRobin**.

max-recursions
Enter an integer to specify the number of times the SBC can recurse through the agent list.

stop-recurse
Enter the list of SIP response codes that terminate recursion within the group. Upon receiving one of the specified response codes, such as 401 unauthorized, or upon generating one of the specified response codes internally, such as 408 timeout, the SBC returns a final diameter response code to the **policy-agent**s in the group and stops trying to route the message.

Enter the response codes as a comma-separated list or as response code ranges.

recursion-timeout
Time in seconds that the SBC waits for max-recursions to finish before timing out. The default is 15 seconds.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

policy-group is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **policy-group**.

public-key

This element is unsupported.

Parameters

name
Enter the name of the public key

type
Select the type of key you want to create.

- Default: rsa
- Values: rsa | dsa

size
Enter the size of the key you are creating.

- Default: 1024
- Values: 512 | 1024 | 2048

Path

public-key is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal > security > public-key**

> **Note**
>
> This is a multiple instance configuration element.

q850-sip-map

The q850-sip-map configuration element is used to map q850 cause codes to SIP response codes.

Parameters

entries
Enter the entries configuration subelement

delete
Delete a q850 to SIP mapping. Enter the q850 code.

edit
Edit a response map by number

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

q850-sip-map is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **q850-sip-map**.

q850-sip-map > entries

The entries subelement is used to create the mapping of q850 cause to SIP reason code.

Parameters

q850-cause
Enter the q850 cause code to map to a SIP reason code

sip-status
Enter the SIP response code that maps to this q850 cause code

- Values: Min: 100 | Max: 699
- Default: 0

sip-reason
Describe the mapped SIP response code

Path

entries is a subelement under the **q850-sip-map** configuration element, which is located under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **q850-sip-map** , and then **entries**.

qos-constraints

The qos-constraints configuration element allows you to enable QoS based routing, which uses the R-Factor on a per-realm basis to cut back on the traffic allowed by a specific realm. Oracle Communications Session Border Controller QoS reporting is a measurement tool that collects statistics on Voice over IP (VoIP) call flows for SIP and H.323. To provide information, the Oracle Communications Session Border Controller writes additional parameters to the Remote Authentication Dial-in User Service (RADIUS) call record and Historical Data Recording (HDR) records.

Parameters

name
Enter the name of a QoS constraints configuration

state
Enable or disable a set of QoS constraints

- Default: enabled
- Values: enabled | disabled

major-factor
Enter a numeric value set the threshold that determines when the Oracle Communications Session Border Controller applies the call reduction rate; must be less than the critical-rfactor

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 0 | Max: 9321 0

critical-rfactor
Enter a numeric value to set the threshold that determines when the Oracle Communications Session Border Controller rejects all inbound calls for the realm, and rejects outbound calls when there is no alternate route

- Default: 0
- Values: Min: 0 | Max: 9321

call-load-reduction
Enter the percentage by which the Oracle Communications Session Border Controller will reduce calls to the realm if the major-rfactor is exceeded; a value of 0 means the call load will not be reduced

- Default: 0
- Values: Min: 0 | Max: 100

Path

qos-constraints is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **qos-constraints**.

radius-servers

Use the **radius-servers** configuration element to define and configure the RADIUS servers that the SBC communicates with.

Path

The **radius-servers** configuration element is in the **authentication** element.

```
ORACLE# configure terminal
ORACLE(configure)# security
ORACLE(security)# authentication
ORACLE(authentication)# radius-servers
ORACLE(radius-servers)#
```

Parameters

The **radius-servers** configuration element contains the following parameters:

address
Enter the IPv4 or IPv6 address of the RADIUS server.

port
Enter the port number on the remote IP address for the RADIUS server.

- Default: 1812
- Valid value: 1645
- Valid value: 1812

state
Enable or disable this configured RADIUS server

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- Values: enabled | disabled

secret
Enter the password the RADIUS server and the SBC share.
This password is not transmitted between the two when the request for authentication is initiated.

nas-id
Enter the NAS ID for the RADIUS server.

realm-id
Enter the RADIUS server realm ID.

retry-limit
Set the number of times the SBC retries to authenticate with this RADIUS server.

- Default: 3
- Min: 1 | Max: 5

retry-time
Enter the time in seconds the SBC waits before retrying to authenticate with this RADIUS server.

- Default: 5
- Min: 5 | Max: 10

maximum-sessions
Enter the maximum number of sessions to maintain with this RADIUS server.

- Default: 255
- Min: 1 | Max: 255

class
Select the class of this RADIUS server as either primary or secondary.

- Default: primary
- Values: primary | secondary

A connection to the primary server is tried before a connection to the secondary server is tried.

dead-time
Set the time in seconds before the SBC retries a RADIUS server that it has designated as dead.

- Default: 10
- Min: 10 | Max: 10000

authentication-methods
Select the authentication method the SBC uses when communicating with the RADIUS server.

- Default: all
- Values: all | chap | eap | mschapv2 | pap

Copyright © 2024, 2026, Oracle and/or its affiliates.

realm-config

The realm-config element is used to configure realms.

Parameters

identifier
Enter the name of the realm associated with this SBC. This is a required field. The identifier field value must be unique.

description
Provide a brief description of the realm-config configuration element

addr-prefix
Enter the IP address prefix used to determine if an IP address is associated with the realm. This field is entered as an IP address and number of bits in the network portion of the address in standard slash notation.

- Default: 0.0.0.0

An IPV6 address is valid for this parameter.

network-interface
Enter the network interface through which this realm can be reached. Entries in this parameter take the form: **<network-interface-ID>:<subport>.<ip_version>**.

> **Note**
>
> Only one network interface can be assigned to a single realm-config object.

media-realm-list
List media realm names the SBC searches to match a user-site and select a media realm for allocating Teams media IP. The first realm in the media-realm-list is the default realm for fall back functionality.

mm-in-realm
Enable or disable media being steered through the Oracle Communications Session Border Controller when the communicating endpoints are located in the same realm

- Default: disabled
- Values: enabled | disabled

mm-in-network
Enable or disable media being steered through the Oracle Communications Session Border Controller when the communicating endpoints are located in different realms within the same network (on the same network-interface). If this field is set to enabled, the Oracle Communications Session Border Controller will steer all media traveling between two endpoints located in different realms, but within the same network. If this field is set to disabled, then each endpoint will send its media directly to the other endpoint located in a different realm, but within the same network.

- Default: enabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

mm-same-ip
Enable the media to go through this Oracle Communications Session Border Controller if the mm-in-realm . When not enabled, the media will not go through the Oracle Communications Session Border Controller for endpoints that are behind the same IP.

- Default: enabled
- Values: enabled | disabled

mm-in-system
Set this parameter to enabled to manage/latch/steer media in the Oracle Communications Session Border Controller. Set this parameter to disabled to release media in the Oracle Communications Session Border Controller. Setting this parameter to disabled will cause the Oracle Communications Session Border Controller to NOT steer media through the system (no media flowing through this Oracle Communications Session Border Controller.

- Default: enabled
- Values: enabled | disabled

bw-cac-non-mm
Set this parameter to enabled to turn on bandwidth CAC for media release

- Default: disabled
- Values: enabled | disabled

msm-release
Enable or disable the inclusion of multi-system (multiple Oracle Communications Session Border Controllers) media release information in the SIP signaling request sent into the realm identified by this realm-config element. If this field is set to enabled, another Oracle Communications Session Border Controller is allowed to decode the encoded SIP signaling request message data sent from a SIP endpoint to another SIP endpoint in the same network to restore the original SDP and subsequently allow the media to flow directly between those two SIP endpoints in the same network serviced by multiple Oracle Communications Session Border Controllers. If this field is set to disabled, the media and signaling will pass through both Oracle Communications Session Border Controllers. If this field is set to enabled, the media is directed directly between the endpoints of a call.

- Default: disabled
- Values: enabled | disabled

qos-enable
Enable or disable the use of QoS in this realm

- Default: disabled
- Values: enabled | disabled

generate-udp-checksum
Enable or disable the realm to generate a UDP checksum for RTP/RTCP packets.

- Default: disabled
- Values: enabled | disabled

This parameter is visible only on Acme Packet 3800s and Acme Packet 4500s that do not have an ETC card installed. The function is enabled and not configurable on all other platforms.

Copyright © 2024, 2026, Oracle and/or its affiliates.

max-bandwidth
Enter the total bandwidth budget in kilobits per second for all flows to/from the realm defined in this element. A max-bandwidth field value of 0 indicates unlimited bandwidth.

- Default: 0
- Values: Min: 0 / Max: 999999999

fallback-bandwidth
Enter the amount of bandwidth available once the Oracle Communications Session Border Controller has determined that the target (of ICMP pings) is unreachable.

- Default: 0
- Values: Min: 0

max-priority-bandwidth
Enter the amount of bandwidth amount of bandwidth you want to want to use for priority (emergency) calls; the system first checks the max-bandwidth parameter, and allows the call if the value you set for priority calls is sufficient.

- Default: 0
- Values: Min: 0 | Max: 999999999

max-latency
This parameter is unsupported.

max-jitter
This parameter is unsupported.

max-packet-loss
This parameter is unsupported.

observ-window-size
This parameter is unsupported.

parent-realm
Enter the parent realm for this particular realm. This must reference an existing realm identifier.

dns-realm
Enter the realm whose network interface's DNS server should be used to resolve FQDNs for requests sent into the realm. If this field value is left empty, the Oracle Communications Session Border Controller will use the DNS of the realm's network interface.

media-policy
Select a media-policy on a per-realm basis (via an association between the name field value configured in this field). When the Oracle Communications Session Border Controller first sets up a SIP or H.323 media session, it identifies the egress realm of each flow and then determines the media-policy element to apply to the flow. This parameter must correspond to a valid name entry in a media policy element.

nsep-media-policy
Enter the name of the media-policy you want to apply to this realm for traffic identified and handled as NSEP traffic. Use this parameter to establish different DSCP marking between NSEP and other media on this realm. This parameter must correspond to a valid name entry in a media policy element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

media-sec-policy
Name of default media security policy.

rtcp-mux
Select to enable RTCP multiplexing, which allows Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) packets to use the same media port numbers.

- Default: disabled
- Values: enabled | disabled

ice-profile
Specify the name of an exitsing ICE profile, which enables a WebRTC client to perform connectivity checks and can provide several STUN servers to the browser.

dtls-srtp-profile
Enter the name of the dtls-srtp-profile you want to apply to DTLS traffic on this realm.

srtp-msm-passthrough
Enables multi system selective SRTP pass through in this realm.

- Default: disabled
- Values: enabled | disabled

class-profile
Enter the name of class-profile to use for this realm for ToS marking

in-session-translations
Enter the subelement that defines session translations to apply to incoming traffic on this realm.

out-session-translations
Enter the subelement that defines session translations to apply to outgoing traffic on this realm.

in-manipulationid
Enter the inbound SIP manipulation rule name

out-manipulationid
Enter the outbound SIP manipulation rule name

average-rate-limit
Enter the average data rate in bits per second for host path traffic from a trusted source

- Default: 0 (disabled)
- Values: Min: 0 | Max: 4294967295

access-control-trust-level
Select a trust level for the host within the realm

- Default: none
- Values:
  - high—Hosts always remains trusted
  - medium—Hosts belonging to this realm can get promoted to trusted, but can only get demoted to untrusted. Hosts will never be put in block-list.

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - low—Hosts can be promoted to trusted list or can get demoted to untrusted list
  - none—Hosts will always remain untrusted. Will never be promoted to trusted list or will never get demoted to untrusted list

max-inbound-per-session-burst-rate
Set the maximum inbound burst rate per session.

- Default: 30
- Values: Min: 1 | Max: 999999999

burst-rate-window-per-session
Set the burst rate window per session.

- Default: 1
- Values: Min: 1 | Max: 999999999

dos-action-at-session
Specify the system's behavior for reacting to session-based DoS attacks.

- Default: none
- permit—If the endpoint initiates the DDoS attack at the session level, the system can demote or deny the endpoint. At first detection of a DDoS attack, the system demotes the endpoint from trusted to untrusted. If there is a second DDoS attack before the UNTRUST_TMO timer expires, the system further demotes the endpoint to deny
- no-deny—If the endpoint initiates the DDoS attack at the session level, the system can demote the endpoint to untrusted. When the UNTRUST_TMO timer expires, the system promotes the endpoint back to the trusted state.
- session-drop—If the endpoint initiates the DDoS attack at the session level, the system takes action on that session only. Specifically, the system terminates the existing session but does not demote or deny the endpoint.

invalid-signal-threshold
Enter the acceptable invalid signaling message rate falling within a tolerance window

- Default: 0
- Values: Min: 0 | Max: 4294967295

maximum-signal-threshold
Enter the maximum number of signaling messages allowed within the tolerance window

- Default: 0 (disabled)
- Values: Min: 0 | Max: 4294967295

untrusted-signal-threshold
Enter the allowed maximum signaling messages within a tolerance window.

- Default: 0
- Values: Min: 0 | Max: 4294967295

nat-trust-threshold
Enter maximum number of denied endpoints that set the NAT device they are behind to denied. 0 means dynamic demotion of NAT devices is disabled.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 | Max: 65535

max-endpoints-per-nat
Maximum number of endpoints that can exist behind a NAT before demoting the NAT device.

- Default: 0 (disabled)
- Values: Min: 0 | Max: 65535

nat-invalid-message-threshold
Maximum number of invalid messages that may originate behind a NAT before demoting the NAT device.

- Default: 0 (disabled)
- Values: Min: 0 | Max: 65535

wait-time-for-invalid-register
Period (in seconds) that the counts before considering the absence of the REGISTER message as an invalid message.

- Default: 0 (disabled)
- Values: Min: 0, 4-300

deny-period
Enter the length of time an entry is posted in the deny list

- Default: 30
- Values: Min: 0 / Max: 4294967295

cac-failure-threshold
Enter the number of CAC failures for any single endpoint that will demote it from the trusted queue to the untrusted queue for this realm.

- Default: 0
- Values: Min: 0 / Max:141842

untrust-cac-failure-threshold
Enter the number of CAC failures for any single endpoint that will demote it from the untrusted queue to the denied queue for this realm.

- Default: 0
- Values: Min: 0 / Max: 4294967295

ext-pol-server
Name of external policy server.

diam-e2-address-realm
The value inserted into a Diameter e2 Address-Realm AVP when a message is received on this realm.

symmetric-latching
Enable, disable and manage symmetric latching between endpoints for RTP traffic.

- Default: disabled
- enabled
- disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- pre-emptive - symmetric latching is enabled, but the SBC sends RTP packets to the received SDP connection address without waiting on the latch.

pai-strip
Enable or disable P-Asserted-Identity headers being stripped from SIP messages as they exit the Oracle Communications Session Border Controller. The PAI header stripping function is dependent on this parameter and the trust-me parameter.

- Default: disabled
- Values: enabled | disabled

trunk-context
Enter the default trunk context for this realm

early-media-allow
Select the early media suppression for the realm

- Values:
  - none: No early media is allowed in either direction
  - both: Early media is allowed in both directions
  - reverse: Early media received by Oracle Communications Session Border Controller in the reverse direction is allowed

enforcement-profile
Enter the name of the enforcement profile (SIP allowed methods).

additional-prefixes
Enter one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.

add-additional-prefixes
Add one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.

remove-additional-prefixes
Remove one or more additional address prefixes. Not specifying the number of bits to use implies all 32 bits of the address are used to match.

restricted-latching
Set the restricted latching mode.

- Default: None
- Values:
  - none: No restricted latching
  - sdp: Use the IP address specified in the SDP for latching purpose
  - peer-ip: Use the peer-ip (Layer 3 address) for the latching purpose
  - sdp-ip-port: Latch to media based on the IP Address received in the SDP c= connect address line, and the port in the mline in the offer and answer.

restriction-mask
Set the restricted latching mask value.

- Default: 32

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 1 | Max: 128

user-cac-mode
Set this parameter to the per user CAC mode that you want to use

- Default: none
- Values:
  - none—No user CAC for users in this realm
  - AOR—User CAC per AOR
  - IP—User CAC per IP

user-cac-bandwidth
Enter the maximum bandwidth per user for dynamic flows to and from the user. By leaving this parameter set to 0 (default), there is unlimited bandwidth and the per user CAC feature is disabled for constraint of bandwidth.

user-cac-sessions
Enter the maximum number of sessions per user for dynamic flows to and from the user. Leaving this parameter set to 0 (default), there is unlimited sessions and the CAC feature is disabled for constraint on sessions

- Default: 0
- Values: Min: 0 / Max: 999999999

icmp-detect-multiplier
Enter the multiplier to use when determining how long to send ICMP pings before considering a target unreachable. This number multiplied by the time set for the icmp-advertisement-interval determines the length of time

- Default: 0
- Values: Min: 0

icmp-advertisement-interval
Enter the time in seconds between ICMP pings the Oracle Communications Session Border Controller sends to the target.

- Default: 0
- Values: Min: 0

icmp-target-ip
Enter the IP address to which the Oracle Communications Session Border Controller should send the ICMP pings so that it can detect when they fail and it needs to switch to the fallback bandwidth for the realm.

- Default: (empty)

monthly-minutes
Enter the monthly minutes allowed

- Default: 0
- Values: Min: 0 / Max: 71582788

options
Enter any optional features or parameters

Copyright © 2024, 2026, Oracle and/or its affiliates.

accounting-enable
Select whether you want accounting enabled within the realm

- Default: enabled
- Values: enabled | disabled

net-management-control
Enable or disable network management controls for this realm

- Default: disabled
- Values: enabled | disabled

delay-media-update
Enable or disable media update delay

- Default: disabled
- Values: enabled | disabled

refer-call-transfer
REFER call transfer

- Default: disabled
- Values: enabled | disabled | dynamic

refer-notify-provisional
Provisional mode for sending NOTIFY message

- Default: none
- Values:
  - none: no intermediate NOTIFY's are to be sent
  - initial: immediate 100 Trying NOTIFY has to be sent
  - all: immediate 100 Trying NOTIFY plus a NOTIFY for each non-100 provisional received by the SD are to be sent

dyn-refer-term
Enable or disable the Oracle Communications Session Border Controller to terminate a SIP REFER and issue a new INVITE. If the dyn-refer-term value is disabled (the default), proxy the REFER to the next hop to complete REFER processing. If the dyn-refer-termvalue is enabled, terminate the REFER and issue an new INVITE to the referred party to complete REFER processing.

- Default: disabled
- Values: enabled | disabled

codec-policy
Select the codec policy you want to use for this realm

codec-manip-in-realm
Enable or disable codec policy in this realm

- Default: disabled
- Values: enabled | disabled

codec-manip-in-network
Enable or disable codec policy in this network.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- enabled | disabled

constraint-name
Enter the name of the constraint you want to use for this realm

call-recording-server-id
This parameter is unsupported.

session-recording-server
A maximum of four names of session-recording-servers, or session-recording-groups, or a combination of both exisiting in thein the realm associated with the session reporting client. Valid values are alpha-numeric characters. session recording groups are indicated by prepending the groupname with SRG:

session-recording-required
Determines whether calls are accepted by the SBC if recording is not available.

- Default: disabled
- enabled—Restricts call sessions from being initiated when a recording server is not available.
- disabled—Allows call sessions to initiate even if the recording server is not available.

xnq-state
This parameter is unsupported.

hairpin-id
This parameter is unsupported.

manipulation-string
Enter a string to be used in header manipulation rules for this realm. 1

manipulation-pattern
Enter the regular expression to be used in header manipulation rules for this realm.

stun-enable
Enable or disable the STUN server support for this realm

- Default: disabled
- Values: enabled | disabled

stun-server-ip
Enter the IP address for the primary STUN server port

- Default: 0.0.0.0

stun-server-ip
Enter the IP address for the primary STUN server port

- Default: 0.0.0.0

stun-server-port
Enter the port to use with the stun-server-ip for primary STUN server port

- Default: 3478
- Values: Min. 1025 | Max. 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

stun-changed-ip
Enter the IP address for the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port; must be different from than the one defined for the stun-server-ip

- Default: 0.0.0.0

stun-changed-port
Enter the port combination to define the CHANGED-ADDRESS attribute in Binding Requests received on the primary STUN server port

- Default: 3479
- Values: Min. 1025 | Max. 65535

flow-time-limit
Enter the total time limit in seconds for the flow. The Oracle Communications Session Border Controller notifies the signaling application when this time limit is exceeded. This field is only applicable to dynamic flows. A value of 0 seconds disables this function and allows the flow to continue indefinitely.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

initial-guard-timer
Enter the time in seconds allowed to elapse before first packet of a flow arrives. If first packet does not arrive within this time limit, Oracle Communications Session Border Controller notifies the signaling application. This field is only applicable to dynamic flows. A value of 0 seconds indicates that no flow guard processing is required for the flow and disables this function.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

subsq-guard-timer
Enter the maximum time in seconds allowed to elapse between packets in a flow. The Oracle Communications Session Border Controller notifies the signaling application if this timer is exceeded. This field is only applicable to dynamic flows. A field value of zero seconds means that no flow guard processing is required for the flow and disables this function.

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

tcp-flow-time-limit
Enter the maximum time in seconds that a media-over-TCP flow can last

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

tcp-initial-guard-timer
Enter the maximum time in seconds allowed to elapse between the initial SYN packet and the next packet in a media-over-TCP flow

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

Copyright © 2024, 2026, Oracle and/or its affiliates.

tcp-subsq-guard-timer
Enter the maximum time in seconds allowed to elapse between all subsequent sequential media-over-TCP packets

- Default: -1, which allows the system to use the global timer settings for this realm.
- Values: Min: 0 / Max: 2147483647

sip-profile
Enter the name of the sip-profile to apply to this realm.

sip-isup-profile
Enter the name of the sip-isup-profile to apply to this realm.

match-media-profiles
Enter the media profiles you would like applied to this realm in the form `<name>::<subname>`. See the Oracle Communications Session Border Controller Configuration Guide for information about wildcard values.

qos-constraints
Enter the name value from the QoS constraints configuration you want to apply to this realm

block-rtcp
Block RTCP from entering or leaving this realm.

- Default: disabled
- Values: enabled | disabled

hide-egress-media-update
Hide changes to ingress RTP egressing into this realm

- Default: disabled
- Values: enabled | disabled

subscription-id-type
Sets the supported Subscription ID Types and the subsequent values inserted into the Subscription-Id-Data AVP's in an AAR message for Rx transactions.

- Default: END_USER_NONE
- Values: END_USER_NONE | END_USER_E164 | END_USER_SIP_URI | END_USER_IMSI

tcp-media-profile
A configured tcp-media-profile name to use within this realm. Used for MSRP.

stun-server-port
Enter the port to use with the stun-server-ip for primary STUN server port

- Default: 3478
- Values: Min. 1025 | Max. 65535

tcp-media-profile
A configured tcp-media-profile name to use within this realm. Used for MSRP.

monitoring-filters
Comma-separated list of monitoring filters used for SIP monitor and trace.

Copyright © 2024, 2026, Oracle and/or its affiliates.

node-functionality
Sets the value inserted into the node-functionality AVP in Rf messages going into this realm.

- P-CSCF
- BGCF
- IBCF
- E-CSCF
- "" - This indicates that this realm should revert to the global node-functionality value.

default-location-string
Used for NPLI functionality.

alt-realm-family
The realm name of the alternate realm, from which to use an IP address in the other address family. If this parameter is within an IPv4 realm configuration, you will enter an IPv6 realm name.

pref-addr-type
Order in which the `a=altc:` lines suggest preference.

- Default: none
- Values: none | ipv4 | ipv6

dns-max-response-size
Enter the maximum size of the DNS response to queries.

- Default: 0; disabled
- Value: 65535

session-max-life-limit
Enter the maximum interval in seconds before the system must terminate long duration calls. This value supercedes the value of **session-max-life-limit** in the **sip-interface** and **sip-config** configuration elements and is itself superceded by the value of **session-max-life-limit** in the **session-agent** configuration element.

- Default: 0; disabled
- Values:
  - 0
  - unlimited
  - 1 - 2073600

> **Note**
>
> See the Configuration Guide for the difference between 0 and unlimited.

sm-icsi-match-for-invite
The ICSI URN to match on to increment the session-based messaging counters.

- Default: urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.msg

sm-icsi-match-for-message
The ICSI URN to match on to increment the event-based messaging counters.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.largemsg

ringback-file
Specifies the name of the media file, stored previously in /code/media, that the system plays when triggered for this realm.

ringback-trigger
Specifies when the system triggers the local media playback function.

- none—The system does not perform local media playback procedures. Based on precedence, however, the system may issue playback based on other element configurations. Local media playback follows the precedence session-agent, realm, then sip-interface.
- disabled—The system does not perform media playback procedures on this flow, regardless of ensuing configurations.
- 180-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message that does not include SDP.
- 180-force—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message.
- 183—Starts playback to caller when 183 is sent to call originator. The system stops the playback on the final response (either 2xx success or 4xx error). Configure this 183 value on the original INVITE ingress realm/sip-interface/session-agent.
- refer—Starts playback to the referee when it receives a REFER. This trigger operates only if the OCSBC actually terminates and performs the refer operation. If the REFER is via proxy, playback is not a triggered. Playback stops when the refer operation is complete with a final response (200-299 or 400-699). Configure this refer value on the ingress realm/sip-interface/session-agent of the transferred call.
- 183-and-refer—Starts playback when both 183 and refer triggers are activated.
- playback-on-header—Starts or stops playback based on the presence of the P-Acme-Playback header and its definitions.

teams-fqdn-in-uri
Enables IP to FQDN replacement in FROM and Contact headers for SIP requests for Teams deployments. Also enables the SBC to send the proprietary X-MS-SBC header in SIP messages on egress realm.

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> This parameter uses the hostname configured under **network-interface**.

sdp-inactive-only
Enables the SBC to change the sendonly and recvonly attribute in SDP to inactive in outgoing SDP for Teams deployments. Also enables the SBC to perform the reverse action in incoming SDP.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

teams-fqdn
Reserved for use with Microsoft Teams integrations only.

merge-early-dialogs
Allows or prevents the merging of early dialogs within forking scenarios.

- Default: disabled
- Values: enabled | disabled

user-site
Sets the user-site names corresponding to the user-site configuration set at the DR. The SBC uses this name to select the realm for allocating media IP. The match for user-site is case insensitive.

srvcc-trfo
Supports SRVCC handover events that need to occur without transcoding by forcing a re-negotiation during the handover if a non-transcodable codec is currently being used.

- Default: empty
- Values: EVS

sti-as
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send AS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mySti GroupName`.

sti-vs
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send VS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mySti GroupName`.

sti-orig-id
Specifies the UUID v4 to be added to STI-AS requests, if not already present, during STIR/SHAKEN functions.

sti-attest
Specifies the attestation value that is sent in AS request, during STIR/SHAKEN functions. The default is empty

- full-attestation
- partial-attestation
- gateway-attestation

sti-signaling-attest
Enable this parameter to instruct the SBC to use attestation level and origination ID headers from the ingress SIP INVITE in the REST query to the STI-AS, if preferred. When enabled, the Attestation-Info and Origination-ID headers override the configured values, if present. If one of the two requested headers is present, the other value is obtained from configured parameters.

- Default: Disable—The system does not use the attestation value and origId from SIP headers.
- Enable—The system uses the attestation value and origId from SIP headers, when present.

Copyright © 2024, 2026, Oracle and/or its affiliates.

feature-trfo
Configure this parameter with the feature or features with which you want to use transcoding free operation (TrFO). Configure multiple parameters by separating them with a comma.

- Default: disable
- rbt
- asymmetric-preconditions

Although you can configure the feature-trfo parameter with multiple parameters, the system only acts on one of those parameters at any give time. Under the condition where more than one parameter applies, the system refers to your configuration's parameter order to determine which function to perform.

auth-attribute
Sub-element providing access to cross-realm surrogate agent management parameters.

fqdn-hostname
Enter the hostname you want to in include in the selected headers for this realm's egress traffic.

fqdn-hostname-in-header
List the headers for which the system includes the hostname that you configured in the fqdn-host-name parameter. Separate multiple values with a comma.

- FROM
- TO
- CONTACT
- R-URI

P-Asserted-Identity
Enter the string you want to use to set the identity within PAI headers for this realm's egress traffic.

P-Asserted-Identity-For
List the methods for which the system includes a PAI header using the PAI identity you set in this realm's p-asserted-identity parameter. Separate multiple values with a comma.

- INVITE
- BYE
- ACK
- REGISTER

nsep-stats
Enables the collection and reporting of NSEP statistics for this realm.

- Default: disabled
- Values: enabled | disabled

steering-pool-threshold
Specifies, in percent utilization, the value above which the system triggers an alarm indicating the realm is running low on steering pool ports.

- Default: 0 (Disables alarm)

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Range: 0 - 100%

steering-pool-lower-threshold
Specifies, in percent utilization, the value below which the system considers steering pool utilization on this realm acceptable. Operates in conjunction with the steering-pool-alarm-monitoring-time to prevent the system from issuing multiple alarms for what you consider the same issue.

- Default: 70
- Range: 1 - 95%

steering-pool-alarm-monitoring-time
Operates in conjunction with the steering-pool-lower-threshold, and specifies in minutes the duration for which the system considers an alarm condition triggered by the steering-pool-threshold as still in effect. After the system triggers this alarm, it uses this window as the amount of time steering pool port usage must be below the steering-pool-lower-threshold before the system can issue a new steering-pool-threshold alarm. This logic prevents the system from issuing multiple alarms for what you consider the same issue.

- Default: 15
- Range: 5 - 600 minutes

suppress-hold-resume-reinvite
Enables the system to suppress INVITEs on one leg of a call from being sent out the other leg. This suppression supports the SIP signaling while reducing traffic on the realm that does not need to act on the INVITE. These flows include call hold, call resume, re-INVITEs with codec changes and re-INVITEs with replaces headers.
When **suppress-hold-resume-reinvite** is enabled, the SBC will not generate an INVITE for Call Hold/Resume scenarios if SIPREC is also enabled.

- Default: disabled
- enabled

snmp-sipmethod-stats
Enables the system to collect SIP method statistics for this realm. When disabled, the system collects SIP method statistics on a system-wide basis.

- Default: disabled
- Values: enabled | disabled

default-teams-realm
Sets the default realm to use for initiating calls to MS Teams clients configured for local media optimization (LMO). When set to **external**, the Oracle Communications Session Border Controller initiates the session expecting that the Teams user is outside their corporate network. When set to an internal realm name, the Oracle Communications Session Border Controller initiates the session expecting that the Teams user is inside their corporate network. See the Oracle SBC with Local Media Optimization for Microsoft Teams Direct Routing technical application note for information about using LMO for Microsoft Teams.

- Default: external
- Values:
  - external

Copyright © 2024, 2026, Oracle and/or its affiliates.

- `<internal_realm_name>`

Path

realm-config is an element under the **media-manager** path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **realm-config.**

> **Note**
>
> This is a multiple instance configuration subelement.

realm-config > in-session-translations

Use the **in-session-translations** element to configure the session translations that apply to incoming traffic on this realm.

Parameters

in-session-translation-id
Enter the id of the session transation to apply to this realm.

state
Declare whether this session translation is enabled or disabled.

- Default: enabled
- Values: enabled | disabled

move
Change the order of execution.
The syntax of the command:

```
move <from-position> <to-position>
```

For example, to move the second session translation into the first position:

```
move 2 1
```

Path

The **in-session-translations** element is under the **media-manager** path.

```
ORACLE# conf term
ORACLE(configure)# media-manager
ORACLE(media-manager)# realm-config
ORACLE(realm-config)# in-session-translations
ORACLE(in-session-translation-list)#
```

> **Note**
>
> This is a multiple instance configuration subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

realm-config > out-session-translations

Use the **out-session-translations** element to configure the session translations that apply to outgoing traffic on this realm.

Parameters

out-session-translation-id
Enter the id of the session transation to apply to this realm.

state
Declare whether this session translation is enabled or disabled.

- Default: enabled
- Values: enabled | disabled

move
Change the order of execution.
The syntax of the command:

```
move <from-position> <to-position>
```

For example, to move the second session translation into the first position:

```
move 2 1
```

Path

The **out-session-translations** element is under the **media-manager** path.

```
ORACLE# conf term
ORACLE(configure)# media-manager
ORACLE(media-manager)# realm-config
ORACLE(realm-config)# out-session-translations
ORACLE(out-session-translation-list)#
```

> **Note**
>
> This is a multiple instance configuration subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

realm-config > auth-attributes

The auth-attributes element is used to configure authentication parameters available for surrogate registration on this realm.

Parameters

auth-realm
Enter the name (realm ID) of the host realm initiating the authentication challenge. This value defines the protected space in which the digest authentication is performed. Valid value is an alpha-numeric character string.

- Default: blank

username
Enter the username of the client. Valid value is an alpha-numeric character string.

- Default: blank

auth-user-lookup
Lookup used for selecting the AuthUser

- Default: blank

password
Enter the password associated with the username of the client. This is required for all LOGIN attempts. Password displays while typing but is saved in clear-text (i.e., *****). Valid value is an alpha-numeric character string.

- Default: blank
- Values: round-robin | hunt

in-dialog-methods
Optionally enter the in-dialog request method(s) that digest authentication uses from the cached credentials. Specify request methods in a list form separated by a space enclosed in parentheses. Valid values are.

- Default: blank
- Values: INVITE | BYE | ACK | OPTIONS | SUBSCRIBE | PRACK | NOTIFY | UPDATE | REFER

Path

auth-attributes is an element under the **media-manager** path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **realm-config**, and then **auth-attributes**

> **Note**
>
> This is a multiple instance configuration subelement.

Copyright © 2024, 2026, Oracle and/or its affiliates.

realm-group

The realm-group configuration element allows you to configure realm groups. Realm groups are sets of source and destination realms that allow early media to flow in the direction you configure.

Parameters

name
Enter the name of this realm group

source-realm
Enter the list of one or more global/SIP realms that you want to designate as source realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. To enter more than one realm in this list, list all items separated by a comma and enclose the entire entry in quotation marks.

destination-realm
Enter the list of one or more global/SIP realms that you want to designate as destination realms for the purpose of blocking early media; this is the realm identifier value for the realms you want on the list. To enter more than one realm in the list, list all items separated by a comma and enclose the entire entry in quotation marks

early-media-allow-direction
Set the direction for which early media is allowed for this realm group.

- Default: both
- Values:
- none—Turns off the feature for this realm group by blocking early media
- reverse - Allows early media to flow from called to caller.
- both - Allows early media to flow to/from called and caller

state
Enable or disable this realm group

- Default: disabled
- Values: enabled | disabled

Path

realm-group is an element of the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal > media-manager > realm-group.**

redundancy

The redundancy element establishes HA parameters for a Oracle Communications Session Border Controller that participates in an HA architecture.

Parameters

state
Enable or disable HA for the Oracle Communications Session Border Controller

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default enabled
- Values enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

log-level
Select the starting log level for the HA process. This value supersedes the value configured in the process-log-level field in the system-config element for the HA process

- Default: info
- Values:
  - emergency
  - critical
  - major
  - minor
  - warning
  - notice
  - info
  - trace
  - debug
  - detail

health-threshold
Enter the health score at which standby Oracle Communications Session Border Controller switches over to the Active state and takes control of all system functionality as the active Oracle Communications Session Border Controller

- Default: 75
- Values: Min: 0 | Max: 100

emergency-threshold
Enter the low health score value that triggers the initializing standby Oracle Communications Session Border Controller to become the active Oracle Communications Session Border Controller immediately. In addition, the active but unhealthy Oracle Communications Session Border Controller, regardless of its health, will not relinquish its Active state if the HA Oracle Communications Session Border Controller peer poised to become active upon switchover also has a health score below this emergency-threshold value.

- Default: 50
- Values: Min: 0 | Max: 100

port
Enter the port number on which the border element redundancy protocol is listening

- Default: 9090

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 1025 | Max: 65535

> **Note**
>
> This parameter is not RTC supported.

advertisement-time
Enter the time in milliseconds the Oracle Communications Session Border Controller continually sends its health score to its HA Oracle Communications Session Border Controller peer(s)

- Default: 500
- Values: Min: 50 | Max: 999999999

percent-drift
Set the percentage of an HA Oracle Communications Session Border Controller peer's advertisement time for this HA Oracle Communications Session Border Controller to wait before considering its peer to be out of service

- Default: 210
- Values: Min: 100 | Max: 65535

initial-time
Enter the number of milliseconds to set the longest amount of time the Oracle Communications Session Border Controller will wait at boot time to change its state from initial to either becoming active or becoming standby. This field is independent of the advertisement-time and percent-drift parameters; it is a timer used to decide the state transition.

- Default: 1250
- Values: Min: 5 / Max: 999999999

becoming-standby-time
Enter the time in milliseconds to wait before transitioning to the Standby state. This field allows the HA Oracle Communications Session Border Controller enough time to synchronize with its HA Oracle Communications Session Border Controller peer. If the HA Oracle Communications Session Border Controller has not become fully synchronized within the time frame established in this field, it will be declared out of service. We recommend setting this parameter to no less than 180000 if configuration checkpointing is used.

- Default: 180000
- Values: Min: 5 / Max: 2147483647

becoming-active-time
Enter the time in milliseconds a previously standby Oracle Communications Session Border Controller takes to become active. This field applies to the following scenarios:

- When the health of an active Oracle Communications Session Border Controller has failed
- When the standby Oracle Communications Session Border Controller is healthier than the active Oracle Communications Session Border Controller

  This is a transitional state.

  – Default: 100

Copyright © 2024, 2026, Oracle and/or its affiliates.

– Values: Min: 5 / Max: 999999999

cfg-port
Enter the port number from which HA checkpoint messages are sent and received. This field supports Configuration Checkpointing. Setting the cfg-port field value to 0 disables configuration checkpointing.

- Default: 1987
- Values: Min: 1025 / Max: 65535; 0

> **Note**
>
> This parameter is not RTC supported.

cfg-max-trans
Enter the size of the HA checkpoint transaction list to store in memory at a time

- Default: 10000
- Values: Min: 0 / Max: 4294967295

> **Note**
>
> This parameter is not RTC supported.

cfg-sync-start-time
Enter the time in milliseconds before HA Oracle Communications Session Border Controller begins sending HA configuration checkpointing requests. This timer begins immediately upon entering the Active state. As long as the active peer is healthy and active, it remains in a constant cycle of (re)setting this parameter's timer and checking to see if it has become standby.

- Default: 5000
- Values: Min: 0 / Max: 4294967295

> **Note**
>
> This parameter is not RTC supported.

cfg-sync-comp-time
Enter the time in milliseconds the standby Oracle Communications Session Border Controller waits before checkpointing with the active Oracle Communications Session Border Controller to obtain the latest configuration transaction information once the initial checkpointing process is complete.

- Default: 1000
- Values: Min: 0 / Max: 4294967295

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not RTC supported.

gateway-heartbeat-interval
Enter the time in seconds between heartbeats on the front interface gateway. This parameter is applicable until a front interface gateway failure occurs. This parameter applies globally to Oracle Communications Session Border Controllers operating in an HA node, but can be overridden on a network interface-by-network interface basis by the value configured in the gw-heartbeat: heartbeat field of the gw-heartbeat subelement in the network-interface element.

- Default: 0
- Values: Min: 0 / Max: 65535

> **Note**
>
> This parameter is not RTC supported.

gateway-heartbeat-retry
Enter the number of front interface gateway heartbeat retries after a front interface gateway failure occurs. The value configured in this field applies globally to Oracle Communications Session Border Controllers operating in HA pair architectures, but can be overridden on a per network interface basis by the value configured in the gw-heartbeat: retry-count field.

- Default: 0
- Values: Min: 0 / Max: 65535

> **Note**
>
> This parameter is not RTC supported.

gateway-heartbeat-timeout
Enter the heartbeat retry timeout value in seconds between subsequent ARP requests to establish front interface gateway communication after a front interface gateway failure occurs. The value configured in this field applies globally to Oracle Communications Session Border Controllers operating in HA pair architectures, but can be overridden on a network interface basis by the value configured in the gw-heartbeat: retry-timeout field.

- Default: 1
- Values: Min: 1 / Max: 65535

> **Note**
>
> This parameter is not RTC supported.

gateway-heartbeat-health
Enter the health score amount to subtract if the timeout value set in the gateway-heartbeat-timeout field has been exceeded without receiving a response from the front interface gateway. The value configured in this field applies globally to Oracle Communications Session

Copyright © 2024, 2026, Oracle and/or its affiliates.

Border Controllers operating in HA nodes, but can be overridden on a network interface basis by the value configured in the gw-heartbeat > health-score field of the gw-heartbeat. A field value of 0 means that the health score is not affected.

- Default: 0
- Values: Min: 0 / Max: 100

> **Note**
>
> This parameter is not RTC supported.

media-if-peercheck-time
Enter the amount of time in milliseconds for the standby system in an HA node to receive responses to its ARP requests via the front interface before it takes over the active role from its counterpart. A value of 0 turns the HA front interface keepalive off

- Default: 0
- Values: Min: 0 / Max: 500

peers
Access the peers subelement

Path

redundancy is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal system redundancy.**

> **Note**
>
> This is a single instance configuration element.

redundancy > peers

The peers subelement establishes the name and state of an HA node.

Parameters

state
Enable or disable HA

- Default: enabled
- Values: enabled | disabled

type
Select the HA peer type and which utility address to use

- Default: unknown
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- primary—HA peer set as the primary Oracle Communications Session Border Controller. It is associated with the utility address configured in the pri-utility-addr field of each network-interface element.
- secondary—HA peer set as the secondary Oracle Communications Session Border Controller. It is associated with the utility address configured in the sec-utility-addr field of each network-interface element.
- unknown—Not assigned HA peer type with associated utility address unknown. This type field option is not valid for configuration checkpointing. Although unknown is the default value, Primary or Secondary field option must be set in order for configuration checkpointing to function properly.

destinations
Access the destinations subelement

Path

peers is a subelement under the redundancy element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **redundancy** , and then **peers.**

> **Note**
>
> This is a multiple instance configuration subelement.

redundancy > peers > destinations

The destinations subelement establishes locations where health and state information is sent and received.

Parameters

address
Enter the IP address and port on the interface of the HA Oracle Communications Session Border Controller peer where this HA Oracle Communications Session Border Controller peer sends HA messages. The parameter format is an IP address and port combination (IP address:port). This IP address must match the interface identified in its HA Oracle Communications Session Border Controller peer's corresponding rdncy-peer-dest > network-interface field. The port portion of this parameter must match the port identified in its HA Oracle Communications Session Border Controller peer's corresponding port field.

network-interface
Enter the name and subport ID of the interface where the HA Oracle Communications Session Border Controller receives HA messages (e.g., wancom1:0). Valid interface names are wancom1 and wancom2 only.

Path

destinationsis a subelement under the peers subelement. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **redundancy** , and then **peers** , and then **destinations**

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> The destinations prompt is displayed as: rdncy-peer-dest.
> This is a multiple instance configuration element.

remove-isup-param

The remove-isup-param command instructs the Oracle Communications Session Border Controller remove a single ISUP parameter added to the sip-isup-profile configuration element, using the extract-isup-param parameter.

Syntax

```
remove-isup-param <argument>
```

Arguments

- generic-number—Remove the generic-number value from the list of extracted ISUP parameter for this profile.
- location-number—Remove the location-number value from the list of extracted ISUP parameter for this profile.
- user-to-user—Remove the user-to-user value from the list of extracted ISUP parameter for this profile.
- calling-party-number—Remove the calling-party-number value from the list of extracted ISUP parameter for this profile.
- inband-announcement—Remove the inband-announcement value from the list of extracted ISUP parameter for this profile.

Mode

Superuser

Example

```
ORACLE# remove-isup-param generic-number
```

resource-monitor-profile

Parameters

The **resource-monitor-profile** configuration element contains the following parameters:

resource-type
The resource to be monitored.

- Values: HEAP

state
Enable or disable monitoring.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

minor-threshold
The threshold value to send a minor-severity report.

- Default: 70
- Min: 50 | Max: 90

minor-precaution-action
The precautionary action to take when a minor severity report is raised for this resource.

- Default: RESOURCE_MONITOR_ALARM
- Values: RESOURCE_MONITOR_ALARM | DECREMENT_HEALTH_SCORE

major-threshold
The threshold value to send a major-severity report.

- Default: 80
- Min: 60 | Max: 90

major-precaution-action
The precautionary action to take when a major severity report is raised for this resource.

- Default: RESOURCE_MONITOR_ALARM
- Values: RESOURCE_MONITOR_ALARM | DECREMENT_HEALTH_SCORE

critical-threshold
The threshold value to send a critical-severity report.

- Default: 90
- Min: 70 | Max: 95

critical-precaution-action
The precautionary action to taken when a critical severity report is raised for this resource.

- Default: DECREMENT_HEALTH_SCORE
- Values: RESOURCE_MONITOR_ALARM | DECREMENT_HEALTH_SCORE

abatement-threshold
The abatement threshold value to revert the performed actions.

- Default: 5
- Min: 5 | Max: 50

healthscore-decrement-value
The health score decrement value.

- Default: 100
- Min: 10 | Max: 100

Path

The **resource-monitor-profile** configuration element is in the **system** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
ORACLE(system)# resource-monitor-profile
ORACLE(resource-monitor-profile)#
```

response-code-and-phrase-config

The **response-code-and-phrase-config** element provides initial access to the parameters you use to configure the response code and phrase feature.

Parameters

name
Specifies the name you use to apply the desired response-code-and-phrase-entry configuration to the response-code-and-phrase-name parameter within the sip-config.

response-code-and-phrase-entry
Provides access to the response-code-and-phrase-entry you configure for this named entry.

Path

response-code-and-phrase-config is an element of the sip-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **response-code-and-phrase-config**.

response-code-and-phrase-entry

The **response-code-and-phrase-entry** sub-element provides access to the parameters you use to configure additional response codes and phrases that you want to track. The system tracks these code/response pairs using ACLI counters (show sipd invite detail), SNMP and HDR. You can configure multiple **response-code-and-phrase-entry** sub-elements for each named **response-code-and-phrase-config**, allowing you to record multiple code/phrase pairs.

Parameters

response-code
Specifies the code number that you want to monitor. Valid values are integers from 100 to 999, limited to three numeric characters and with a default of 100.

response-phrase
Specifies the text returned as a reason for INVITE rejection that is associated with the code number configured above, and that you want to monitor. Valid values are alphabetic characters, with a maximum number of characters limited to 64.
You must enclose phrases with multiple words within double quotes. For example, to configure the phrase Stale Date, enter the text "Stale Date".

Path

response-code-and-phrase-entry is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **response-code-and-phrase-config**, and then **response-code-and-phrase-entry**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

rph-policy

The rph-policy element defines an override resource value and an insert resource value for ETS/WPS namespaces. These are applied to NMC rules.

Parameters

name
Enter the name of this RPH policy; this is the value used when applying this RPH policy to an NMC rule.

- Default: None

override-r-value
Set the value the Oracle Communications Session Border Controller uses to override the r-values in the original RPH.

- Default: None

insert-r-value
Set the value the Oracle Communications Session Border Controller inserts into the RPH.

Path

rph-policy is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **rph-policy**.

rph-profile

The rph-profile contains information about how the Oracle Communications Session Border Controller should act on the namespace(s) present in Resource-Priority headers.

Parameters

name
Enter the name of this RPH profile; this is the value used when applying this RPH profile to an NMC rule.

- Default: none

r-value
Enter a list of one or more r-values used for matching. Valid namespaces include WPS, ETS and ESNET. Valid values for the parameters that take r-values are wps.x, ets.x and esnet.x where x is 0 through 4. When applicable, WPS values must be entered before ETS values.

- Default: none

media-policy
Enter the name of this RPH profile; this is the value used when applying this RPH profile to an NMC rule.

- Default: none

call-treatment
Select the call treatment method for a non-ETS call that contains RPH matching this profile.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: accept
- Values: accept | reject | priority

Path

rph-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **rph-profile**.

rtcp-policy

The rtcp-policy is used to specify an individual rule controlling how the Oracle Communications Session Border Controller generates RTCP reports for the realm to which the rtcp-policy is assigned.

Parameters

name
Enter the name of this RTCP policy configuration. Use this name to assign the **rtcp-policy** to one or more realms.

rtcp-generate
Select the function this RTCP policy performs.

- Default: disabled
- Values:
  - none—Disables this policy.
  - all-calls—Oracle Communications Session Border Controller generates RTCP report information for all calls that pass through the realm.
  - xcoded-calls-only— Oracle Communications Session Border Controller generates RTCP report information only for the transcoded calls that pass through the realm.

Path

rtcp-policy is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **rtcp-policy**.

s8hr-profile

The authentication configuration element is used for configuring an authentication profile.

Parameters

name
Specifies the name for this S8HR-profile instance.

register-hold-for-plmn-info
Specifies the number of seconds desired to hold REGISTERs while waiting for PLMN information. The valid value is 0-30.

- Disable: 0
- Default: 16
- Values: 0 - 30

Copyright © 2024, 2026, Oracle and/or its affiliates.

plmn-id-prefix
Specifies the prefix string used for P-Visited-Network-ID headers for sessions using this profile.

emergency-reject-on-ident-error
When enabled, causes the system to reject an emergency session if user identity validation fails.

- Default: disabled
- Values: enabled/disabled

emergency-403-reason
Specifies the reason attached to a 403 when the system rejects an emergency session.

local-mnc
Specifies the local MNC where the SBC resides. This value should be a 2 or 3-digit integer.

local-mcc
Specifies the local MCC where the SBC resides. This value should be a 3-digit integer.

encrypt-disabled-mnc-mcc
Specifies the list of networks for which the system must disable encryption for roaming UEs handled by this profile. Enter an asterisk to disable encryption for all roaming networks.

```
ORACLE(s8hr-profile)# encrypt-disabled-mnc-mcc 033444 456789
```

Path

s8hr-profile is an element under the session-router path. The full path from the topmost prompt is: **configure terminal** , and then **session-router** , and then **s8hr-profile.**

sdes-profile

The sdes-profile configuration element lets you configure the parameter values offered or accepted during SDES negotiation.

Parameters

name
Sets the name of this object.

crypto-list
Sets the the encryption and authentication algorithms accepted or offered by this sdes-profile The crypto-list attribute supports the following ciphers on the Acme Packet 6300, Acme Packet 6350, and Acme Packet 4600:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32 (not available if FIPS is enabled)
- ARIA_CM_192_HMAC_SHA1_80 (not available if FIPS is enabled)
- ARIA_CM_192_HMAC_SHA1_32 (not available if FIPS is enabled)

The crypto-list attribute supports the following ciphers on the Acme Packet 3900, Acme Packet 4900, Acme Packet 1100, and virtual platforms:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32 (not available if FIPS is enabled)
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_256_GCM

srtp-auth
UNUSED

- Default: enabled
- Values: enabled | disabled

srtp-encrypt
This parameter enables or disables the encryption of RTP packets. With encryption enabled, the default condition, the SBC offers RTP encryption, and rejects an answer that contains an UNENCRYPTED_SRTP session parameter in the crypto attribute.
With encryption disabled, the SBC does not offer RTP encryption and includes an UNENCRYPTED_SRTP session parameter in the SDP crypto attribute; it accepts an answer that contains an UNENCRYPTED_SRTP session parameter.

- Default: enabled
- Values: enabled | disabled

srtcp-encrypt
This parameter enables or disables the encryption of RTCP packets. With encryption enabled, the default condition, the SBC offers RTCP encryption, and rejects an answer that contains an UNENCRYPTED_SRTCP session parameter in the crypto attribute.
With encryption disabled, the SBC does not offer RTCP encryption and includes an UNENCRYPTED_SRTCP session parameter in the SDP crypto attribute; it accepts an answer that contains an UNENCRYPTED_SRTCP session parameter.

- Default: enabled
- Values: enabled | disabled

mki
This parameter enables or disables the inclusion of the MKI:length field in the SDP crypto attribute.

- Default: disabled
- Values:
  - enabled – an MKI field is sent within the crypto attribute (16 bytes maximum)
  - disabled – no MKI field is sent

egress-offer-format
Sets any manipulation on SDP offer.

- Default: same-as-ingress
- Values:
  - same-as-ingress - the SBC leaves the profile of the media lines unchanged.

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - simultaneous-best-effort - the SBC Adds an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile, and Adds an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile
  - rfc5939-compliant - the SBC attempts to initiate and RFC 5939 compliant SDP exchange, but falls back to RFC 3562 if the presented signaling does not establish end-to-end support.

srtp-rekey-on-reinvite
This parameter enables or disables the re-keying upon the receipt of a SIP reINIVTE that contains SDP for the STRP Re-keying feature.

- Default: enabled
- Values: enabled | disabled

use-ingress-session-params
Enter the list of values for which the SBC will accept and (where applicable) mirror the UA's proposed cryptographic session parameters. If you want to enter multiple values, you can put them in the same command line entry separated by commas. For example srtcp-encrypt,srtp-auth,srtp-encrypt. You can also enter the values within double quotes. For example "srtcp-encrypt,srtp-auth,srtp-encrypt" or within parenthesis (srtcp-encrypt,srtp-auth,srtp-encrypt). You cannot use spaces as separators.

- srtp-auth—Decides whether or not authentication is performed in SRTP
- srtp-encrypt—Decides whether or not encryption is performed in SRTP
- srtcp-encrypt—Decides whether or not encryption is performed in SRTCP

```
ORACLE(sdes-profile)# use-ingress-session-params (srtcp-encrypt,srtp-
auth,srtp-encrypt)
```

Path

sdes-profile is a configuration element under the security > media-security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **media-security**, and then **sdes-profile**.

security-config

The security-config configuration element allows you to configure global TLS parameters.

Parameters

ocsr-monitoring-traps
Enable ocsr monitoring traps

- Default: enabled
- Values: enabled | disabled

srtp-msm-password
The shared secret used to derive the key for encrypting SDES keying material that is placed in the media attribute of an SDP media description.

srtp-msm-attr-name
Specifies the name of the media attribute used to convey SDES keying information within a SDP media description.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: X-acme-srtp-msm

image-integrity-value
Sets the known SHA-256 HMAC value that is computed for the boot image.

local-cert-exp-trap-int
The interval, in minutes, at which the local certificate expiration trap interval is sent when certificates are expired or are in the pre-expiration warning period.

- Default: 0 (disabled)
- Range: 0 to 4294967295

local-cert-exp-warn-period
The local certificate expiration warning period in days. If you do not set this value, the system issues the associated trap if it determines that any certificate is expiring within 30 days. If you do set this value, your setting takes precedence over this 30 day period.

- Default: 30
- Range: 0 (disabled) then 30 to 4294967295

Path: **security-config** is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **security-config**.

security > global-trusted-ca

The trusted-root-ca sub-element creates local trusted CA stores and defines the lists of certificates that you can apply to one or more tls-profiles objects.

Parameters

name
Specifies the name for this global-trusted-ca object. You apply this name to one or more tls-profiles for use by those objects.

state
Enables or disables this global-trusted-ca object. When enabled, the global-trusted-ca uses the CAs configured in this list to validate certificates. Values include:

- Enabled (default)
- Disabled

trusted-ca-certificates-list
Specifies the names of root CA's which this list trusts. There must be a corresponding certificate-record with the same name for each CA in this list. You can configure any number of root CA's per list, all of which are used by the applicable tls-profile(s).
Enter multiple entries by listing entries within parenthesis, (), and separating them with a space. You can also add or remove a single entry to an existing list by prefixing the applicable name with a plus sign (+) to add, and a minus sign (-) to remove.

Path

global-trusted-ca is a subelement under the **security** configuration element under the security path. The full path from the topmost prompt is: **configure terminal** , and then **security** , and then **global-trusted-ca**

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-agent

The session-agent element defines a signaling endpoint that can be configured to apply traffic shaping attributes and information regarding next hops or previous hops.

Parameters

hostname
Enter the hostname of this session agent. This is a required entry that must follow the Hostname (or FQDN) Format or the IP Address Format. Hostname values must be unique.

An IPV6 address is valid for this parameter.

> **Note**
>
> The hostname parameter does not accept values ending in *.

ip-address
Enter the IP address of session agent if hostname value is an FQDN

An IPV6 address is valid for this parameter.

port
Enter the port number for this session agent.

- Default: 5060
- Values: Min: 0; 1025 | Max: 65535

state
Enable or disable the session agent

- Default: enabled
- Values: enabled | disabled

app-protocol
Select the signaling protocol used to signal with the session agent

- Default: SIP
- Values: H323 | SIP

app-type
Set the H.323 session agent type as a gateway or a gatekeeper. This field is mandatory if the app-protocol parameter is set to H323. If the app-protocol parameter is set to SIP, then this field must be left blank.

- Values: H323-GW | H323-GK

transport-method
Select the IP protocol used for communicating with this session agent

- Default: UDP
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- UDP—UDP used as the transport method
- UDP+TCP—If the system determines that routes over TCP and UDP are both available, it initially uses UDP as the transport method. If a failure or timeout occurs in response to the UDP INVITE, the system uses TCP. When you select this transport method, the system always sends INVITEs via UDP as long as it receives a response.

  If the available route(s) only use one transport, either UDP or TCP, the system uses that transport method.
- DynamicTCP—Dynamic TCP connections are the transport method for this session agent. A new connection must be established for each session originating outbound from the SBC to the session agent. This connection is torn down at the end of a session.
- StaticTCP— Static TCP connections are the transport method for this session agent. Once a connection is established, it will remain and not be torn down.
- StaticSCTP—SCTP is used as the transport method.
- DynamicTLS—Dynamic TLS connections are the transport method for this session agent. A new connection must be established for each session originating outbound from the SBC to the session agent. This connection is torn down at the end of a session.
- StaticTLS— Static TLS connections are the transport method for this session agent. Once a connection is established, it will remain and not be torn down.
- ANY—support all transport methods

realm-id
Enter the realm for sessions coming from or going to this session agent. Entries in this field must follow the Name Format. This field must correspond to a valid identifier field entry in a realm-config.

egress-realm-id
Enter the name of the realm you want defined as the default egress realm used for ping messages. The Oracle Communications Session Border Controller will also use this realm when it cannot determine the egress realm for normal routing.

description
Describe the session-agent element. Entries in this field must follow the Text Format.

carriers
Enter the carrier names associated with this session agent. If this list is empty, any carrier is allowed. If it is not empty, only local policies that reference one or more of the carriers in this list will be applied to requests coming from this session agent. This list can contain as many entries within it as necessary. Entries in this field must follow the Carrier Format.

allow-next-hop-lp
Unsupported

match-identifier
Match-identifier is a sub-element of session-agent. Configure the match-identifier parameters to identify the session-agent.

associated-agents
Enter the list of session-agents configured on the Oracle Communications Session Border Controller

Copyright © 2024, 2026, Oracle and/or its affiliates.

constraints
Enable or disable the constraints established in this element in the fields that follow (maximum numbers of sessions allowed, maximum session rates, and timeout values) that are applied to the sessions sent to the session agent

- Default: disabled
- Values: enabled | disabled

max-sessions
Enter the maximum number of sessions allowed by the session agent; 0 means there is no constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-sessions
Enter the maximum number of inbound sessions allowed from this session agent

- Default: 0
- Values: Min: 0 / Max: 999999999

max-outbound-sessions
Enter the maximum number of simultaneous outbound sessions that are allowed to the session agent; 0 means there is no constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-burst-rate
Enter the number of session invitations per second allowed to be sent to or received from the session agent. A session is rejected if the calculated per-second rate exceeds this value.

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-burst-rate
Enter the maximum inbound burst rate in INVITEs per second from this session agent

- Default: 0
- Values: Min: 0 / Max: 999999999

max-outbound-burst-rate
Enter the maximum outbound burst rate in INVITEs per second

- Default: 0
- Values: Min: 0 / Max: 999999999

max-sustain-rate
Enter the maximum rate of session invitations per second allowed to or from the session agent within the current window. The period of time over which the rate is calculated is always between one and two window sizes. A session is rejected only if the calculated per-second rate exceeds the max-sustain-rate value. The value set for the max-sustain-rate field must be larger than the value set for the max-burst-rate field.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 | Max: 999999999

max-inbound-sustain-rate
Enter the maximum inbound sustain rate in INVITEs per second

- Default: 0
- Values: Min: 0 / Max: 999999999

max-outbound-sustain-rate
Enter the maximum outbound sustain rate in INVITEs per second

- Default: 0
- Values: Min: 0 / Max: 999999999

min-seizures
Enter the minimum number of seizures that, when exceeded, cause the session agent to be marked as having exceeded its constraints. Calls will not be routed to the session agent until the time-to-resume has elapsed.

- Default: 5
- Values: Min: 1 | Max: 999999999

min-asr
Enter the minimum percentage, that if the session agent's ASR for the current window falls below this percentage, the session agent is marked as having exceeded its constraints and calls will not be routed to it until the time-to-resume has elapsed

- Default: 0%
- Values: Min: 0% /|Max: 100%

cac-trap-threshold
The CAC (session or burst-rate) utilization threshold expressed as a percent that when exceeded generates a trap

- Default: 0
- Values: Min: 0 / Max: 99

time-to-resume
Enter the number of seconds after which the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it exceeded some constraint).

- Default: 0
- Values: Min: 0 | Max: 999999999

ttr-no-response
Enter the time delay in seconds to wait before the SA (Session Agent) is put back in service (after the SA is taken out-of-service because it did not respond to the Oracle Communications Session Border Controller).

- Default: 0
- Values: Min: 0 | Max: 999999999

in-service-period
Enter the time in seconds the session-agent must be operational (once communication is re-established) before the session agent is declared to be in-service. This value gives the session agent adequate time to initialize.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 0 | Max: 999999999

burst-rate-window
Enter the burst window period in seconds used to measure the burst rate. The term “window” refers to the period of time over which the burst rate is computed.

- Default: 0
- Values: Min: 0 | Max: 999999999

sustain-rate-window
Enter the sustained window period in seconds used to measure the sustained rate. The term “window” refers to the period of time over which the sustained rate is computed.

- Default: 0
- Values: Min: 10 | Max: 999999999

  The value you set here must be higher than or equal to the value you set for the burst rate window.

> **Note**
>
> If you are going to use this parameter, you must set it to a minimum value of 10.

max-inbound-per-session-burst-rate
Set the maximum inbound burst rate per session.

- Default: 30
- Values: Min: 1 | Max: 999999999

burst-rate-window-per-session
Set the burst rate window per session.

- Default: 1
- Values: Min: 1 | Max: 999999999

dos-action-at-session
Specify the system's behavior for reacting to session-based DoS attacks.

- Default: none
- permit—If the endpoint initiates the DDoS attack at the session level, the system can demote or deny the endpoint. At first detection of a DDoS attack, the system demotes the endpoint from trusted to untrusted. If there is a second DDoS attack before the UNTRUST_TMO timer expires, the system further demotes the endpoint to deny
- no-deny—If the endpoint initiates the DDoS attack at the session level, the system can demote the endpoint to untrusted. When the UNTRUST_TMO timer expires, the system promotes the endpoint back to the trusted state.
- session-drop—If the endpoint initiates the DDoS attack at the session level, the system takes action on that session only. Specifically, the system terminates the existing session but does not demote or deny the endpoint.

req-uri-carrier-mode
Select how a carrier determined by the local policy element should be added to the outgoing message

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: None
- Values:
  - None—Carrier information will not be added to the outgoing message
  - uri-param—Adds a parameter to the Request-URI (e.g., cic-XXX)
  - prefix—Adds the carrier code as a prefix to the telephone number in the Request-URI (in the same manner as is done in the PSTN)

proxy-mode
Select how SIP proxy forwards requests coming from the session agent. If this parameter is empty, its value is set to the value of the proxy-mode parameter in the sip-interface element by default. If the proxy-mode field in the element is also empty, the default is proxy.

- Values
  - proxy—If the Oracle Communications Session Border Controller is an SR, the system will proxy the request coming from the session agent and maintain the session and dialog state. If the Oracle Communications Session Border Controller is a Oracle Communications Session Border Controller, system will behave as a B2BUA when forwarding the request.
  - redirect—System will send a SIP 3xx reDIRECT response with contacts (found in the local-policy) to the previous hop
  - record-route—The Oracle Communications Session Border Controller forwards requests with a record-route

redirect-action
Select the action the SIP proxy takes when it receives a Redirect (3xx) response from the session agent. If the response comes from a session agent and this field is empty, the system uses the redirect action value defined in the sip-interface.

- Values:
  - proxy—SIP proxy passes the response back to the previous hop. The response will be sent based on the proxy-mode of the original request.
  - recurse—SIP proxy sends the original request to the list of contacts in the Contact header of the response, serially (in the order in which the contacts are listed in the response)
  - Recurse-305-only—recurse on the contacts in the 305 response

loose-routing
Enable or disable loose routing

- Default: enabled
- Values: enabled | disabled

send-media-session
Enable or disable the inclusion of a media session description in the INVITE sent by the Oracle Communications Session Border Controller. The only instance in which this field should be set to disabled is for a session agent that always redirects requests, meaning that it returns an error or 3xx response instead of forwarding an INVITE message. Setting this field to disabled prevents the Oracle Communications Session Border Controller from establishing flows for that INVITE message until it recurses the 3xx response.

- Default: enabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

response-map
Enter the name of the sip-response-map element set in the session router element to use for translating inbound final response values

ping-method
Enter the SIP message/method to use to “ping” a session agent

Setting this field value to the OPTIONS method might produce a lengthy response from certain session agents and could potentially cause performance degradation on your Oracle Communications Session Border Controller.
When entering the OPTIONS method as a parameter to **ping-method**, you can extend the command with the **hops** parameter to limit the number of hops each OPTIONS ping packet can traverse. The codeblock below presents the syntax you can use to set the maximum number of hops to 8.

```
ORACLE(session-agent)# ping-method OPTIONS;hops=8
```

ping-interval
Set how often to ping a session agent in seconds

- Default: 0
- Values: Min: 0 | Max: 999999999

ping-send-mode
Set the mode with which you want to send ping messages to session agents

- Default: keep-alive
- Values: keep-alive | continuous

ping-all-addresses
Enable pinging each IP address dynamically resolved via DNS. If disabled (default), the SBC only pings the first available resolved IP address.

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> When a host name resolves to multiple IP addresses, the SBC maintains state only for the DNS address as a whole. As long as one IP address is active, the state of the session agent is active; if all IP addresses are out of service, the session agent is out of service.

options
Establish customer-specific features and/or parameters. This value can be a comma separated list of “feature=<value>" or "feature" parameters.

spl-options
Establish customer-specific features and/or parameters. This value can be a comma separated list of “feature=<value>" or "feature" parameters.

Copyright © 2024, 2026, Oracle and/or its affiliates.

media-profiles
Start up an outgoing call as a Fast Start call with the information in the media profile used for the logical channels when the incoming call is slow start for an H.323 operation. This list is used to determine if a source and/or destination of a call is a session agent on that list. If a media profiles list is configured in the matching session-agent element, then the frame and codec information in the corresponding media profile will be used for the outgoing call. If the media-profiles list in the session-agent element is empty, the h323-stack > media-profiles list will be consulted. This field should reference the codec that you expect the gatekeeper/ gateway to use. This media-profiles entry must correspond to at least one valid name field entry in a media profile element that has already been configured.

in-session-translations
Enter the **in-session-translations** subelement to apply session translations to incoming traffic.

out-session-translations
Enter the **out-session-translations** subelement to apply session translations to outgoing traffic.

trust-me
Enable or disable the trust of this session agent; used for privacy features

- Default: disabled
- Values: enabled | disabled

request-uri-headers
Enter a list of embedded headers extracted from the Contact header that will be inserted in the re INVITE message

stop-recurse
Enter a list of returned response codes that this session agent will watch for in order to stop recursion on the target's or contact's messages

local-response-map
Enter the name of local response map to use for this session agent. This value should be the name of a sip-response-map configuration element.

ping-to-user-part
The user portions of the Request-URI and To: headers that define the destination of a session agent ping message.

ping-from-user-part
The user portion of the From: header that defines the source of a session agent ping message.

ping-response
Enable the SBC to consider OPTIONS received as pings and respond locally for Teams deployments.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> In offline mode, the SBC responds to SIP OPTIONS pings as configured in the **reg-reject-response-upon-offline** parameter on the **sip-config** element, regardless of the whether **ping-response** is enabled or disabled.

li-trust-me
Set this parameter to enabled to designate this session agent as trusted for P-DCS-LAES use

- Default: disabled
- Values: enabled | disabled

in-manipulationid
Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Oracle Communications Session Border Controller via this session agent

out-manipulationid
Enter the name of the SIP header manipulations configuration to apply to the traffic exiting the Oracle Communications Session Border Controller via this session agent

p-asserted-id
Set the configurable P-Asserted-Identity header for this session agent. This value should be a valid SIP URI.

trunk-group
Enter trunk group names and trunk group contexts to match in either IPTEL or custom format; one session agent can accommodate 500 trunk groups. If left blank, the Oracle Communications Session Border Controller uses the trunk group in the realm for this session agent. Multiple entries are surrounded in parentheses and separated from each other with spaces. You can add and delete single entries from the list using plus (+) and minus (-) signs without having to overwrite the whole list.

Entries for this list must one of the following formats: tgrp:context or tgrp.context.

max-register-sustain-rate
Specify the registrations per second for this session agent. The constraints parameter must be enabled for this parameter to function.

- Default: 0 (disabled)
- Values: Min: 0 | Max: 999999999

early-media-allow
Select the early media suppression for the session agent

- Values:
  - none—No early media allowed
  - reverse—Allow early media in the direction of calling endpoint
  - both—Allow early media in both directions

invalidate-registrations
Enable or disable the invalidation of all the registrations going to this SA when its state transitions to “out of service”

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values enabled | disabled

rfc2833-mode
Select whether 2833/UII negotiation will be transparent to the Oracle Communications Session Border Controller (pre-4.1 behavior), or use 2833 for DTMF

- Default: none
- Values:
  - none—The 2833-UII interworking will be decided based on the h323-stack configuration.
  - transparent—The session-agent will behave exactly the same way as before and the 2833 or UII negotiation will be transparent to the Oracle Communications Session Border Controller. This overrides any configuration in the h323-stack even if the stack is configured for “preferred” mode.
  - preferred—The session-agent prefers to use 2833 for DTMF transfer and would signal that in its TCS. However, the final decision depends on the remote H323EP.

rfc2833-payload
Enter the payload type used by the SA in preferred rfc2833-mode

- Default: 0
- Values: Valid Range: 0, 96-127

> **Note**
>
> When this value is zero, the global “rfc2833-payload” configured in the H323 configuration element will be used instead. For SIP SA, the payload defined in the SIP Interface will be used, if the SIP-I is configured with rfc2833-mode as “preferred”.

codec-policy
Enter the codec policy you want to apply to this session agent

enforcement-profile
Enter the enforcement policy set of allowed SIP methods you want to use for this session agent

- Default: None
- Values: Name of a valid enforcement-profile element

emergency-dscp-profile
Specifies the name of the emergency DSCP profile you want to apply to this session-agent.

refer-call-transfer
Enable or disable the refer call transfer feature for this session agent

- Default: disabled
- Values: enabled | disabled

refer-notify-provisional
Sends NOTIFY message after provisional messages are received in a REFER scenario.

- Default: none

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values:
  - none—The system does not send any NOTIFY messages after receiving provisional messages.
  - initial—The system sends a NOTIFY, including 100 Trying, immediately after accepting the REFER.
  - all— The system sends an immediate 100 Trying NOTIFY and a NOTIFY for each non-100 provisional received.

reuse-connections
Enter the SIP TCP connection reuse mode. The presence of “reuse-connections” in the options field of the sip-interface will cause the Oracle Communications Session Border Controller to reuse all inbound TCP connections for sending rquests to the connected UA.

- Default: tcp
- Values: tcp | sctp | tls | none

tcp-keepalive
Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost.

- Default: none
- Values: none | enabled | disabled

tcp-reconn-interval
Set the amount of time in seconds before retrying a TCP connection.

- Default: 0
- Values: 0, 2-300

max-register-burst-rate
Enter the maximum number of new registrations you want this session agent to accept within the registration burst rate window. When this threshold is exceeded, the Oracle Communications Session Border Controller responds to new registration requests with 503 Service Unavailable messages.

- Default: 0
- Values: Min: 0 / Max: 999999999

register-burst-window
Enter the window size in seconds for the maximum number of allowable SIP registrations.

- Default: 0
- Values: Min: 0 / Max: 999999999

rate-constraints
Access the rate-constraints subelement

ping-in-service-response-codes
Enter the response codes that keep a session agent in service when they appear in its response to the Oracle Communications Session Border Controller’s ping

- Default: None
- Values: SIP Response codes

Copyright © 2024, 2026, Oracle and/or its affiliates.

out-service-response-codes
Enter the response codes that take a session agent out of service when they appear in its response to the Oracle Communications Session Border Controller's ping request or any dialog-creating request.

- Default: None
- Values: SIP Response codes

manipulation-string
Enter a string you want used in the header manipulation rules for this session-agent. Enter a value to references the $HMR_STRING variable used to populate SIP headers and elements using HMR

manipulation-pattern
Enter the regular expression to be used in header manipulation rules for this session-agent.

sip-profile
Enter the name of the sip-profile you want to add to the session-agent

sip-isup-profile
Enter the name of the sip-isup-profile you want to add to the session-agent.

load-balance-dns-query
Sets the method the Oracle Communications Session Border Controller uses to send messages to when it queries a DNS server and receives multiple A-Records. The strategy configured here is used to select which of the multiple addresses the Oracle Communications Session Border Controller forwards the message to first.

- Default: hunt
- Values: hunt | round-robin

kpml-interworking
Enable or disable KPML interworking.

- Default: inherit
- Values: inherit | enabled | disabled

kpml2833-iwf-on-hairpin
When enabled, specifies that the system supports KPML to RFC2833 interworking for hairpinned calls. This requires that kpml-interworking to also be enabled.

- Default: inherit
- Values: inherit | enabled | disabled —When enabled, allows the Oracle Communications Session Border Controller to present the correct digit encapsulation (KPML or RFC2833) when hairpinned back to the original interface.

precedence
Specifies the selection precedence of Session Agents with same IP address.

- Default: 0 (disabled)
- Values: Min: 0 / Max: 4294967295

monitoring-filters
Comma-separated list of monitoring filters used for SIP monitor and trace.

auth-attribute
Enter the auth-attribute configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-recording-server
A maximum of four names of session-recording-servers, or session-recording-groups, or a combination of both exisiting in the realm associated with the session reporting client. Valid values are alpha-numeric characters. Session recording groups are indicated by prepending the groupname with **SRG:**

session-recording-required
Determines whether calls are accepted by the SBC if recording is not available.

- Default: disabled
- enabled—Restricts call sessions from being initiated when a recording server is not available.
- disabled—Allows call sessions to initiate even if the recording server is not available.

sm-icsi-match-for-invite
The ICSI URN to match on to increment the session-based messaging counters.

- Default: urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.msg

sm-icsi-match-for-message
The ICSI URN to match on to increment the event-based messaging counters.

- Default: urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.largemsg

ringback-file
Specifies the name of the media file, stored previously in /code/media, that the system plays when triggered for this realm.

ringback-trigger
Specifies when the system triggers the local media playback function.

- Default: none
- none—The system does not perform local media playback procedures. Based on precedence, however, the system may issue playback based on other element configurations. Local media playback follows the precedence session-agent, realm, then sip-interface.
- disabled—The system does not perform media playback procedures on this flow, regardless of ensuing configurations.
- 180-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message that does not include SDP.
- 180-force—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message.
- 183—Starts playback to caller when 183 is sent to call originator. The system stops the playback on the final response (either 2xx success or 4xx error). Configure this 183 value on the original INVITE ingress realm/sip-interface/session-agent.
- refer—Starts playback to the referee when it receives a REFER. This trigger operates only if the OCSBC actually terminates and performs the refer operation. If the REFER is via proxy, playback is not a triggered. Playback stops when the refer operation is complete with a final response (200-299 or 400-699). Configure this refer value on the ingress realm/sip-interface/session-agent of the transferred call.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- 183-and-refer—Starts playback when both 183 and refer triggers are activated.
- 183-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 183 message that does not include SDP.
- playback-on-header—Starts or stops playback based on the presence of the P-Acme-Playback header and its definitions.

sti-as
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send AS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mystiGroupName`.

sti-vs
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send VS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mystiGroupName`.

sti-orig-id
Specifies the UUID v4 to be added to STI-AS requests, if not already present, during STIR/SHAKEN functions.

sti-attest
Specifies the attestation value that is sent in AS request, during STIR/SHAKEN functions. The default is empty

- full-attestation
- partial-attestation
- gateway-attestation

sti-signaling-attest
Enable this parameter to instruct the SBC to use attestation level and origination ID headers from the ingress SIP INVITE in the REST query to the STI-AS, if preferred. When enabled, the Attestation-Info and Origination-ID headers override the configured values, if present. If one of the two requested headers is present, the other value is obtained from configured parameters.

- Default: Disable—The system does not use the attestation value and origId from SIP headers.
- Enable—The system uses the attestation value and origId from SIP headers, when present.

fax-servers
Enter the name of the **session-group** you have configured to be the group of fax machines to which this **session-agent** directs fax traffic when it receives a fax tone.

trigger-oos-alarm
Enables the system to trigger an alarm if and when this session agent goes out of service.

- Default: Disabled
- Values: Enabled/Disabled

static-tcp-source-port
Set the static TCP source port to use when connecting to this session agent.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: 0, 1025 - 65535

Path

session-agent is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-agent.**

This is a multiple instance configuration element.

session-agent > auth-attributes

The auth-attributes element provides the parameters used by the Oracle Communications Session Border Controller to perform digest authentication with the parent session agent.

Parameters

auth-realm
Enter the name (realm ID) of the host realm initiating the authentication challenge. This value defines the protected space in which the digest authentication is performed. Valid value is an alpha-numeric character string.

- Default: blank

username
Enter the username of the client. Valid value is an alpha-numeric character string.

- Default: blank

password
Enter the password associated with the username of the client. This is required for all LOGIN attempts. Password displays while typing but is saved in clear-text (i.e., *****). Valid value is an alpha-numeric character string.

- Default: blank
- Values: round-robin | hunt

in-dialog-methods
Optionally enter the in-dialog request method(s) that digest authentication uses from the cached credentials. Specify request methods in a list form separated by a space enclosed in parentheses. Valid values are.

- Default: blank
- Values: INVITE | BYE | ACK | OPTIONS | SUBSCRIBE | PRACK | NOTIFY | UPDATE | REFER

Path

auth-attributes is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router**, and then **session-agent**, and then **auth-attributes**.

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-agent > in-session-translations

Use the **in-session-translations** element to configure the session translations that apply to incoming traffic on this session-agent.

Parameters

in-session-translation-id
Enter the id of the session transation to apply to this session-agent.

state
Declare whether this session translation is enabled or disabled.

- Default: enabled
- Values: enabled | disabled

move
Change the order of execution.
The syntax of the command:

```
move <from-position> <to-position>
```

For example, to move the second session translation into the first position:

```
move 2 1
```

Path

The **in-session-translations** element is under the **session-router** path.

```
ORACLE# conf term
ORACLE(configure)# session-router
ORACLE(session-router)# session-agent
ORACLE(session-agent)# in-session-translations
ORACLE(in-session-translation-list)#
```

> **Note**
>
> This is a multiple instance configuration subelement.

session-agent > out-session-translations

Use the **out-session-translations** element to configure the session translations that apply to outgoing traffic on this session-agent.

Parameters

out-session-translation-id
Enter the id of the session transation to apply to this session-agent.

Copyright © 2024, 2026, Oracle and/or its affiliates.

state
Declare whether this session translation is enabled or disabled.

- Default: enabled
- Values: enabled | disabled

move
Change the order of execution.
The syntax of the command:

```
move <from-position> <to-position>
```

For example, to move the second session translation into the first position:

```
move 2 1
```

Path

The **out-session-translations** element is under the **session-router** path.

```
ORACLE# conf term
ORACLE(configure)# session-router
ORACLE(session-router)# session-agent
ORACLE(session-agent)# out-session-translations
ORACLE(out-session-translation-list)#
```

> **Note**
>
> This is a multiple instance configuration subelement.

session-agent > match-identifier

The match-identifier sub-element provides the parameters for the session-agents representing nodes behind Oracle Communications Session Border Controller to assist in the identification of the session-agents.

Parameters

identifier-rule
Configure with the name of a **session-agent-id-rule**

match-value
Enter a string value to be matched with the value in the SIP header for identifying a session agent.

> **Note**
>
> The comparison between the **match-value** and the value of the SIP header parameter and is an exact and case-sensitive match.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

session-agent is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-agent> match-identifier**

> **Note**
>
> This is a multiple instance configuration element.

session-agent > rate-constraints

The rate-constraints subelement for the session-agent configuration element allows you to configure rate constraints for individual session agents, which can then be applied to the SIP interface where you want them used.

Parameters

method
Enter the SIP method name for the method you want to throttle

- Values:
  - NOTIFY
  - OPTIONS
  - MESSAGE
  - PUBLISH
  - REGISTER

max-inbound-burst-rate
For the SIP method you set in the method parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints.

- Default: 0
- Values: Min: 0 | Max: 999999999

max-outbound-burst-rate
For the SIP method you set in the method parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints.

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-sustain-rate
For the SIP method you set in the method parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints

- Default: 0
- Values: Min: 0 | Max: 999999999

Copyright © 2024, 2026, Oracle and/or its affiliates.

max-outbound-sustain-rate
For the SIP method you set in the method parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints

- Default: 0
- Values: Min: 0 | Max: 999999999

Path

rate-constraints is an element of the **session-router** path. The full path from the topmost ALCI prompt is:**configure terminal**, and then **session-router**, and then **session-agent rate-constraints.**

session-agent-group

The session-agent-group element creates a group of Session Agents and/or groups of other SAGs. The creation of a SAG indicates that its members are logically equivalent and can be used interchangeably. This allows for the creation of constructs like hunt groups for application servers or gateways.

Parameters

group-name
Enter the name of the session-agent-group element. This required entry must follow the Name Format, and it must be unique.

description
Describe the session agent group element

state
Enable or disable the session-agent-group element

- Default: enabled
- Values: enabled | disabled

app-protocol
Distinguish H.323 session agent groups from SIP session agent groups

- Default: SIP
- Values: H323 | SIP

strategy
Select the session agent allocation options for the session-agent-group. Strategies determine how session agents will be chosen by this session-agent-group element.

- Default: Hunt
- Values:
  - Hunt—Selects session agents in the order in which they are listed
  - RoundRobin—Selects each session agent in the order in which they are listed in the dest list, selecting each agent in turn, one per session. After all session agents have been used, the first session agent is used again and the cycle continues.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- LeastBusy—Selects the session agent that has the fewest number of sessions relative to the max-outbound-sessions constraint or the max-sessions constraint (i.e., lowest percent busy) of the session-agent element
- PropDist—Based on programmed, constrained session limits, the Proportional Distribution strategy proportionally distributes the traffic among all of the available session-agent elements
- LowSusRate—Routes to the session agent with the lowest sustained rate of session initiations/invitations

dest
Enter one or more destinations (i.e., next hops) available for use by this session-agent group. The destination value(s) must correspond to a valid IP address or hostname.

trunk-group
Enter trunk group names and trunk group contexts to match in either IPTEL or custom format. If left blank, the Oracle Communications Session Border Controller uses the trunk group in the realm for this session agent group. Multiple entries are surrounded in parentheses and separated from each other with spaces.

Entries for this list must one of the following formats: tgrp:context or tgrp.context.

sag-recursion
Enable or disable SIP SAG recursion for this SAG

- Default: disabled
- Values: enabled | disabled

stop-sag-recurse
Enter the list of SIP response codes that terminate all further recursions, including those external to the SAG. On encountering the specified response code(s), the Oracle Communications Session Border Controller returns a final response to the UAC and stops trying to route the message. This includes not attempting to contact higher-cost SAs.

You can enter the response codes as a comma-separated list or as response code ranges.

- Default: 401, 407

sip-recursion-policy
Enter the SIP recursion policy for the session-agent-group, if configured in the session-router.

Path

session-agent-groupis an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-group.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-agent-id-rule

The session-agent-id-rule specifies the SIP header of the ingress SIP message that can be used in identifying the session-agents. The rule consists of four parameters: name, match-header, match-parameter and uri-type. All the parameters must follow the Name Format.

Parameters

name
Enter a name for the session-agent-id-rule(s). This required entry

match-header
Enter a name for the match-header. This required entry.

match-parameter
Enter a name for the match-parameter. This parameter is optional.

uri-type
Enter a name for the uri-type. This is an optional parameter.

- Values : uri_param, uri_header, uri_user, uri_host, uri_port, uri_user_param, uri-display, uri-user-only, uri-phone-number-only.

Path

session-agent-id-rule is an element under the session-router-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-agent-id-rule.**

> **Note**
>
> This is a multiple instance configuration element.

session-constraints

The session-constraints configuration element allows you to create session layer constraints in order to manage and police session-related traffic including maximum concurrent sessions, maximum outbound concurrent sessions, maximum session burst rate, and maximum session sustained rate.

The SIP interface configuration’s constraint-name parameter invokes the session constraint configuration you want to apply. Using the constraints you have set up, the Oracle Communications Session Border Controller checks and limits traffic according to those settings for the SIP interface. Of course, if you do not set up the session constraints or you do not apply them in the SIP interface, then that SIP interface will be unconstrained. If you apply a single session-constraint element to multiple SIP interfaces, each SIP interface will maintain its own copy of the session-constraint.

> **Note**
>
> The Oracle Communications Session Border Controller supports five concurrent SSH and/or SFTP sessions.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

name
Enter the name for this session constraint. This must be a unique identifier that you use when configuring a SIP interface on which you are applying it. This is a required parameter.

state
Enable or disable this session constraint

- Default: enabled
- Values: enabled | disabled

max-sessions
Enter the maximum sessions allowed for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-sessions
Enter the maximum inbound sessions allowed for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-outbound-sessions
Enter the maximum outbound sessions allowed for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-burst-rate
Enter the maximum burst rate (invites per second) allowed for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-burst-rate
Enter the maximum inbound burst rate (number of session invitations per second) for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-outbound-burst-rate
Enter the maximum outbound burst rate (number of session invitations per second) for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-sustain-rate
Enter the maximum rate of session invitations allowed within the current window for this constraint

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 | Max: 999999999

max-inbound-sustain-rate
Enter the maximum inbound sustain rate (of session invitations allowed within the current window) for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

max-outbound-sustain-rate
Enter the maximum outbound sustain rate (of session invitations allowed within the current window) for this constraint

- Default: 0
- Values: Min: 0 | Max: 999999999

min-seizures
Enter the minimum number of seizures for a no-answer scenario

- Default: 5
- Values: Min: 1 | Max: 999999999

min-asr
Enter the minimum ASR in percentage

- Default: 0
- Values: Min: 0 | Max: 100

cac-trap-threshold
The CAC (session or burst-rate) utilization threshold expressed as a percent that when exceeded generates a trap.

- Default: 0
- Values: Min: 0 / Max: 99

time-to-resume
Enter the number of seconds that is used to place an element (like a session agent) in the standby state when it has been taken out of service because of excessive transaction timeouts

- Default: 0
- Values: Min: 0 | Max: 999999999

ttr-no-response
Enter the time delay in seconds to wait before changing the status of an element (like a session agent) after it has been taken out of service because of excessive transaction timeouts

- Default: 0
- Values: Min: 0 | Max: 999999999

in-service-period
Enter the time in seconds that elapses before an element (like a session agent) can return to active service after being placed in the standby state

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 | Max: 999999999

burst-rate-window
Enter the time in seconds that you want to use to measure the burst rate

- Default: 0
- Values: Min: 0 | Max: 999999999

> **Note**
>
> A default value of 0 means that the burst-rate-window is of 1 second.

sustain-rate-window
Enter the time in seconds used to measure the sustained rate.

- Default: 0
- Values: Min: 0 | Max: 999999999

The value you set here must be higher than or equal to the value you set for the burst rate window.

rate-constraints
Access the rate-constraints subelement

Path

session-constraintsis an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal > session-router > session-constraints.**

session-constraints > rate-constraints

The rate-constraints subelement for the session-constraints configuration element allows you to configure rate constraints for individual session constraints, which can then be applied to the SIP interface where you want them used.

Parameters

method
Enter the SIP method name for the method you want to throttle

- Values:
  - NOTIFY
  - OPTIONS
  - MESSAGE
  - PUBLISH
  - REGISTER

max-inbound-burst-rate
For the SIP method you set in the method parameter, enter the number to restrict the inbound burst rate on the SIP interface where you apply these constraints.

- Default: 0

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 | Max: 999999999

max-outbound-burst-rate
For the SIP method you set in the method parameter, enter the number to restrict the outbound burst rate on the SIP interface where you apply these constraints.

- Default: 0
- Values: Min: 0 | Max: 999999999

max-inbound-sustain-rate
For the SIP method you set in the method parameter, enter the number to restrict the inbound sustain rate on the SIP interface where you apply these constraints

- Default: 0
- Values: Min: 0 | Max: 999999999

max-outbound-sustain-rate
For the SIP method you set in the method parameter, enter the number to restrict the outbound sustain rate on the SIP interface where you apply these constraints

- Default: 0
- Values: Min: 0 | Max: 999999999

method
Enter the SIP method name for the method you want to throttle

Path

session-constraints> > **rate-constraints** is an element of the session-router path. The full path from the topmost ALCI prompt is: **configure terminal**, and then **session-router**, and then **session-constraints**, and then **rate-constraints**.

session-recording-group

The **session-recording-group** element allows you to configure SIPREC server groups.

Parameters

name
Unique name for the session recording group that is a collection of one or more session recording servers. This name can be referenced when configuring realm-config, session-agent, and sip-interface by prepending this object with SRG:

description
Brief description of this session recording group. This parameter is optional.

strategy
Strategy for selecting an individual session recording server.

- Default: hunt
- Values:
  - hunt

Copyright © 2024, 2026, Oracle and/or its affiliates.

- roundrobin
- leastbusy
- propdist
- lowsusrate

simultaneous-recording-servers
The number of simultaneous SIP dialogs that the session reporting client (Oracle Communications Session Border Controller) establishes to the session reporting servers in the session reporting group per communication session.

- Default: 1
- Min: 1 / Max: 10

session-recording-servers
Names of the session recording servers configuration objects that belong to this session recording group. Valid values are alpha-numeric characters.

Path

session-recording-group is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system**, and then **session-router** , and then **session-recording-group.**

session-recording-server

The **session-recording-server** element allows you to configure SIPREC functionality.

Parameters

name
Name of this session recording server element.

description
Brief description of this session recording server. This parameter is optional.

realm
Realm in which this session recording server is located.

mode
Operating mode of this session recording server.

- selective—Unique recording server created per communication session
- persistent

destination
Address of the session recording server that defines the SIP address (request URI) of the session recording server. Enter values in the format IP address or FQDN. Default is no value specified.

port
The port portion of the destination address.

- Default: 5060
- Min: 1024 / Max: 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

transport-method
Protocol used to communicate with the recording server.

- Default: DynamicTCP
- UDP
- UDP+TCP
- DynamicTCP
- StaticTCP
- DynamicTLS
- StaticTLS
- DTLS
- TLS+DTLS
- StaticSCTP

force-parity
Enables the system to enforce port number parity for flows between the system and the session recording server.

- Default: Disabled
- Values: Enabled | Disabled

ping-method
SIP method type to ping with session recording server.

ping-interval
Rate at which to ping the Session Agent configured as a session recording server.

- Default: 0
- Min: 0 / Max: 4294967295

refresh-interval
Enables the SIP OPTIONS request/response mechanism, and assign a value to the refresh-timer toward the SIPREC server. This measures the maximum allowed interval (in seconds) between the OPTIONS request sent by the call-recording client and the OPTIONS response returned by the call-recording server.
By default, refresh-interval is set to 0, which disables detection of a failed recording session dialog. Assignment of any non-zero value enables detection and sets the allowable interval between OPTIONS requests and responses.

- Default: 0
- Min: 0 / Max: 60

Path

session-recording-server is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-recording-server.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-router-config

The session-router-config element allows you to configure whether or not session-related functionality is enabled within your network, whether it contains a Oracle Communications Session Border Controller SR or SD.

Parameters

state
Enable or disable this session-related functionality on the system

- Default: enabled
- Values: enabled | disabled

system-number-type
Define the telephone number format used in local policy and local policy lookups

- Default: Pots
- Values:
  - Pots—Telephone numbers are in Decimal routing number format (0-9). This is the default and recommended setting.
  - E164—Telephone numbers are in E.164 format as defined by the global-number format of the tel URI defined in RFC 3966
  - Routing—Telephone numbers are in Penta Decimal routing numbers (0-9, A-F). This value is not currently used but reserved for future enhancements.

sr-primary-name
Enter the name of the primary session router; must match the target name in the boot parameters of the primary SR

sr-primary-address
Enter the IP Address of the maintenance interface of the primary session router; must match the "inet on ethernet" address in the boot parameters of the primary SR

sr-secondary-name
Enter the name of the secondary session router; must match the target name in the boot parameters of the secondary SR

sr-secondary-address
Enter the IP Address of the maintenance interface of the secondary session router. This must match the "inet on ethernet" address in the boot parameters of the secondary SR.

divide-resources
Indicate whether or not resources are divided by the number of configured session directors. This includes:

- realm-config bandwidth
- session-agent max-sessions
- session-agent max-outbound-sessions
- session-agent max-burst-rate
- session-agent max-sustain-rate

Copyright © 2024, 2026, Oracle and/or its affiliates.

- – Default: disabled
  - – Values: enabled | disabled

match-lp-src-parent-realms
Enable or disable local policy parent realm matching based on a parent realm

- Default: disabled
- Values: enabled | disabled

nested-realm-stats
Enable or disable using session constraints for nested realms across the entire system

- Default: disabled
- Values: enabled | disabled

reject-message-threshold
Enter the minimum number of message rejections allowed in the reject-message-window time on the Oracle Communications Session Border Controller (when using the SIP manipulation action reject) before generating an SNMP trap

- Default: 0 (no trap is sent)
- Values: Min: 0 / Max: 999999999

reject-message-window
Enter the time in seconds that defines the window for maximum message rejections allowed before generating an SNMPS trap

- Default: 10
- Values: Min: 1 / Max: 999999999

force-report-trunk-info
Enable or disable generation of VSAs for trunk group information even when you are not using trunk-group routing; VSAs 65-68 to report originating and terminating trunk group information

- Default: disabled
- Values: enabled | disabled

session-directors
Access the session-directors subelement.

holidays
Access the session-router-holidays subelement.

additional-lp-lookups
Enter the number of additional local policy per message lookups

- Default: 0 (disables multistaged local policy lookup)
- Values: Min: 0 | Max: 5

max-routes-per-lookup
Enter the maximum number of routes per local policy lookup

- Default: 0 (no limit on the number of returned routes)
- Values: Min: 0 | Max: 999999999

Copyright © 2024, 2026, Oracle and/or its affiliates.

total-lp-routes
Enter the total number of routes for all local policy lookups per message request

- Default: 0 (no limit on the number of returned routes)
- Values: Min: 0 | Max: 999999999

multi-stage-src-realm-override
Sets the system to use the original received realm as the source realm for multistage local policy lookups through every stage when set to enabled. A setting of disabled sets the system to use the previous stage's next-hop as the source realm in the current stage.

- Default: disabled
- Values: enabled | disabled

retry-after-upon-offline
Supports load balancing restart for when the Oracle Communications Session Border Controller is configured as a cluster member in conjunction with the Oracle Communications Session-aware Load Balancer.

- Default: disabled
- Values: enabled | disabled

Path

session-router-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-router.**

> **Note**
>
> This is a single instance configuration element.

session-router > holidays

The session-router-holidays configuration subelement establishes the holiday schedule to which the Oracle Communications Session Border Controller conforms.

Parameters

date
Enter the date of a holiday in **yyyy-mm-dd:hh:mm:ss** format. A session router holidays entry will not function properly unless it is a valid

description
Describe the holiday

Path

session-router-holidays is a subelement under the session-router-config element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **session-router** , and then **holidays**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This is a multiple instance configuration element.

session-timer-profile

The session-timer-profile element is used to configure support for RFC 4028 Session Timers.

Parameters

name
The name of this session-timer-profile element. This value is configured in a sip-interface's session-timer-profile parameter.

session-expires
The value of the session expires header in seconds

- Default: 1800
- Values: 64-999999999

min-se
The value of the Min-SE header in seconds (this is a minimum session expires value).

- Default: 90
- Values: 64-999999999

force-reinvite
Sets if the Oracle Communications Session Border Controller will send a reINVITE to refresh the session timer when applicable

- Default: disabled
- Values: enabled | disabled

request-refresher
Set on the outbound side of a call what the Oracle Communications Session Border Controller sets the refresher parameter to. Valid values are uac,, uas, or none.

- Default: uac
- Values: nane | uac | uas

response-refresher
Set on the inbound side the value of the refresher parameter in the 200OK message.

- Default: uas
- Values: uac | uas

Path

session-timer-profileis an element under the session-router path. The full path from the topmost ACLI prompt is:**configure terminal**, and then **session-router**, and then **session-timer-profile**.

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-translation

In the **session-translation** element, you give your session translation an identifier and then enter the **session-trans-rule** subelement to define translation rules. Once the **session-translation** element is configured, you can apply it to a realm or a session agent.

Parameters

id
Enter the identifier or name for this set of session translation rules. Use this id when applying a session translation to a realm or a session agent.

session-trans-rule
Enter the **session-trans-rule** subelement.

Path

The **session-translation** element is under the session-router path.

```
ORACLE# conf t
ORACLE(configure)# session-router
ORACLE(session-router)# session-translation
ORACLE(session-translation)#
```

session-translation > session-trans-rule

In the **session-trans-rule** element, you can enable or disable specific rules, declare whether a rule is required, and define the order in which your rules execute.

Parameters

rule-id
Enter the `id` value of the translation rule you want to group within this session translation.

mandatory
Declare whether this rule is required.
If a mandatory rule fails, all the translation rules in the parent **session-translation** object are rolled back. If a non-mandatory rule fails, the other rules within the **session-translation** element continue to execute.

- Default: disabled
- Values: disabled | enabled

state
Declare whether this rule is enabled or disabled.

- Default: enabled
- Values: disabled | enabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

move
Change the order of execution.

```
move <from-position> <to-position>
```

For example, to move the group's second rule to the first position so that it gets executed first, run this command:

```
move 2 1
```

Path

The **session-trans-rule** element is under the session-router path.

```
ORACLE# conf t
ORACLE(configure)# session-router
ORACLE(session-router)# session-translation
ORACLE(session-translation)# session-trans-rule
ORACLE(session-trans-rule)#
```

schedule-backup

The schedule-backup configuration element allows you to configure general collection commands for backing up your configuration on the Oracle Communications Session Border Controller.

Parameters

admin-state
Enables or disables scheduled backup for this system.

- Default: disable
- Values: enable | disable

config-backup
Provides access to the **config-backup** sub-element.

Path

schedule-backup is an element of the system-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system-config**, and then **schedule-backup**.

> **Note**
>
> This is a single instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

schedule-backup > config-backup

The config-backup configuration sub-element allows you to configure specific detail about when you back up your configuration on the Oracle Communications Session Border Controller.

Parameters

admin-state
Enable or disable this configuration backup feature. This parameter is disabled by default.

- disabled (default)
- enabled

interval
Specifies the interval the system uses before it pushes a new backup.

- weekly—7 days from last backup (default)
- daily—24 hours from last backup
- monthly—30 days from last backup

retry-interval
Specifies the interval the system waits before it tries to resend a configuration backup after an attempt fails.

- Default: 5 minutes
- Values: Min: 5 | Max: 30

retry-count
Specifies the maximum number of times the system tries to resend a configuration backup after prior attempts fail.

- Default: 5 retries
- Values: Min: 2 | Max: 10

push-failure-alarm
Enables or disables the generation of alarms and traps in case of any push-receiver failures. This alarm is of severity type Warning.

- Default: enabled
- Values: enabled | disabled

push-receiver
Access the push-receiver sub-element.

Path

config-backup is a subelement element of the system-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system-config**, and then **schedule-backup**, and then **config-backup**.

> **Note**
>
> This is a single instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

schedule-backup > config-backup > push-receiver

The push-receiver configuration sub-element allows you to configure the Oracle Communications Session Border Controller to push your backup configuration files to a specified node.

Parameters

address
Specifies the hostname or IP address to which the Oracle Communications Session Border Controller pushes the current configuration file.

user-name
Specifies the login user name for the specified server used when pushing the current configuration file.

password
Specifies the login password for the specified server used when pushing the current configuration file.

data-store
Enter the absolute path on the specified server in which to put the current configuration file.

protocol
Specifies the protocol with which to send the scheduled backup the current configuration file.

- Default SFTP
- Values SFTP

Path

push-receiver is a subelement element of the system-config path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system-config**, and then **schedule-backup**, and then **config-backup**, and then **push-receiver**.

> **Note**
>
> This is a multiple instance configuration element.

sip-advanced-logging

The sip-advanced-logging configuration element allows you to configure advanced logging objects on the Oracle Communications Session Border Controller.

Parameters

name
Name to display on the log message for this set of criteria.

state
Specifies whether this named instance is enabled or disabled.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: enabled
- Values: enabled | disabled

level
Log level for this advanced logging set of criteria. This corresponds to the system's available log levels.

- Default: DEBUG
- Values: ZERO | NONE | EMERGENCY | CRITICAL | MAJOR | MINOR | WARNING | NOTICE | INFO | TRACE | DEBUG | DETAIL

scope
The range of SIP messages and, if configured, media for which this advanced logging criteria creates log messages.

- Default: session-and-media
- Values: request-only | transaction | session | session-and-media

matches-per-window
The number of matches, within the window size, for which the system generates log messages.

- Default: 1
- Values: An integer between 1 and 999999999

window-size
The amount of time, in seconds, to sample for matches within the traffic.

- Default: 1
- Values: An integer between 1 and 999999999

condition
Type this parameter to enter the adv-logging-conditions subelement. Specify the match criteria for which the system creates log messages. Each logging criteria set supports multiple match conditions.

Path: **sip-advanced-logging** is an element of the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-advanced-logging.

> **Note**
>
> This is a multiple instance configuration element.

sip-advanced-logging > condition

The sip-advanced-logging's condition subelement allows you to configure multiple sets of matching criteria for the associated sip-advanced-logging element on the Oracle Communications Session Border Controller.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

match-type
A string identifying the type of information within the SIP message on which the system attempts to find a matching value.

- Default: recv-agent
- Values: request-type | recv-agent | recv-realm | request-uri-user | request-uri-host | to-header-user | to-header-host | from-header-user | from-header-host | call-id

match-procedure
Indicates whether the match-value attribute will contain regex or an exact string.

- Default: exact-match
- Values: exact-match | regex-match

match-value
A string the system uses as the matching string within the SIP message.

- If the match-type is "request-type", valid values include:
  - REGISTER | INVITE | ACK | BYE | CANCEL | PRACK | OPTION | INFO | SUBSCRIBE | NOTIFY | REFER | UPDATE | MESSAGE | PUBLISH
- For all other match-types, enter the string the system must find in the message.

Path: **adv-log-condition** is a subelement of the sip-advanced-logging element. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-advanced-logging > condition.

> **Note**
>
> This is a multiple instance configuration subelement.

sip-config

The sip-config element is used to define the parameters for this protocol specific to the SBC communicating with SIP.

Parameters

state
Enable or disable the SIP operations

- Default: enabled
- Values: enabled | disabled

operation-mode
Select the SIP operation mode

- Default: dialog
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- disabled—Setting this parameter to disabled sets it to its default, dialog.
- stateless—Stateless proxy forwarding. SIP requests are forwarded based on the Request-URI and local policy. No transaction, session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.
- transaction—Transaction stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The SBC maintains transaction state in accordance with RFC 3261. No session or dialog state is maintained. No media state is maintained, and session descriptions in the SIP messages are not modified.
- session—Session stateful proxy mode. SIP requests are forwarded based on the Request-URI and local policy. The SBC maintains transaction state in accordance with RFC 3261. The SD also maintains session state information. A Record-Route header is inserted in requests so that the SBC will remain in the path. No media state is maintained, and session descriptions in the SIP messages are not modified.
- dialog—Dialog stateful B2BUA mode. The SBC maintains full transaction, session, and dialog state. If media management is enabled, full media state is also maintained and the SBC modifies session descriptions in SIP messages to cause the media to flow through the SBC.

dialog-transparency
Enable or disable SIP dialog transparency service to prevent the SBC from generating a unique Call-ID and modifying dialog tags

- Default: enabled
- Values: enabled | disabled

home-realm-id
Enter the identifier of the home realm. This is the network to which the SBC's SIP proxy (B2BUA) is logically connected. If configured, this field must correspond to a valid identifier field entry in a realm-config.

egress-realm-id
Enter the default egress realm identifier

auto-realm-id
Enter the auto config realm identifier

nat-mode
Select the home realm NAT mode. This is used to indicate whether the home realm is "public" or "private" address space for application of the SIP-NAT function.

- Default: none
- Values:
  - none—No SIP-NAT is necessary
  - private—Indicates that the home realm is private address space, and all other external realms are public address space. Addresses in the home realm will be encoded in SIP URIs sent into the external realm. The addresses are decoded when the URIs enter the home realm.

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - public—Indicates that the home realm is public address space. Addresses from external realms are encoded in SIP URIs as they enter the home realm. Addresses are decoded as they enter the external realm that the address originated in.

registrar-domain
Enter the domain name for identifying which requests for which Hosted NAT Traversal (HNT) or registration caching applies. The right-most portion of the "host" part of the Request-URI is matched against this value. An asterisk "*" is used to indicate any domain.

registrar-host
Enter the hostname or IP address of the SIP registrar for the HNT and registration caching function. An asterisk "*" is used when there are multiple SIP registrars and normal routing using the Request-URI or local policy is to be applied.

An IPV6 address is valid for this parameter.

registrar-port
Enter the port number of the SIP registrar server

- Defaul:t 0
- Range: 0, 1025 - 65535

register-service-route
Select the service-route usage for REGISTER requests.

- Default: always
- Values:
  - never—Never use service-route for REGISTER
  - always—Always user service-route for REGISTER
  - removal—Use service-route for de-registration
  - session—Use service-route when the UA has a session
  - session+removal—Use service-route for de-registration and for when the UA has a session

init-timer
Enter the initial timeout value in milliseconds for a response to an INVITE request, and it applies to any SIP request in UDP. In RFC 3261, this value is also referred to as TIMER_T1.

- Default: 500
- Values: Min: 0 / Max: 4294967295

max-timer
Enter the maximum retransmission timeout in milliseconds for SIP. In RFC 3261, this value is also referred to as TIMER_T2.

- Default: 4000
- Values: Min: 0 / Max: 4294967295

trans-expire
Enter the number of seconds used by the system to determine when to time-out SIP transactions. This timer is equivalent to TIMER_B in RFC 3261, and the same value is used for TIMER_D, TIMER_F, TIMER_H, and TIMER_J as set out in the same RFC.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 32
- Values: Min: 0 / Max: 2147473

initial-inv-trans-expire
Establishes a global, default transaction timeout value (expressed in seconds) used exclusively for initial INVITE transactions. The default value, 0, indicates that a dedicated INVITE Timer B is not enabled. Non-default integer values enable a dedicated Timer B and set the timer value.

- Default: 0
- Values: Min: 0 / Max: 2147473

invite-expire
Enter the TTL in seconds for a SIP client transaction after receiving a provisional response. This timer is equivalent to TIMER_C in RFC 3261.

- Default:: 180
- Values: Min: 0 / Max: 2147473

inactive-dynamic-conn
Enter the time limit in seconds for inactive dynamic connections

- Default: 32
- Values Min: 0 / Max: 4294967295

enforcement-profile
Enter the name of the enforcement profile (SIP allowed methods).

emergency-dscp-profile
Specifies the name of the emergency DSCP profile you want to apply to this sip-config.

pac-method
Enter the PAC ping method.

- Values: string

pac-interval
Enter the PAC ping interval.

- Default: 10
- Values Min: 0 / Max: 2147483647

pac-strategy
Enter the PAC distribution strategy.

- Default: PropDist
- Values: RoundRobin, LeastBusy, PropDist, LowSusRate

pac-load-weight
Enter the PAC CPU load weighting factor.

- Default: 1
- Values Min: 0 / Max: 100

pac-session-weight
Enter the PAC active sessions weighting factor.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 1
- Values Min: 0 / Max: 100

pac-route-weight
Enter the PAC SD-Route weighting factor.

- Default: 1
- Values Min: 0 / Max: 100

pac-callid-lifetime
Enter the PAC CallId route table entry lifetime.

- Default: 600
- Values Min: -2147483648 / Max: 2147483647

pac-user-lifetime
Enter the PAC User route table entry lifetime.

- Default: 3600
- Values Min: -2147483648 / Max: 2147483647

red-sip-port
Enter the port for sending or receiving SIP checkpoint messages. Setting this to 0 disables SIP HA on the SBC.

- Default: 1988
- Range: 0, 1025 - 65535

> **Note**
>
> This parameter is not RTC supported.

red-max-trans
Enter the size of the SIP signaling transaction list in entries stored in memory

- Default: 10000
- Values: Min: 0 / Max: 50000

> **Note**
>
> This parameter is not RTC supported.

red-sync-start-time
Enter the time in milliseconds before the HA SBC begins SIP signaling state checkpointing. As long as this HA SBC is healthy and active, it remains in a constant cycle of (re)setting this field's timer and checking to see if it has become standby.

- Default: 5000
- Values: Min: 0 / Max: 999999999

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not RTC supported.

red-sync-comp-time
Enter the time in milliseconds the standby SBC waits before checkpointing with the active SBC to obtain the latest SIP signaling transaction information once the initial checkpointing process is complete

- Default: 1000
- Values: Min: 0 / Max: 999999999

> **Note**
>
> This parameter is not RTC supported.

add-reason-header
Enables the system to add the reason header into response messages and CDRs for RFC 3326 support. Enabling this parameter also enables reason header interworking during native SIP-ISUP interworking.

- Default: disabled
- Values: enabled | disabled

sip-message-len
Set the size constraint in bytes on a SIP message

- Default: 4096
- Values: Min: 0 / Max: 65535

enum-sag-match
Enable or disable matching this SAG's group name to hostname portions of ENUM NAPTR or LRT replacement URIs.

- Default: disabled
- Values: enabled | disabled

extra-method-stats
Enable or disable the expansion SIP Method tracking feature. Enabling this parameter provides multiple enhancements to method counters, including:

- Enables the system to track transaction messages for specific SIP session agents, SIP realms, and SIP interfaces.
- Enables the system to provide message rate statistics for SIP traffic via ACLI and HDR output.
- Enables the configuration of specific method constraints.
- Enables the system to output counts of method success, timeout and failure events for SUBSCRIBE, NOTIFY and MESSAGE methods.

Values include:

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

extra-enum-stats
Enable or disable the ENUM extra statistics tracking feature.

- Default: disabled
- enabled | disabled

mps-volte
Enable or disable the Multimedia Priority Services for VoLTE.

- Default: disabled
- Values: enabled | disabled

rph-feature
Set the state of NSEP support for the global SIP configuration

- Default: disabled
- Values: enabled | disabled

nsep-user-sessions-rate
Set the CPS for call rates on a per user basis for NSEP. A value of 0 disables the call admission control on a per user basis.

- Default: 0
- Values: 0-999999999

nsep-sa-sessions-rate
Enter maximum acceptable number of SIP INVITES (NSEP sessions) per second to allow for SIP session agents. 0 means there is no limit.

- Default: 0
- Values Min: 0 / Max: 999999999

registration-cache-limit
Set the maximum number of SIP registrations that you want to keep in the registration cache. A value of 0 means there is no limit on the registration cache, therefore disabling this feature.

- Default: 0
- Values: Min: 0 / Max: 999999999

register-use-to-for-lp
Enable or disable the use of an ENUM query to return the SIP URI of the Registrar for a SIP REGISTER message for routing purposes

- Default: disabled
- Values: enabled | disabled

options
Enter customer-specific features and/or parameters. This optional field allows for a comma separated list of “feature=<value>" or "feature" parameters for the sip-config element.

refer-src-routing
Enable or disable the use of the referring party’s source realm lookup policy to route subsequent INVITEs after static or dynamic REFER handling has been terminated. When disabled, the system derives the lookup from the source realm of the calling party.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

add-ucid-header
Enable or disable the using the UCID to correlate replicated SIP message information when you use SRR.

- Default: disabled
- Values enabled | disabled

proxy-sub-events
Configured list of SIP event package names that you want the SBC to proxy (rather than maintain state) to the destination. You can enter more than one value by enclosing multiple values in quotations marks

allow-pani-for-trusted-only
Allow PANI header only for trusted domains

- Default: inherit
- Values: inherit | enabled | disabled

atcf-stn-sr
Enter the value of the Session Transfer Interface, Single Radio (STN-SR).

atcf-psi-dn
Enter the value to use for the Public Service Identity Domain Name (PSI-DN).

atcf-route-to-sccas
When set to disabled (default), the handover update, an INVITE, is routed to the IMS Core. When enabled, the INVITE is routed directly to the SCCAS.

- disabled
- enabled | disabled

eatf-stn-sr
E-STN-SR allocated by EATF in INVITE handover message.

pass-gruu-contact
Enable or disable the sip-config to parse for GR URI parameter in the contact header in non-registered endpoints' messages.

- Default: disabled
- Values enabled |disabled

sag-lookup-on-redirect
Enable/disable lookup of SAG name on a redirect

- Default: disabled
- Values enabled | disabled

set-disconnect-time-on-bye
Sets the disconnect time reflected in a RADIUS CDR to when the SBC receives a BYE message.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

refer-reinvite-no-sdp
Globally enables the SBC to exclude SDP in re-INVITE responses sent to transfer-targets.

- Default: disabled
- Values: enabled | disabled

msrp-delayed-bye-timer
Enables the delayed transmission of SIP BYE requests, for active MSRP sessions. This parameter specifies the maximum delay period allowed before transmitting the delayed BYE request.

- Default 15
- Min: 0 / Max: 60

> **Note**
>
> A value of 0 disables this parameter.

transcoding-realm
Name of a configured realm designated as the separate realm for the public SIP interface, to be used only for communication with the T-SBC in pooled transcoding deployments.

transcoding-agents
IP address, session agent hostname, or SAG name in this list if you want them to be used as transcoding agents. You can make multiple entries in any combination of these values. For example, you might list an IPv6 address, a session agent, and a SAG. To make multiple entries in the list using in one command line, enclose the entire list in parentheses, separating each with a space.

- To add a transcoding agent to an existing list, put a plus sign before the value you want to add, e.g. +154.124.2.8.
- To remove a transcoding agent from an existing list, put a minus sign before the value you want to remove, e.g. -154.124.2.8.

create-dynamic-sa
To support the creation of dynamic session agents for remote S-CSCFs on in-coming service routes, change this parameter from disabled (default) to enabled.

- Default: disabled
- Values: enabled | disabled

node-functionality
a global value to insert into the Node-Functionality AVP when the Oracle Communications Session Border Controller sends ACRs over the Rf interface to an appropriate destination.

- Default: P-CSCF
- Values: P-CSCF | BGCF | IBCF | E-CSCF

match-sip-instance
Enables the use of the `+sip-instance-id` when matching incoming calls with the registration cache.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

sa-routes-stats
This enables collecting session agent statistics for DNS-resolved session agents.

- Default: disabled
- Values: enabled | disabled

sa-routes-traps
This enables traps on DNS resolved session-agents when a route changes state.

- Default: disabled
- Values: enabled | disabled

rx-sip-reason-mapping
This enables the Rx Interface Reason Header Usage mapping feature.

- Default: disabled
- Values: enabled | disabled

add-ue-location-in-pani
Set this to add UE Location string in PANI header when available.

- Default: disabled
- Values: enabled | disabled

hold-emergency-calls-for-loc-info
Timer to hold emergency calls until the system receives location information from the PCRF.

- Default: 0
- Values: 0 - 4294967295

npli-upon-register
This adds the ability to capture Network Provided Location Information during the Registration process.

- Default: inherit
- Values: inherit | enabled | disabled

msg-hold-for-loc-info
Maximum number of seconds that the system will hold MESSAGEs for location information for the NPLI for Short Message feature.

- Default: 0—disabled
- Values: 0 - 30 seconds

cache-loc-info-expire
Maximum number of seconds after which the system will drop network location information for the NPLI for Short Message feature, unless the **keep-cached-loc-info-after-timeout** parameter is enabled.

- Default: 32
- Values: Min: 0 / Max: 4294967295

Copyright © 2024, 2026, Oracle and/or its affiliates.

keep-cached-loc-info-after-timeout
If this option is enabled, the location information will be left in the cache and used in subsequent MESSAGEs after the **cache-loc-info-expire** time expires.

- Default: disabled
- Values: enabled | disabled

atcf-icsi-match
ATCF ISCI matching rule for the ATCF ISCI Invite Matching feature.

- Value: enter the ICS string you want to match.

start-hold-timer-event
Starts the hold timer according to the trigger configured.

- Default: AAR
- Values: AAR | AAA

hist-to-div-for-cause-380
Determines whether to interwork cause 380 messages within history-Info and Diversion header interworking.

- Default: disabled
- Values:
  - enabled—enables the message interworking.
  - disabled—disables the message interworking.

anonymize-history-for-untrusted
Enables anonymization of history and diversion headers for untrusted peers.

- Default: disabled
- Values: enabled | disabled

asymm-preconditions-evs-swb-support
Enable this parameter to perform an internal bandwidth mapping of EVS codecs when presented with the super-wideband codec option within the context of transcoding free operation (TrFO) for asymmetric preconditions.

- Default: disable
- enabled

sms-report-timeout
Specifies the amount of time, in seconds, before the system discards accounting for a message because it did not receive a delivery report /submit SMS report.

- Default: 32
- Values: 1-100000 seconds

retry-after-upon-offline
When the system is becoming an offline state, refresh registrations for endpoints that do not have any active calls are rejected with a configurable response code defined in this parameter. The default for this parameter is the 503 Service Unavailable message and includes a Retry-After header with a configurable timer set in retry-after-upon-offline. Note that if this value is set to 0, the SBC returns Retry-After:0, which means immediately.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 0 / Max: 999999999

reg-reject-response-upon-offline
Refresh registrations for endpoints that do not have any active calls are rejected with a configurable response code defined in this parameter. The default for this parameter is the 503 Service Unavailable message and includes a Retry-After header with a configurable timer set in **retry-after-upon-offline**.

user-agent
Reserved for use with Microsoft Teams integrations only.

precondition-enhancement
Enable or disable asymmetric precondition enhancement.

- Default: disabled
- Values: enabled | disabled

precondition-med-enhancement
Enables support for multiple early dialogs with preconditions and TrFO.

- Default: Disable
- Values: enable/disable

internal-503-threshold
Specifies, in percent utilization, the value above which the system triggers an alarm indicating the system is sending an excessive number of “503 Service unavailable” messages in response to INVITEs.

- Default: 0 (Disables alarm)
- Range: 0 - 100%

internal-503-lower-threshold
Specifies, in percent utilization, the value below which the system considers the number of “503 Service unavailable” messages it sends in response to INVITEs as acceptable. Operates in conjunction with the 503-alarm-monitoring-time to prevent the system from issuing multiple alarms for what you consider the same issue.

- Default: 40
- Range: 1 - 95%

503-alarm-monitoring-time
Operates in conjunction with the internal-503-lower-threshold, and specifies in minutes the duration for which the system considers an alarm condition triggered by the internal-503-threshold as still in effect. After the system triggers this alarm, it uses this window as the amount of time the number of “503 Service unavailable” messages sent must be below the internal-503-lower-threshold before the system can issue a new internal-503-threshold alarm. This logic prevents the system from issuing multiple alarms for what you consider the same issue.

- Default: 15
- Range: 5 - 600 minutes

response-code-and-phrase-config-name

Copyright © 2024, 2026, Oracle and/or its affiliates.

Enter the name of the response-code-and-phrase-config that you want to apply to the system globally. You can only apply one response-code-and-phrase-config at a time.

Path

sip-config is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-config.**

> **Note**
>
> This is a single instance configuration element.

sip-feature

The sip-feature element defines how the Oracle Communications Session Border Controller's B2BUA should treat specific option tags in SIP headers.

Parameters

name
Enter the option tag name that will appear in the Require, Supported, or Proxy-Require headers of SIP messages

realm
Enter the realm with which the feature is associated; to make the feature global, leave this parameter blank

support-mode-inbound
Select the treatment of feature (option tag) in a Supported header for an inbound packet

- Default: pass
- Values:
  - pass—B2BUA should include the tag in the corresponding outgoing message
  - strip—Tag should be excluded in the outgoing message. Use strip mode to not use the extension.

required-mode-inbound
Select the treatment of feature (option tag) in a Require header for an inbound packet

- Default: reject
- Values:
  - pass—B2BUA should include the tag in the corresponding outgoing message
  - reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

proxy-require-mode-inbound
Select the treatment of feature (option tag) in a Proxy-Require header for an inbound packet

- Default: pass
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - pass—B2BUA should include the tag in the corresponding outgoing message
  - reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

support-mode-outbound
Select the treatment of feature (option tag) in a Supported header for an outbound packet

- Default: pass
- Values:
  - pass—B2BUA should include the tag in the corresponding outgoing message
  - strip—Tag should be excluded in the outgoing message

require-mode-outbound
Select the treatment of feature (option tag) in a Require header for an outbound packet

- Default: reject
- Values:
  - pass—B2BUA should include the tag in the corresponding outgoing message
  - reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

proxy-require-mode-outbound
Select the treatment of feature (option tag) in a Proxy-Require header for an outbound packet

- Default: pass
- Values:
  - pass—B2BUA should include the tag in the corresponding outgoing message
  - reject—B2BUA should reject the request with a 420 (Bad Extension) response. The option tag will be included in an Unsupported header in the reject response.

Path

sip-feature is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-feature.**

> **Note**
>
> If an option tag is encountered that is not configured as a SIP feature, the default treatments described in each of the field descriptions (name, support-mode, require-mode, and proxy-require-mode) included in this section will apply. Therefore, a sip-feature element only needs to be configured when non-default treatment is required. This is a multiple instance element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-feature-caps

Configure to support SRVCC handover and other ATCF functionality.

Parameters

state
When enabled, the feature adds the Feature-Caps header to messages.

- Default: disabled
- Values: enabled | disabled

atcf-management-uri
Identifies the feature capability indicator that will be used to transport the ATCF management URI. When the value is **management** and the value of **state** is **enabled**, the Feature-Caps header "g.3gpp atcf-mgmt-uri" is added and the value of **atcf-psi-dn** in the **sip-config** configuration element. When the value is **psi** and the value of **state** is **enabled**, the Feature-Caps header "g.3gpp atcf-psi" is added and the value is the value of **atcf-psi-dn** in the **sip-config** configuration element.

- Default: disabled
- Values: disabled | management | psi

atcf-alerting
When enabled, the system adds the Feature-Caps header to messages and turns on the alerting feature.

- Default: disabled
- Values: enabled | disabled

atcf-pre-alerting
When enabled, the system adds the Feature-Caps header to messages and turns on the pre-alerting feature.

- Default: disabled
- Values: enabled | disabled

Path

sip-feature-caps is an element within the **session-router** path.

sip-interface

The sip-interface element allows you to configure a SIP interface for your Oracle Communications Session Border Controller.

Parameters

state
Enable or disable the SIP interface

- Default: enabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> Oracle does not recommend disabling and re-enabling a sip-interface operating with TCP ports. Depending on conditions and circumstances, you may not be able to re-enable this sip-interface without rebooting the system. If you need to disable, then re-enable a sip-interface, ensure that:
>
> - There are no ESTABLISHED in-bound sockets
> - The access-control-trust-level of the realm must not be configured to low or medium

realm-id
Enter the name of the realm to which the SIP interface applies

description
Provide a brief description of the **sip-interface** configuration element

sip-ports
Access the sip-ports subelement

carriers
Enter a list of carriers related to the sip-config. Entries in this field must follow the Carrier Format.

trans-expire
Set the transaction expiration timer in seconds

- Default: 0
- Values: Min: 0 | Max: 2147473

initial-inv-trans-expire
Transaction expiration time <TIMER_B> for initial INVITE.

- Default: 0
- Values: 0 - 2147473

invite-expire
Set the INVITE transaction expiration timer in seconds

- Default: 0
- Values: Min: 0 | Max: 2147473

max-redirect-contacts
Enter the maximum number of contact and route attempts in case of a redirect

- Default: 0
- Values: Min: 0 | Max: 10

proxy-mode
Set the default SIP request proxy mode

- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - proxy—Forward all SIP requests to other session agents
  - redirect—Send a SIP 3xx redirect response with contacts (found in the local policy) to the previous hop
  - record-route—Forward requests with Record-Route (for stateless and transaction and operation modes only)

redirect-action
Set handling of Redirect (3xx) response messages from a session agent.

- Default: Empty
- Values:
  - Proxy—Send the response back to the previous hop
  - Recurse—Recurse on the contacts in the response
  - Recurse-305-only—Recurse on the contacts in the 305 response

contact-mode
Select the contact header routing mode

- Default: none
- Values:
  - none
  - maddr
  - strict-route
  - loose-route

nat-traversal
Select the type of HNT functionality for SIP

- Default: none
- Values:
  - none—NAT Traversal is disabled
  - always—Performs HNT when SIP-Via and transport addresses do not match

> **Note**
>
> The **nat-traversal** parameter can establish an important media handling behavior. If you set **nat-traversal** on a **sip-interface** to **always**, this setting supersedes any multi-media configuration that would otherwise release the media. Instead, the SBC recognizes when a flow's leg is behind a NAT during the signaling, and ignores any configuration that would release the media. The SBC then sets up the end to end media flow in MBCD and performs its HNT function for that flow.

  - rport—Performs HNT when Via rport parameter is present and SIP-Via and transport addresses do not match

nat-interval
Enter the expiration time in seconds for the system's cached registration entry for an endpoint doing HNT

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 30
- Values: Min: 1 | Max: 4294967295

tcp-nat-interval
Enter the TCP NAT traversal registration interval in seconds

- Default: 90
- Values: Min: 0 / Max: 999999999

registration-caching
Enable or disable registration cache used for all UAs rather than those behind NATs

- Default: disabled
- Values: enabled | disabled

min-reg-expire
Enter the minimum registration expiration time in seconds for HNT registration caching

- Default: 300
- Values: Min: 0 | Max: 999999999

registration-interval
Enter the expiration time in seconds for the Oracle Communications Session Border Controller's cached registration entry for an endpoint (non-HNT)

- Default: 3600
- Values: Min: 1 | Max: 999999999

route-to-registrar
Indicate whether or not the SD should forward a request addressed to the registrar to the SIP registrar as opposed to sending the request to the registered contact in the registration cache

- Default: disabled
- Values: enabled | disabled

secured-network
Enable or disable sending messages on unsecured transport

- Default: disabled
- Values: enabled | disabled

teluri-scheme
Enable or disable the conversion of SIP URIs to Tel URIs

- Default: disabled
- Values: enabled | disabled

uri-fqdn-domain
Change the host part of the URIs to the FQDN value set here. This applies to the Request-URI, From header, and To header in non-dialog requests sent from the SIP interface.

trust-mode
Select the trust mode for this SIP interface

- Default: all

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values:
  - all—Trust all previous and next hops except untrusted session agents
  - agents-only—Trust only trusted session agents
  - realm-prefix—Trust only trusted session agents or address matching realm prefix
  - registered—Trust only trusted session agents or registered endpoints
  - None—Trust nothing

max-nat-interval
Enter the amount of time in seconds that testing should not exceed for adaptive HNT. The system will keep the expires interval at this value.

- Default: 3600
- Values: Min: 0 | Max: 999999999

nat-int-increment
Enter the amount of time in seconds to use as the increment in value in the SIP expires header for adaptive HNT

- Default: 10
- Values: Min: 0 | Max: 999999999

nat-test-increment
Enter the amount of time in seconds that will be added to the test timer for adaptive HNT

- Default: 30
- Values: Min: 0 | Max: 999999999

sip-dynamic-hnt
Enable or disable adaptive HNT

- Default: disabled
- Values: enabled | disabled

tcp-max-nat-interval
Specifies the amount of time in seconds that testing over TCP connections should not exceed for adaptive HNT. The system keeps the expires interval at this value.

- Default: 3600 seconds
- Values: Min: 0 | Max: 999999999

tcp-nat-int-increment
Specifies the amount of time in seconds to use as the increment in value in the SIP expires header for adaptive HNT testing for TCP connections.

Values include:

- Default: 10 seconds
- Values: Min: 0 | Max: 999999999

tcp-nat-test-increment
Specifies the amount of time in seconds that will be added to the test timer for adaptive HNT testing for TCP connections.

Values include:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 30 seconds
- Values: Min: 0 | Max: 999999999

tcp-sip-dynamic-hnt
Enables the system to perform its dynamic hosted NAT traversal feature for connections using TCP as the transport protocol.

Values include:

- Default: disabled
- Values: enabled | disabled

stop-recurse
Enter a list of returned response codes that this SIP interface will watch for in order to stop recursion on the target's or contact's messages

port-map-start
Set the starting port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping.

- Default: 0
- Values: Min: 1025 | Max: 65535

port-map-end
Set the ending port for the range of SIP ports available for SIP port mapping. A value of 0 disables SIP port mapping. This value must be larger than the port-map-start parameter's value.

- Default: 0
- Values: Min: 1025 | Max: 65535

in-manipulationid
Enter the name of the SIP header manipulations configuration to apply to the traffic entering the Oracle Communications Session Border Controller via this SIP interface

out-manipulationid
Enter the name of the SIP header manipulations configuration to apply to the traffic exiting the Oracle Communications Session Border Controller via this SIP interface

manipulation-pattern
Number of seconds after de-registration to kill TCP connection

manipulation-string
Enter the string used in header manipulation rules for this sip-interface.

sip-ims-feature
Enable or disable IMS functionality on this SIP interface

- Default: disabled
- Values: enabled | disabled

subscribe-reg-event
Enables the Oracle Communications Session Border Controller to generate SIP registration events.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

operator-identifier
Set the operator identifier value to be inserted into a P-Charging-Vector header. The direction of the call determines whether this value is inserted into the orig-ioi or the term-ioi parameter in the P-Charging-Vector header. This string value MUST begin with an alpha character.

anonymous-priority
Set the policy priority parameter for this SIP interface. It is used to facilitate emergency sessions from unregistered endpoints. This value is compared against a policy priority parameter in a local policy configuration element.

- Default: none
- Values:
  - none
  - normal
  - non-urgent
  - urgent
  - emergency

max-incoming-conns
Enter the maximum number of TCP/TLS connections for this sip interface

- Default: 0 (disabled)
- Values: Min: 0 / Max: 20000

per-scr-ip-max-incoming-conns
Enter the maximum number of TCP/TLS connections per peer IP address

- Default: 0
- Values: Min: 0 / Max: 20000; setting a value of 0 disables this parameter.

inactive-conn-timeout
Enter the timeout, measured in seconds for idle TCP/TLS connections

- Default: 0
- Values: Min: 0 / Max: 999999999; setting a value of 0 disables the timer.

untrusted-conn-timeout
Enter the timeout time, in seconds, for untrusted endpoints on TCP/TLS connections

- Default: 0
- Values: Min: 0 (disabled) | Max: 999999999

network-id
Set the value that will be inserted into the P-Visited-Network-ID header

ext-policy-server
Enter the name of external policy server used as the CLF for this SIP interface

default-location-string
Set a default location string to insert into P-Access-Network-Info header when the CLF does not return this value

Copyright © 2024, 2026, Oracle and/or its affiliates.

charging-vector-mode
Set the state of P-Charging-Vector header handling

- Default pass
- Values:
  - none—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, not extracting RADIUS information
  - pass—Pass the P-Charging-Vector header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, extracting RADIUS information.
  - delete—Delete the P-Charging-Vector header received in an incoming SIP message before it is forwarded out of the Oracle Communications Session Border Controller
  - insert—Inserts the P-Charging-Vector header in an incoming SIP message that does not contain the P-Charging-Vector header. If the incoming message contains the P-Charging-Vector header, the Oracle Communications Session Border Controller will overwrite the P-Charging-Vector header with its values.
  - delete-and-respond—Removes the P-Charging-Vector from incoming requests for a session and store it. Then the Oracle Communications Session Border Controller inserts it into outbound responses related to that session in a P-Charging-Vector header.
  - conditional-insert—Inserts the P-Charging-Vector header in an incoming SIP message that does not contain the P-Charging-Vector header. If the incoming message contains the P-Charging-Vector header, the Oracle Communications Session Border Controller passes the P-Charging-Vector header untouched as the message is forwarded, extracting RADIUS information.
  - insert-ioi-pass—Inserts the P-Charging-Vector header in an incoming SIP message that does not contain a P-Charging-Vector header. If the incoming message contains the P-Charging-Vector header, the SBC overwrites the ICID values with the self-generated values and Orig/Term IOI would be used as received in incoming SIP message. In case the incoming SIP message doesn't contains the IOI, the egress message would not have any IOIs.

    Typically used to perform IOI management in peering deployments.

> **Note**
>
> Note that the default setting for the **charging-vector-mode** is pass for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes **none**.

charging-function-address-mode
Set the state of P-Charging-Function-Address header handling

- Default: pass
- Values:
  - none—Pass the P-Charging-Function-Address header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, not extracting RADIUS information

Copyright © 2024, 2026, Oracle and/or its affiliates.

- pass—Pass the P-Charging-Function-Address header received in an incoming SIP message untouched as the message is forwarded out of the Oracle Communications Session Border Controller, extracting RADIUS information.
- delete—Delete the P-Charging-Function-Address header received in an incoming SIP message before it is forwarded out of the Oracle Communications Session Border Controller
- insert—Inserts the P-Charging-Function-Address header in an incoming SIP message that does not contain the P-Charging-Function-Address header. If the incoming message contains the P-Charging-Function-Address header, the Oracle Communications Session Border Controller will prepend its configured values to the header.
- insert-reg-cache—To be configured on the SIP interface facing the UE, configures the Oracle Communications Session Border Controller to replace the PCFA with the most recently cached values rather than the ccf-address you set to be static in your configuration. The cached values come from one of the following that the Oracle Communications Session Border Controller has received most recently: request, response, registration, or local configuration.
- delete-and-respond—To be configured on the SIP interface facing the S-CPCF, configures the Oracle Communications Session Border Controller to strip out the latest cached PCFA.
- conditional-insert—Inserts the P-Charging-Function-Address header in an incoming SIP message that does not contain the P-Charging-Vector header. If the incoming message contains the P-Charging-Function-Address header, the Oracle Communications Session Border Controller passes the P-Charging-Function-Address header untouched as the message is forwarded, extracting RADIUS information.

> **Note**
>
> Note that the default setting for the **charging-function-address-mode** is pass for new SIP interface configurations. If you are upgrading and there are pre-existing SIP interfaces in your (upgraded) configuration, the default becomes none.

ccf-address
Set the CCF address value that will be inserted into the P-Charging-Function-Address header

ecf-address
Set the ECF address value that will be inserted into the P-Charging-Function-Address header

term-tgrp-mode
Select the mode for routing for terminating trunk group URIs

- Default: none
- Values:
  - none—Disable routing based on trunk groups
  - iptel—Use trunk group URI routing based on the IPTEL formats
  - egress-uri—Use trunk group URI routing based on the egress URI format

implicit-service-route
Enable or disable the implicit service route behavior

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values:
  - enabled
  - disabled
  - strict

rfc2833-payload
Enter the payload type used by the SIP interface in preferred rfc2833-mode

- Default: 101
- Values: Min: 96 | Max: 127

rfc2833-mode
Choose whether the SIP interface will behave exactly the same way as before and the 2833or UII negotiation will be transparent to the Oracle Communications Session Border Controller, transparent, or whether the sip-interface prefers to use 2833 for DTMF transfer and would signal that in its SDP, preferred. However the final decision depends on the remote endpoint.

- Default: transparent
- Values: transparent | preferred | dual

constraint-name
Enter the name of the constraint being applied to this interface

response-map
Enter the name of the response map being applied to this interface

local-response-map
Enter the name of the local response map being applied to this interface

sec-agree-feature
Determines if sec-agree feature is enabled.

- Default disabled
- Values enabled | disabled

sec-agree-pref
Determines the security protocol preferences used with Sec-agree support

- Default: ipsec3gpp
- Values:
  - ipsec3gpp — support only IMS-AKA protocol
  - tls — support only TLS protocol
  - ipsec3gpp-tls — support both IMS-AKA and TLS, preferred protocol is IMS-AKA
  - tls-ipsec3gpp — support both TLS and IMS-AKA, preferred protocol is TLS

ims-aka-feature
This parameter is unsupported.

enforcement-profile
Enter the name of the enforcement profile associated with this SIP interface

Copyright © 2024, 2026, Oracle and/or its affiliates.

emergency-dscp-profile
Specifies the name of the emergency DSCP profile you want to apply to this sip-interface.

route-unauthorized-calls
Enter the name of the SA or SAG you want to route unauthorized calls

tcp-keepalive
Enable or disable standard keepalive probes to determine whether or not connectivity with a remote peer is lost.

- Default: none
- Values: none | enabled | disabled

add-sdp-invite
Enable or disable this SIP interface inserting an SDP into either an INVITE or a REINVITE

- Default: disabled
- Values:
  - disabled—Do not insert an SDP
  - invite—Insert an SDP in the invite
  - reinvite—Insert an SDP in the reinvite
  - both—Insert an SDP in both the invite and reinvite

add-sdp-profile
Enter a list of one or more media profile configurations you want to use when the Oracle Communications Session Border Controller inserts SDP into incoming INVITEs that have no SDP. The media profile contains media information the Oracle Communications Session Border Controller inserts in outgoing INVITE.

add-sdp-in-msg
Identifies the messages in which to insert SDP offers or answers. The only allowable value is **18xresp**. The default is null (no value).

- Default: null
- Values:
  - 18xresp—For an offerless INVITE that needs preconditions, causes the Oracle Communications Session Border Controller to insert the SDP, as configured in the media profile names listed in **add-sdp-profiles-in-msg**, in the 18x (183) response towards the UE.

add-sdp-profile-in-msg
Identifies a list of media profiles that contain, based on the codec, the SDP to insert in the 18x response when **add-sdp-in-msg** is configured.

sip-profile
Enter the name of the sip-profile to apply to this interface.

sip-isup-profile
Enter the name of the sip-isup-profile to apply to this interface.

tcp-conn-dereg
Number of seconds after de-registration to kill TCP connection.

- Default 0 (disabled)

Copyright © 2024, 2026, Oracle and/or its affiliates.

tunnel-name
Tunnel traffic for load balancer. Traffic sent to/from this interface will be encapsulated in an RFC 2003 compliant tunnel to/from the load balancer usign the associated network-interface's tunnel name.

register-keep-alive
Sets the use of RFC 5626 CRLF Keepalives on this sip interface.

- Default: none
- Values:
  - none—disables this feature
  - always— Keepalive always added to SIP-Via
  - bnat— Keepalive added to SIP-Via when SIP-via and transport addresses do not match (indicates endpoint is behind a NAT)

kpml-interworking
Enables or disables the KPML to RFC2833 interwokring feature.

- Default: disabled
- Values: enabled | disabled

kpmlRFC2833-iwf-on-hairpin
When enabled, specifies that the system supports KPML to RFC2833 interworking for hairpinned calls. This requires that kpml-interworking to also be enabled.

- Default: disabled
- Values: enabled | disabled —When enabled, allows the Oracle Communications Session Border Controller to present the correct digit encapsulation (KPML or RFC2833) when hairpinned back to the original interface.

msrp-delay-egress-bye
Delay egress BYE message.

- Default: disabled
- Values: enabled | disabled

send-380-response
The phrase entered in this parameter is inserted into the <reason> element in the <alternative-service> element in the XML body in the 380 response returned to an endpoint when the call cannot be completed. This is in compliance with GSMA's Voice over LTE specification (IR. 92).

pcscf-restoration
Configure a reason phrase, enclosed in quotes, that will be included in the P-CSCF restoration response, the reason field of a 504 response sent back to the UE.

session-timer-profile
A session-timer-profile name is configured here to apply that session timer profile to this SIP interface.

session-recording-server
A maximum of four names of session-recording-servers, or session-recording-groups, or a combination of both exisiting in the realm associated with the session reporting client. Valid values are alpha-numeric characters. session recording groups are indicated by prepending the groupname with **SRG:**

Copyright © 2024, 2026, Oracle and/or its affiliates.

session-recording-required
Determines whether calls are accepted by the SBC if recording is not available.

- Default: disabled
- Values:
  - enabled—Restricts call sessions from being initiated when a recording server is not available.
  - disabled—Allows call sessions to initiate even if the recording server is not available.

service-tag
Service tag

p-early-media-header
Used to enable P-Early-Media SIP header support.

- Default: Disabled
- Values:
  - disabled—(the default value) disables support
  - add—enables support and allows the SBC/P-CSCF to add the P-Early-Media header to SIP messages.
  - modify—enables support and allows the SBC/P-CSCF to modify or strip the P-Early-Media header in SIP messages.
  - support—adds additional PEM support, including enforcing PEM from trusted sources, preventing system modification of PEM direction, not adding PEM if absent from SIP replies and adding PEM if it is not advertised in the initial INVITE.

p-early-media-direction
Used to specify the supported directionalities. for P-Early-Media header support.

- sendrecv—send and accept early media
- sendonly—send early media
- recvonly—receive early media
- inactive—reject/cancel early media

options
Enter optional features and/or parameters

spl-options
Enter any optional features or parameters
.

diversion-info-mapping-mode
Configure this parameter to specify how the Diversion and History-Info headers map to and interwork on the interface.

- Default none
- Values:
  - none—no conversion applied

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - div2hist—any Diversion headers in the initial INVITEs going out of this SIP interface will be converted to History-iInfo headers before sending
  - force—behavior is the same as **div2hist** when a Diversion header is present in the incoming INVITE if there are no Diversion headers, a History-Info header for the current URI is added in the outgoing INVITE
  - hist2div—any History-Info headers in the initial INVITEs going out of this sip interface will be converted to Diversion headers before sending

atcf-icsi-match
Matches the icsi value for atcf call.

asymmetric-preconditions
Identifies whether to enable preconditions interworking on the interface. Allowable values are **enabled** and **disabled**. The default is **disabled**. You cannot enable asymmetric preconditions unless you have first set the value of **sip-interface > options** to **100rel-interworking**.

- Default: disabled
- Values:
  - enabled—Enables preconditions interworking on the interface.
  - disabled—Disables preconditions interworking on the interface.

asymmetric-preconditions-mode
Identifies, when the value of **asymmetric-preconditions** is **enabled**, whether to send egress INVITEs immediately or to delay them until preconditions have been met. Allowable values are **send-with-delay** and **send-with-nodelay**.

- Default: send-with-nodelay
- Values:
  - send-with-delay—Delays INVITEs on the egress interface until preconditions are met on the ingress interface.
  - send-with-nodelay—Forwards INVITEs to the egress interface immediately, but holds the responses until preconditions are met on the ingress interface.

sm-icsi-match-for-invite
The ICSI URN to match on to increment the session-based messaging counters. For example - urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg

- Default: empty

sm-icsi-match-for-message
The ICSI URN to match on to increment the event-based messaging counters.

- Default: urn:rrn-7:3gpp-service.ims.icsi.oma.cpm.largemsg

s8hr-profile
Enter the name of the S8HR profile to apply to this SIP interface

playback-file
Specifies the name of the media file, stored previously in /code/media, that the system plays when triggered for this sip-interface.

playback-trigger
Specifies when the system triggers the local media playback function.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- 180-force—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message.
- 180-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message that does not include SDP.

npli-profile
Enter the name of the NPLI profile to apply to this SIP interface

hist-to-div-for-cause-380
Determines whether to interwork cause 380 messages within history-Info and Diversion header interworking.

- Default: inherit
- Values:
  - inherit—uses the setting specified in the sip-config.
  - enabled—enables the message interworking.
  - disabled—disables the message interworking.

user-agent
Reserved for use with Microsoft Teams integrations only.

ringback-file
Specifies the name of the media file, stored previously in /code/media, that the system plays when triggered for this realm.

ringback-trigger
Specifies when the system triggers the local media playback function.

- Default: none
- Values:
  - none—The system does not perform local media playback procedures. Based on precedence, however, the system may issue playback based on other element configurations. Local media playback follows the precedence session-agent, realm, then sip-interface.
  - disabled—The system does not perform media playback procedures on this flow, regardless of ensuing configurations.
  - 180-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message that does not include SDP.
  - 180-force—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 180 message.
  - 183—Starts playback to caller when 183 is sent to call originator. The system stops the playback on the final response (either 2xx success or 4xx error). Configure this 183 value on the original INVITE ingress realm/sip-interface/session-agent.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- refer—Starts playback to the referee when it receives a REFER. This trigger operates only if the OCSBC actually terminates and performs the refer operation. If the REFER is via proxy, playback is not a triggered. Playback stops when the refer operation is complete with a final response (200-299 or 400-699). Configure this refer value on the ingress realm/sip-interface/session-agent of the transferred call.
- 183-and-refer—Starts playback when both 183 and refer triggers are activated.183-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 183 message that does not include SDP.
- 183-no-sdp—Defines the trigger by which the system starts local media playback to caller. This parameter causes playback trigger whenever the called leg responds with a 183 message that does not include SDP.
- playback-on-header—Starts or stops playback based on the presence of the P-Acme-Playback header and its definitions.

sti-as
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send AS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mystiGroupName`.

sti-vs
Specifies the name of an sti-server-group name or a space-separated list of sti-server (up to four allowed) to which the SBC shall send VS requests. When configuring a group name, use the prefix `stg:` followed by your group name. For example, `stg:mystiGroupName`.

sti-orig-id
Specifies the UUID v4 to be added to STI-AS requests, if not already present, during STIR/SHAKEN functions.

sti-attest
Specifies the attestation value that is sent in AS request, during STIR/SHAKEN functions. The default is empty

- full-attestation
- partial-attestation
- gateway-attestation

sti-signaling-attest
Enable this parameter to instruct the SBC to use attestation level and origination ID headers from the ingress SIP INVITE in the REST query to the STI-AS, if preferred. When enabled, the Attestation-Info and Origination-ID headers override the configured values, if present. If one of the two requested headers is present, the other value is obtained from configured parameters.

- Default: Disable—The system does not use the attestation value and origId from SIP headers.
- Enable—The system uses the attestation value and origId from SIP headers, when present.

allow-diff2833-clock-rate-mode
Specifies whether and how the SBC can present an SDP answer towards ingress that contains a telephone-event clock rate that is not the same as the audio codec clock rate. When this parameter is disabled, the SBC does not send telephone-event with a different clock rate than audio codec as an answer towards the ingress.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: Disabled
- Values:
  - use-2833-clock-rate—Allow the use of different clock rates and generate RFC2833 packets using the telephone-event clock rate.
  - use-codec-clock-rate—Allow the use of different clock rates and generate RFC2833 packets using the codec clock rate.

fax-continue-session
Retains an ongoing fax call when a refresh or non-refresh REINVITE is received.

- Default : None
- Values:
  - None - If both ingress and egress realms have none value then the fax session/call can get interrupted and terminated on receiving a REINVITE. If one realm is configured with none then the REINVITE can get rejected or the call can switch from fax to voice depending upon the conditions.
  - faxToVoice - If the Oracle Communications Session Border Controller receives a non-refresh REINVITE with non-faxable codec from the UE that initiated the fax call, then the call switches from fax to voice and REINVITE forwards to the other end.
  - faxToVoiceNotAllowed - If the Oracle Communications Session Border Controller receives a non-refresh REINVITE with non-faxable codec from the UE that initiated the fax call, then Oracle Communications Session Border Controller rejects the REINVITE and the fax call/session continues.

Path

sip-interface is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-interface.**

> **Note**
>
> This is a multiple instance configuration element.

sip-interface > sip-ports

The sip-ports subelement indicates the ports on which the SIP proxy or B2BUA will listen for connections.

Parameters

address
Enter the IP address of the host associated with the sip-port entry

An IPV6 address is valid for this parameter.

port
Enter the port number for this sip-port

- Default: 5060
- Values: Min: 1 / Max: 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

transport-protocol
Select the transport protocol associated for this sip-port

- Default: UDP
- Values:
  - TCP
  - UDP
  - TLS
  - SCTP

multi-homed-addrs
Enter one or more IP addresses that are multihomed on this SIP Interface, for use with SCTP. Multiple IP addresses are entered in parentheses, separated by spaces.

tls-profile
Select the type of anonymous connection from session agents allowed.

> **Note**
>
> This parameter is only visible with appropriate licensing.

allow-anonymous
Select the type of anonymous connection from session agents allowed.

- Default: all
- Values:
  - all—Allow all anonymous connections
  - agents-only—Only requests from session agents allowed
  - realm-prefix—Session agents and address matching realm prefix
  - registered—Session agents and registered endpoints (REGISTER allowed from any endpoint)
  - register-prefix—All connects from SAs that match agents-only, realm-prefix, and registered agents

ims-aka-profile
Enter the name value for the IMS-AKA profile configuration to use for a SIP port

Path

sip-ports is a subelement is under the sip-config element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-interface** , and then **sip-ports.**

> **Note**
>
> There must be at least one sip-port entry configured within the sip-config and there can be as many entries as necessary for the sip-port. This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-isup-profile

The sip-isup-profile element allows you to set up a SIP ISUP format interworking. You can apply a configured SIP ISUP profile to a realm, session agent or SIP interface.

Parameters

name
Enter a unique identifier for this SIP ISUP profile. This name is used when you apply the profile to realms, session agents, and SIP interfaces.

isup-version
Specify the ISUP version to which you want to convert.

- Default: ansi-2000
- Values: ansi-2000 | itu-t926 | gr-317 | etsi-356 | spirou

convert-isup-format
Enable or disable this parameter to perform SIP ISUP format version interworking. If this feature is set to disabled, the feature is turned off.

- Default: disabled
- Values: enabled | disabled

iwf-for-183
Enable this parameter to always interwork 183 messages. Set the value to pem-controlled to interwork the 183 if it contains the value sendonly or sendrecv.

- Default: enabled
- Values: enabled | disabled | pem-controlled
- "enabling this will always interwork 183 message. pem-controlled means 183 will be interworked only if 183 contains PEM with value sendonly or sendrecv"

extract-isup-param
Specifies the ISUP parameters within IAM messages to be interworked for SIP-I inbound calls, both SIP-I to SIP and SIP-I to SIP-I. For SIPI outbound calls, both SIP to SIP-I and SIP-I to SIP-I, interworks the in-band announcements parameter in ACM/CPG messages with the P-Early-Media SIP header.

- Default: empty
- Values: generic-number | location-number | user-to-user | calling-party-number | inband announcement

remove-isup-param
Specifies an ISUP parameter to remove from the extract-isup-param list. Execute this function using one value at a time to refine your extract-isup-param list.

- Default: empty
- Values: generic-number | location-number | user-to-user | calling-party-number | inband announcement

country-code
Enter the text string to insert as (?) during native SIP-ISUP interworking and when performing portability interworking.

Copyright © 2024, 2026, Oracle and/or its affiliates.

portability-method
Enable this parameter to exclude interworking of 183 messages to ACMs during SIP to ISUP interworking.

- Default: none
- Values: none | concatenate

Path

sip-isup-profile is an element under the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-isup-profile.

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation

The sip-manipulation feature lets the SBC add, modify, and delete SIP headers and SIP header elements.

Parameters

name
Enter the name of this list of header rules.

header-rules
Access the header-rules subelement.

mime-rules
Access the mime-rules subelement.

mime-isup-rules
Access the mime-isup-rules-rules subelement.

mime-sdp-rules
Access the mime-sdp-rules-rules subelement which is used to configure HMR for SDP bodies.

import
Enter the complete file name, including .gz, of a previously exported sip-manipulation rule.

export
Enter the file name of a SIP manipulation to export configuration information a designated file.

description
Describe what the set of header rules is doing.

Path

The **sip-manipulation** element is under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-manipulation.**

sip-manipulation > header-rules

The header-rules subelement is used to define one action to perform on a given SIP header.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

name
Enter the name of the header to which this rule applies. This name must match a header name.

action
Select the action you want applied to the header specified in the name parameter.

- Default: none
- Values:
  - none—No action taken
  - add —Add a new element, if it does not already exist
  - store — Store the element
  - sip-manip — Specify the sip-manipulation for element
  - replace — Replace the elements
  - find-replace-all - Find and replace all elements with a a new value
  - delete-element — Delete the specified element, if it exists
  - delete-header — Delete the specified header, if it exists
  - log — Log the action if element criteria are met
  - reject — Reject the element if element criteria matches with match-val-type parameter.

match-value
Enter the exact value to be matched. The action you specify is only performed if the header value matches.

msg-type
Select the message type to which this header rule applies

- Default: any
- Values:
  - any—Both Requests and Reply messages
  - request—Request messages only
  - reply— Reply messages only
  - out-of-dialog - Initial request only (dialog creating request)

methods
Enter a list of SIP methods that this header rule applies to. An empty value applies this header rule to all SIP method messages.

- Default: none

element-rules
Access the element rules sub-subelement

header-name
Enter the header name for which the rules need to be applied

Copyright © 2024, 2026, Oracle and/or its affiliates.

comparison-type
Select the comparison type that the match-value uses

- Default: case-sensitive
- Values:
  - case-sensitive
  - case-insensitive
  - pattern-rule
  - refer-case-sensitive
  - refer-case-insensitive
  - boolean

new-value
The new value to be used in add or manipulate actions. To clear the new-value enter an empty string.

Path

header-rules is a subelement under the **sip-manipulation** configuration element, under the **session-router** path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-manipulation** , and then **header-rules.**

sip-manipulation > header-rules > sip-element-rules

The sip-element-rules sub-element is used to define a list of actions to perform on a given SIP header.

Parameters

name
Enter the name of the element to which this rule applies. The name parameter does not apply for the following element types: header-value, uri-user, uri-host, uri-port, uri-header. You still need to enter a dummy value here for tracking purposes.

type
Select the type of element on which to perform the action

- Default: none
- Values:
  - header-value—Full value of the header
  - header-param-name—Header parameter name
  - header-param—Parameter portion of the header
  - uri-display—Display of the SIP URI
  - uri-user—User portion of the SIP URI
  - uri-host—Host portion of the SIP URI
  - uri-port—Port number portion of the SIP URI

Copyright © 2024, 2026, Oracle and/or its affiliates.

- uri-param-name—Name of the SIP URI param
- uri-param—Parameter included in the SIP URI
- uri-header-name—SIP URI header name
- uri-header—Header included in a request constructed from the URI
- uri-user-param—User parameter of the SIP URI
- status-code—Status code of the SIP URI
- reason-phrase—Reason phrase of the SIP URI
- uri-user-only—URI username without the URI user parameters
- uri-phone-number-only—User part of the SIP/TEL URI without the user parameters when the user qualifies for specific BNF

action
Select the action to take to the element specified in the name parameter, if there is a match value

- Default: none
- Values:
  - none—No action taken
  - add —Add a new element, if it does not already exist
  - store — Store the element
  - sip-manip — Specify the sip-manipulation for element
  - replace — Replace the elements
  - find-replace-all - Find and replace all elements with a a new value
  - delete-element — Delete the specified element, if it exists
  - delete-header — Delete the specified header, if it exists
  - log — Log the action if element criteria are met
  - reject — Reject the element if element criteria matches with match-val-type parameter.

match-val-type
Select the type of value that needs to be matched for the action to be performed

- Default: ANY
- Values:
  - ANY— Both IP or FQDN values
  - IP—IP value
  - FQDN—FQDN value

match-value
Enter the value to match against the element value for a manipulation action to be performed

new-value
Enter the explicit value for a new element or replacement value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Use double quotes around string values
- Pre-defined parameters always start with a $. Valid pre-defined parameters are:
  - $ORIGINAL—Original value of the element is used.
  - $LOCAL_IP—Local IP address is used when you receive an inbound address.
  - $REMOTE_IP—Remote IP address is used.
  - $REMOTE_VIA_HOST—Remote VIA host part is used.
  - $TRUNK_GROUP—Trunk group is used.
  - $TRUNK_GROUP_CONTEXT—Trunk group context is used.
- Operators are:

Operator	Description
+	Append the value to the end. For example: "acme"+"packet" generates "acmepacket"
+^	Prepends the value. For example: "acme"+^"packet" generates "packetacme"
-	Subtract at the end. For example: "112311"-"11" generates "1123"
-^	Subtract at the beginning. For example: "112311"-^"11" generates "2311"

parameter-name
Enter the element parameter name for which the rules need to be applied

comparison-type
Select the type of comparison to be used for the match-value

- Default: case-sensitive
- Values: case-insensitive | case-sensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-manipulation** , and then **header-rules** , and then **element-rules.**

Path

element-rules is a sub-subelement under the **header-rules** subelement under the **sip-manipulation** configuration element, under the **session-router** path.

sip-manipulation > mime-isup-rules

The mime-isup-rules configuration allows you to perform HMR operations on SIP ISUP binary bodies.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

name
Enter a unique identifier for this MIME ISUP rule.

content-type
Enter the content type for this MIME rule. This value refers to the specific body part in the SIP message body that is to be manipulated.

isup-spec
Enter the ISUP encoding specification for the ISUP body; this specifies how the Oracle Communications Session Border Controller is to parse the binary body.

- Default: ansi-2000
- Values: ansi-2000 | itu-99 | gr-317 | etsi-356 | spirou

isup-msg-types
Enter the specific ISUP message types (such as IAM and ACM). that the Oracle Communications Session Border Controller uses with the msg-type parameter (which identifies the SIP message) in the matching process. The values of this parameter are a list of numbers rather than enumerated values because of the large number of ISUP message types.

- Values: Min: 0 / Max: 255

msg-type
Enter the SIP message type on which you want the MIME rules to be performed.

- Default: any
- Values: any | request | reply | out-of-dialog

methods
Enter the list of SIP methods to which the MIME rules apply, such as INVITE, ACK, or CANCEL. There is no default for this parameter.

action
Select the type of action you want to be performed.

- Default: none
- Values: none | add | delete | manipulate | store | sip-manip | find-replace-all | reject | log | monitor

comparison-type
Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

Copyright © 2024, 2026, Oracle and/or its affiliates.

new-value
When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.

mime-header-rules
Access the mime-headers subelement.

isup-param-rules
Access the isup-param-rules subelement.

Path

sip-mime-isup-rules is a subelement under the sip-manipulation element. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-manipulation > mime-isup-rules.

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation > mime-isup-rules > mime-header-rules

The mime-header-rules subelement of mime-isup-rules allows you to configure a SIP header manipulation to add an ISUP body to a SIP message.

Parameters

name
Enter a unique identifier for this MIME header rule.

mime-header-name
Enter the value used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | store | sip-manip | replace | find-replace-all | delete | log | monitor | reject

comparison-type
Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

Copyright © 2024, 2026, Oracle and/or its affiliates.

new-value
Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

Path

mime-header-rules is a subelement under the sip-manipulation>mime-isup-rules element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > mime-header-rules.**

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation > mime-isup-rules > isup-param-rules

The isup-parameter-rules element is used to create, manipulate, and store different parameters in the body of ISUP message.

If the action is add, the default value of the Number Qualifier Indicator byte is always 0x06 (the Additional Calling Party number). When a different value is needed, you can replace 0x06 using the table ability of the object type 192[x]. See the "IAM Interworking Support" section in the *ACLI Configuration Guide*.

Parameters

name
Enter a unique identifier for this ISUP parameter rule. This parameter is required and has no default.

type
Using ISUP parameter mapping, enter the ISUP parameters on which you want to perform manipulation. This parameter takes values between 0 and 255, and you must know the correct ISUP mapping value for your entry. The Oracle Communications Session Border Controller calculates the offset and location of this parameter in the body.

> **Note**
>
> The value returned from the body does not identify the type or length, only the parameter value. For example, a parameter-type value of 4 acts on the Called Party Number parameter value.

- Default: 0
- Values: Min: 0 / Max: 255

format
Enter the method for the Oracle Communications Session Border Controller to convert a specific parameter to a string representation of that value.

- Default: hex-ascii

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: raw-binary | hex-ascii | bcd | binary-ascii | ascii-string | number-param

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | store | sip-manip | replace | find-replace-all | delete | log | monitor | reject

comparison-type
Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.

Path

isup-param-rulesis a subelement under the sip-manipulation>mime-isup-rules element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-isup-rules > isup-param-rules.**

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation > mime-rules

The mime-rules configuration element allows you to set parameters in the MIME rules that the Oracle Communications Session Border Controller uses to match against specific SIP methods and message types.

Parameters

name
Enter a unique identifier for this MIME rule.

content-type
Enter the SIP content type for which you want the MIME rules to be applied.

msg-type
Enter the SIP message type on which you want the MIME rules to be performed.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: any
- Values: any | request | reply | out-of-dialog

methods
Enter the list of SIP methods to which the MIME rules apply. There is no default for this parameter.

format
Specifies the encode/decode format for the mime content.

- Default: ascii-string
- Values: ascii-string, hex-ascii, binary-ascii

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | delete | manipulate | store | sip-manip | find-replace-all | reject | log | monitor

comparison-type
Select a method to determine how the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the body part in the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
When the action parameter is set to add or to manipulate, enter the new value that you want to substitute

methods
Enter the list of SIP methods to which the MIME rules apply. There is no default for this parameter.

mime-header-rules
access the mime-headers subelement.

Path

mime-rules is a subelement under the sip-manipulation element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-manipulation > mime-rules > mime-headers

The mime-headers configuration allows you to configure MIME headers, which operate on the specific headers in the match body part of the SIP message.

Parameters

name
Enter a name for this MIME header rule. This parameter is required and has no default.

mime-header-name
Enter the value to be used for comparison with the specific header in the body part of the SIP message. There is no default for this parameter.

action
Choose the type of action you want to be performed.

- Default: none
- Values: add | replace | store | sip-manip | find-replace-all | none

comparison-type
Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
Enter the value to match against the header in the body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

Path

mime-headers is a subelement under the sip-manipulation>mime-rules element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation > mime-rules>mime-headers.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-manipulation > mime-sdp-rules

The mime-sdp-rules configuration allows you to configure HMR for SDP.

Parameters

name
Enter a name for this SDP header rule. This parameter is required and has no default.

msg-type
Select the message type to which this header rule applies

- Default: any
- Values:
  - any—Both Requests and Reply messages
  - request—Request messages only
  - reply— Reply messages only
  - out-of-dialog— Initial request only (dialog creating request)

methods
Enter the list of SIP methods to which the MIME rules apply, such as INVITE, ACK, or CANCEL. There is no default for this parameter.

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | delete | manipulate | store | sip-manip | find-replace-all | reject | log | monitor

comparison-type
Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
When the action parameter is set to**add** or to **manipulate** enter the new value that you want to substitute.

mime-header-rules
See "sip-manipulation mime-isup-rules > mime-header-rules"

sdp-session-rules
list of sdp-session-rules. See "sip-manipulation > mime-sdp-rules > sdp-session-rules"

Copyright © 2024, 2026, Oracle and/or its affiliates.

sdp-media-rules
list of sdp-media-rules. See "sip-manipulation > mime-sdp-rules > sdp-media-rules"

Path

mime-headers is a subelement under the sip-manipulation>mime-rules element. The full path from the topmost ACLI prompt is: **configure terminal > session-router > sip-manipulation >mime-sdp-rules**.

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation > mime-sdp-rules > sdp-session-rules > sdp-line-rules

The sdp-line-rules configuration allows you to configure HMR for SDP.

Parameters

name
Enter a name for this SDP header rule. This parameter is required and has no default.

type
descriptor type specifying which line of the SDP will be manipulated

- Values: a-z

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | store | sip-manip | replace | find-replace-all | delete | log | monitor | reject

comparison-type
Select a method to determine how the header in the body part of the SDP is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
When the action parameter is set to add or to manipulate, enter the new value that you want to substitute

Copyright © 2024, 2026, Oracle and/or its affiliates.

sdp-line-rules
Specifies the list of sdp-line-rules.

move
Position of configuration object to move (optional).

Path

sdp-line-rules is a subelement under the sip-manipulation>mime-sdp-rules > sdp-session-rules (and sdp-media-rules) subelement. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-manipulation > **mime-sdp-rules** , and then **sdp-session-rules** (or sdp-media-rules) > sdp-line-rules.

> **Note**
>
> This is a multiple instance configuration element.

sip-manipulation > mime-sdp-rules > sdp-media-rules

The sdp-media-rules configuration allows you to configure HMR for SDP.

Parameters

name
Enter a name for this SDP header rule. This parameter is required and has no default.

media-type
Enter the media type to manipulate. For example - audio, video etc.

action
Choose the type of action you want to be performed.

- Default: none
- Values: none | add | delete | manipulate | replace | store | sip-manip | find-replace-all | reject | log

comparison-type
Select a method to determine how the header in the body part of the SIP message is compared. This choice dictates how the Oracle Communications Session Border Controller processes the match rules against the SIP header.

- Default: case-sensitive
- Values: case-sensitive | case-insensitive | pattern-rule | refer-case-sensitive | refer-case-insensitive | boolean

match-value
Enter the value to match against the SDP body part of the SIP message. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators.

new-value
When the action parameter is set to add or to manipulate, enter the new value that you want to substitute.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sdp-line-rules
Where you configure the list of SDP line rules. See sip-manipulation mime-sdp-rules sdp-session-rules sdp-line-rules

Path

sdp-media-rulesis a subelement under the sip-manipulation>mime-sdp-rules element. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-manipulation > **mime-sdp-rules** , and then **sdp-media-rules**.

> **Note**
>
> This is a multiple instance configuration element.

sip-monitoring

The **sip-monitoring** element is used to configure the SIP Monitor and Trace feature.

Parameters

match-any-filter
When enabled, causes the system to perform cumulative filter matching.

- Default: disabled
- enabled | disabled

state
Administrative state of the SIP Monitor and Trace feature.

- Default: disabled
- enabled | disabled

short-session-duration
Specifies the maximum session duration (in seconds) to be considered a short session.

- Default: 0
- Min: 0 / Max: 999999999

monitoring-filters
List of configured filter names to be applied on a global basis. Multiple filters can be entered in a comma-separated list with no spaces. You may add or remove configured filters on a one-time basis with the + or - key. You may enter a * as a wildcard to filter all session data.

interesting-events
Enter the **interesting-events** configuration element.

trigger-window
Time in seconds to reach the trigger threshold.

- Default: 30
- Min: 0 / Max: 999999999

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

sip-monitoring is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **session-router**, and then **sip-monitoring.**

sip-monitoring interesting-events

The **interesting-events** element is used to configure the SIP Monitor and Trace feature.

Parameters

type
The interesting event to monitor.

- short-session
- local-rejection

trigger-threshold
Number of interesting events that occur within the trigger-window parameter value for monitoring to commence.

- Default: 0
- Min: 0 / Max: 999999999

trigger-timeout
Time in seconds to reach the trigger threshold.

- Default: 0
- Min: 0 / Max: 999999999

Path

interesting-events is a subelement under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **session-router**, and then **sip-monitoring**, and then **interesting-event.**

sip-nat

The sip-nat element is used for configuring SIP-NAT across realms.

Parameters

realm-id
Enter the name of the external realm. This required realm-id must be unique.

domain-suffix
Enter the domain name suffix of the external realm. This suffix is appended to encoded hostnames that the SIP-NAT function creates. This is a required field.

ext-proxy-address
Enter the IP address of the default next-hop SIP element (a SIP proxy) in the external network. This is a required field. Entries in this field must follow the IP Address Format.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ext-proxy-port
Enter the port number of the default next-hop SIP element (a SIP proxy) in the external network

- Default: 5060
- Values: Min: 1025 / Max: 65535

ext-address
Enter the IP address on the network interface in the external realm. This required entry must follow the IP address format.

home-address
Enter the IP address on the network interface in the home realm. This required entry must follow the IP address format.

home-proxy-address
Enter the IP address for the home proxy (from the perspective of the external realm). An empty home-proxy-address field value signifies that there is no home proxy, and the external address will translate to the address of the Oracle Communications Session Border Controller's SIP proxy. Entries in this field must follow the IP Address Format.

home-proxy-port
Enter the home realm proxy port number

- Default: 0
- Values: Min: 0; 1025 / Max: 65535

route-home-proxy
Enable or disable requests being routed from a given SIP-NAT to the home proxy

- Default: disabled
- Values: enabled | disabled | forced

address-prefix
Enter the address prefix subject to SIP-NAT encoding. This field is used to override the address prefix from the realm config for the purpose of SIP-NAT encoding.

- Default: *
- Values:
  - <IP address>:[/num-bits]
  - *—indicates that the addr-prefix in the realm-config is to be used
  - 0.0.0.0—indicates that addresses NOT matching the address prefix of the home realm should be encoded

tunnel-redirect
Enable or disable certain headers in a 3xx Response message being received and NATed when sent to the initiator of the SIP INVITE message

- Default: disabled
- Values: enabled | disabled

use-url-parameter
Select how SIP headers use the URL parameter (parameter-name) for encoded addresses that the SIP-NAT function creates. A value of none indicates that Oracle Communications Session Border Controller functionality remains unchanged and results in the existing behavior

Copyright © 2024, 2026, Oracle and/or its affiliates.

of the Oracle Communications Session Border Controller. From-to and phone are used for billing issues related to extracting digits from the encoded portion of SIP messages along with the parameter-name field.

- Default: none
- Values:
  - none
  - from-to
  - phone
  - all

parameter-name
Enter the URL parameter name used when constructing messages. This field is used in SIP-NAT encoding addresses that have a use-url-parameter field value of either from-to or all. This field can hold any value, but it should not be a recognized name that another proxy might use.

user-nat-tag
Enter the username prefix used for SIP URLs

- Default: -acme-

host-nat-tag
Enter the hostname prefix used for SIP URLs

- Default: ACME-

headers
Enter the type of SIP headers to be affected by the Oracle Communications Session Border Controller's sip-nat function. The URIs in these headers will be translated and encrypted, and encryption will occur according to the rules of this sip-nat element. Entries in this field must follow this format: <header-name>=<tag>.

- Default: Type headers -d <enter>

The default behavior receives normal SIP-NAT treatment. SIP-NAT header tags for SIP IP address replacement are listed below:

- fqdn-ip-tgt—Replaces the FQDN with the target address
- fqdn-ip-ext—Replaces the FQDN with the SIP-NAT external address
- ip-ip-tgt—Replaces FROM header with target IP address
- ip-ip-ext—Replaces FROM header withSIP-NAT external address

delete-headers
Remove headers from the list of SIP headers configured in the headers field

Path

sip-nat is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-nat.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-profile

The sip-profile configuration element allows you to configure SIP profiles on the Oracle Communications Session Border Controller.

Parameters

name
Enter a unique identifier for this SIP profile. You will need this SIP profile's name when you want to apply this profile to a realm, SIP interface, or SIP session agent

redirection
Set this value to specify the redirection action, including which call forwarding information to include, within the context of SIP Diversion interworking.

- Default: inherit
- Values: inherit | none | isup | diversion | history-info

ingress-conditional-cac-admit
Set this parameter to enabled to use conditional bandwidth CAC for media release on the ingress side of a call. Set this parameter to inherit for the value to be inherited from the realm-config, sip-interface, or sip-interface

- Default: inherit
- Values: enabled | disabled | inherit

egress-conditional-cac-admit
Set this parameter to enabled to use conditional bandwidth CAC for media release on the egress side of a call.

- Default: inherit
- Values: enabled | disabled | inherit

forked-cac-bw
Select the method for the CAC bandwidth to be configured between the forked sessions.

- Default: inherit
- Values:
  - per-session—The CAC bandwidth is configured per forked session
  - shared—The CAC bandwidth is shared across the forked sessions
  - inherit—Inherit value from realm-config or sip-interface

cnam-lookup-server
Enter the name of an **enum-config** to query ENUM servers for CNAM data.

cnam-lookup-dir
Set this parameter to ingress or egress to identify where the system performs a CNAM lookup with repsect to where the call traverses the system.

- Default: egress
- Values: ingress | egress

Copyright © 2024, 2026, Oracle and/or its affiliates.

cnam-unavailable-ptype
Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=p parameter was returned in a CNAM response.

cnam-unavailable-utype
Set this parameter to a string, no more than 15 characters, to indicate that the unavailable=u parameter was returned in a CNAM response.

replace-dialogs
Enables the Oracle Communications Session Border Controller to process messages with the Replaces: header. It also adds the replaces parameter to the to the Supported header in the realms where it is applied. The inherit value falls back to the higher level of configuration precedence.

- Default: inherit
- inherit | enabled | disabled

Path: **sip-profile** is an element of the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sip-profile.

> **Note**
>
> This is a multiple instance configuration element.

sip-q850-map

The sip-q850-map configuration element is used to map SIP response codes to q850 cause codes.

Parameters

entries
Enter the entries configuration subelement

delete
Delete a SIP to q850 mapping. Enter the SIP code.

edit
Edit a response map by number

Path

sip-q850-map is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-q850-map**

sip-q850-map > entries

The entries subelement is used to create the mapping of q850 cause to SIP reason code.

Parameters

q850-cause
Enter the q850 cause code to map to a SIP reason code

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-status
Enter the SIP response code that maps to this q850 cause code

- Values: Min: 100 / Max: 699
- Default: 0

q850-reason
Describe text to accompany the mapped SIP response code

Path

Entries is a subelement under the **sip-q850-map** configuration element, which is located under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-q850-map** , and then **entries**.

sip-recursion-policy

This element defines a sip-recursion policy that is applied to a session agent or session agent group.

Parameters

name
Name for this SIP Recursion Policy. This value will be referenced by individual session agents' or session agent groups' **sip-recursion-policy** parameter.

description
A textual description of this SIP Recursion Policy instance. If the description includes spaces, enclose all words within double quotes.

global-count
The maximum number of recursions to take before terminating recursion and sending the response back to the requester. Entering 0 here disables a maximum recursion counter.

- Default: 0
- Values: Min: 0 / Max: 4294967295

mode
The method of considering subsequent responses from one SIP peer containing identical response codes.

- Default: consecutive
- Values:
  - consecutive - Stops recursion after the response code is received the **attempts** number of times, consecutively.
  - absolute - Stops recursion after the response code is received the **attempts** number of times in total, counting from the first reply.

sip-resp-code-attempts
Typing this parameter accesses the **sip-response-code** subelement.

Path

sip-recursion-policy is an element of the session-router path. The full path from the topmost ACLI prompt is **configure terminal**, and then **session-router**, and then **sip-recursion-policy**

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-recursion-policy > sip-response-code

This subelement is used to configure the number of retries the system should perform for a specific SIP peer's response, as a response code value.

Parameters

response-code
SIP response code number to associate with an attempt number through this configuration element.

- Default: 503
- Range: 300 - 599

attempts
When a message with the above configured response-code is received, this parameter shall be the number of times to direct a request toward a routing target before trying the next target on the routing list. Application of this value is determined by the sip-recursion-policy mode parameter.

- Default: 1
- Range: 1 - 1000

Path

sip-response-code is a subelement of the **sip-recursion-policy** path. The full path from the topmost ACLI prompt is **configure terminal**, and then **session-router**, and then **sip-recursion-policy**, and then **sip-response-code**

sip-response-map

The sip-response-map element establishes SIP response maps associated with the upstream session agent.

Parameters

name
Name of SIP response map

entries
Access the entries subelement

delete
Remove the selected response-map entry

Path

sip-response-map is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-response-map.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sip-response-map > entries

The entries subelement establishes the status code(s) for both received and transmitted messages and the reason phrase(s) of a SIP response map.

Parameters

recv-code
Enter the original SIP response code received

- Values: Min: 100 / Max: 699
- Default: 0

xmit-code
Enter the setting of translated SIP response code transmitted

- Values: Min: 100 / Max: 699
- Default: 0

reason
Enter the setting of translated response comment or reason phrase to send denoted by an entry in quotation marks

method
Enter the SIP method name you want to use for this SIP response map entry

register-response-expires
Enter the time you want to use for the expires time when mapping the SIP method you identified in the method parameter. By default, the expires time is the Retry-After time (if there is one in the response) of the expires value in the Register request (if there is no Retry-After expires time). Any value you configure in this parameter (when not using the defaults) should never exceed the Register request's expires time.

- Values: Min: 0 / Max: 999999999

Path

entries is a subelement of the sip-response-map element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sip-response-map** , and then **entries**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

sipura-profile

The **sipura-profile** element is analogous to existing sdes-profiles or IKE security associations in that all these objects specify materials (certificates, protocol suites, etc.) available in support of cryptographic operations.

Syntax

```
sipura-profile <name | crypto-list | certificate-file-name>
```

Parameters

name
A unique name for this sipura profile.

crypto-list
Cryptographic algorithm for this profile.

- Default: AES_CM_128_HMAC_MD5
- AES_CM_128_HMAC_MD5

certificate-file-name
Required parameter to specify the file name of the minicertificate presented by the SBC in support of Linksys/sipura operations. This file must have been previously installed in the /code/sipura directory. When identifying the file, use the complete file name, to include the file extension, but omit the directory path.

Path

sipura-profile is an element of the media-security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **system**, and then **security**, and then **media-security**, and then **sipura-profile.**

snmp-community

The snmp-community element defines the NMSs from which the Oracle Communications Session Border Controller will accept SNMP requests.

> **Note**
>
> The snmp-community element is not used if the session delivery SNMP agent operates in SNMPv3 mode.

Parameters

community-name
Enter the name of the SNMP community to which a particular NMS belongs. This required entry must follow the Name Format. The community-name field values must be unique.

access-mode
Select the access level for each snmp-community element

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: READ-ONLY
- Values:
  - READ-ONLY—Allows GET requests
  - READ-WRITE—Unsupported

ip-addresses
Enter the IP address(es) for SNMP communities for authentication purposes. Entries must follow the IP Address Format. This parameter can accept IPv4, IPv6, or a combination of the two.

Path

The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **snmp-community.**

> **Note**
>
> This is a multiple instance configuration element.

snmp-address-entry

The **snmp-address-entry** element is used by an SNMPv3 agent to store SNMPv3 target IP addresses to be used in the generation of SNMP trap messages.

Parameters

address-name
Use this required parameter to specify the SNMPv3 manager hostname.
Values:

- Default: none
- <string> that is 1 to 24 characters.

address
Use this required parameter to enter the IP address and optional port number.

- Value: <ip-address:port> of the SNMPv3 target IP address and the optional port number, which is used for sending SNMP trap notifications and is not used in access control. Port 161 is the default port number.

mask
Use this optional parameter to enter a subnetwork (subnet) mask.
Values:

- Default: 255.255.255.255
- <subnet-mask>

Path

snmp-address-entry is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **snmp-address-entry.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

snmp-group-entry

The **snmp-group-entry** element is used by an SNMPv3 agent to create a group of users that belong to a particular security model who can read, write, and add SNMP objects and receive trap notifications.

> **Note**
>
> This element must be configured in order for an SNMPv3 agent to work.

Parameters

name
Use this required parameter to enter the SNMPv3 group name.

- Default: none
- Values: <group-name-string> that is 1 to 24 characters.

mp-model
Use this required parameter to enter the message processing model

- Default: v3
- Values: v2 | v3

security-level
Use this required parameter to enter the security level of the SNMP group.

- Default: authPriv
- Values:
  - **noAuthNoPriv**—This value specifies that the user group is authenticated by a string match of the user name and requires no authorization and no privacy similar to SNMPv1 and SNMPv2. This value is specified with the **sec-model** parameter and its **v1v2** value and can only be used with the **community-string** parameter not specified.
  - **authNoPriv**—This value specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols without privacy.

    > **Note**
    >
    > If the **sec-model** parameter is specified to the **v1v2** value, the **community-string** parameter (not configured) defines a coexistence configuration where SNMP version 1 and 2 messages with the community string from the hosts indicated by the **user-list** parameter and the corresponding **snmp-user-entry** and **snmp-address-entry** elements are accepted.

  - **authPriv**—This default value specifies that the user group is authenticated by using either the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocols and provided privacy by using AES128 authentication. This value is specified with the SNMP **sec-model** parameter and its **v3** value.

Copyright © 2024, 2026, Oracle and/or its affiliates.

community-string
Use this optional parameter to allow the co-existence of multiple SNMP message version types for this security group.

- Value: <community-string> that is 1 to 24 characters.

> **Note**
>
> If a community-string is configured, the **sec-model** parameter value can be only **v1v2**.

user-list
Use this required parameter to configure host names.

- Value: <string> that is 1 to 24 characters and must match the name of the **user-name** parameter of the **snmp-user-entry** element.

> **Note**
>
> This parameter is configured with the **sec-model** and **sec-level** parameters.

If the **user-list** value does not match an existing user name, the **snmp-group-entry** element configuration is invalid when verifying your configuration.

read-view
Use this required parameter to specify a name for the SNMP group's read view for a collection of MIB subtrees.

- Value: <group-read-view-string> that is 1 to 24 characters.

write-view
Use this required parameter to specify a name for the SNMP group's write view for a collection of MIB subtrees.

- Value: <name-token> write view that is 1 to 24 characters.

notify-view
Use this required parameter to specify a name for the SNMP group's notification view for a collection of MIB subtrees.

- Value: <group-notify-view-string> that is 1 to 24 characters.

Path

snmp-view-entry is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **snmp-group-entry.**

snmp-user-entry

The required **snmp-user-entry** element is used to create an identity for one or more SNMPv3 users, their security level, passwords for secure authentication and privacy. This element provides a way to identify a user, protect the user from a different SNMP agent that uses message capture and replay, and protect the user from a network traffic source that uses an incorrect password or security level.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

user-name
Enter the name of the user authorized for retrieving SNMPv3 information.

- Default: **none**
- Values: <user name string> that is 1 to 24 characters.

auth-protocol
Use this required parameter to enter the HMAC-SHA2-256 or HMAC-SHA2-512 authentication protocol.

- Default: **sha512**
- Values: **none** | **sha256** | **sha512**

auth-password
Enter the authorization password for this user. This value is obscured when displayed at the ACLI.

- Default: none
- Values: <password-string> that is 6 to 64 characters.

priv-protocol
Use this required parameter to enter the AES or CBC-DES privacy protocol.

- Default: **aes128**
- Values: **none** | **aes128**

priv-password
Enter the privacy password for this user. This value is obscured when displayed at the ACLI.

- Default: none
- Values: <password-string> that is 6 to 64 characters.

address-list
Enter the required address list name(s) for this user, which must match an **address-name** parameter that you specified when you configured the **snmp-address-entry** element.

- Default: none
- Values: <address-string> that is 1 to 24 characters. You can specify multiple address list names by separating them with a comma.

Path

snmp-community is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **snmp-user-entry.**

> **Note**
>
> This is a multiple instance configuration element.

Copyright © 2024, 2026, Oracle and/or its affiliates.

snmp-view-entry

The **snmp-view-entry** element is used by an SNMPv3 agent to include or exclude access to single or multiple MIB OID nodes for an SNMP view name. An SNMP view is a mapping between SNMP scalar and tabular objects and the access rights available for this SNMP view. Scalar objects define a single object instance and tabular objects define multiple related object instances grouped in MIB tables.

> **Note**
>
> This element must be configured in order for an SNMPv3 agent to work.

Parameters

name
Use this required parameter to enter the SNMP view name.

- Default: none
- Values: <string> that is 1 to 24 characters.

For example:

- view-name AcmeSbcMibView

included-list
Use this required parameter to include access rights for object Identifier (OID) nodes.

- Values: <OID> number separated by a dot (.) in which each subsequent OID (from 0 to 32) is a sub-identifier.

  For example:

  - 1.3.6.1.6
  - (1.3.6.1.2 1.3.6.1.4.1.9148) - You can enter multiple values enclosed in parenthesis and separated by space or comma.

excluded-list
Use this optional parameter to exclude access rights for OID nodes.

- Values: <OID> number separated by a dot (.) in which each subsequent OID (from 0 to 32) is a sub-identifier.

  For example:

  - 1.3.6.1.4.1.9148.3.3
  - (1.3.6.1.4.1.9148.3.3 1.3.6.1.4.1.9148.3.5) - You can enter multiple values enclosed in parenthesis and separated by space or comma.

Path

snmp-view-entry is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **snmp-view-entry.**

Copyright © 2024, 2026, Oracle and/or its affiliates.

spl-config

Parameters

plugins
Use this parameter to enter the plugins path as described next. In the plugins path you will configure local plugin files for use.

spl-options
Enter any optional features or parameters

Path

spl-config is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **spl-config.**

spl-config > plugins

Parameters

name
Enter the SPL package to load. The default location is /code/spl. You may enter a single SPL plugin within a package as follows: SPL_PACKAGE:MODIFY-HEADER

move
Move plugin

Path

spl-config is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **spl-config** , and then **plugins.**

ssh-config

The **ssh-config** element is used to set the attributes of the SSH/SFTP server.

Parameters

rekey-interval
Enter the number of minutes before rekeying an SSH session.

- Default: 60
- Values: Min: 60 / Max: 600

rekey-byte-count
Enter the number of bytes, as a power of 2, to be transmitted before rekeying an SSH session. For example: 31 means 2^31 or 2147483648 bytes.

- Default: 31
- Values: Min: 20 / Max: 31

Copyright © 2024, 2026, Oracle and/or its affiliates.

encr-algorithms
Enter the list of encryption algorthims which the SSH server should offer during session negotiation. Entries may be single values or a comma-separated list in double quotes. The SSH session will use the first algorithm which both the client and server support. The list of supported ciphers are updated per release as weaker ciphers are deprecated and then removed. See the Release Notes for the list of algorithms supported in this release.

- Default: Type ? to see the default algorithms for this release.
- Values: Type ? to see the supported values for this release.

hmac-algorithms
Enter the list of HMAC algorithms which the SSH server should offer during session negotitation. Entries may be single values or a comma-separated list in double quotes. The SSH session will use the first algorithm which both the client and server support. See the Release Notes for the list of algorithms supported in this release.

- Default: Type ? to see the default algorithms for this release.
- Values: Type ? to see the supported values for this release.

hostkey-algorithms
Enter the list of host key algorithms which the SSH server should offer during session negotitation. Entries may be single values or a comma-separated list in double quotes. The SSH session will use the first algorithm which both the client and server support. See the Release Notes for the list of algorithms supported in this release.

- Default: Type ? to see the default algorithms for this release.
- Values: Type ? to see the supported values for this release.

keyex-algorithms
Enter the list of key exchange algorithms which the SSH server should offer during session negotitation. Entries may be single values or a comma-separated list in double quotes. The SSH session will use the first algorithm which both the client and server support. See the Release Notes for the list of algorithms supported in this release.

- Default: Type ? to see the default algorithms for this release.
- Values: Type ? to see the supported values for this release.

proto-neg-time
Enter the number of seconds allocated for SSH session negotiation.

- Default: 60
- Values: Min: 30 / Max: 60

tcp-keep-alive
Enable or disable the TCP keep-alive timer.

- Default: enabled
- Values: enabled | disabled

client-idle-timeout
Enter the number of minutes after which an inactive client will be disconnected. A value of 0 disables the idle client timeout.

- Default: 0
- Values: Min: 0 / Max: 59

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

ssh-config is an element under the security path. The full path from the topmost ACLI prompt is: **configure terminal** , **security** , **ssh-config**.

static-flow

The static-flow element sets preconfigured flows that allow a specific class of traffic to pass through the Oracle Communications Session Border Controller unrestricted.

Parameters

in-realm-id
Enter the ingress realm or interface source of packets to match for static flow translation. This in-realm-id field value must correspond to a valid identifier field entry in a realm-config. This is a required field. Entries in this field must follow the Name Format.

description
Provide a brief description of this static-flow configuration object.

in-source
Enter the incoming source IP address and port of packets to match for static flow translation. IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-source parameter takes the format: `in-source <ip-address>[:<port>]`

- Default: 0.0.0.0
- Values: Port: Min: 0 / Max: 65535

This parameter accepts an IPv6 value.

in-destination
Enter the incoming destination IP address and port of packets to match for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 matches packets received on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The in-destination parameter takes the format: `in-destination <ip-address>[:<port>]`

- Default: 0.0.0.0
- Values: Port: Min: 0 / Max: 65535

This parameter accepts an IPv6 value.

out-realm-id
Enter the egress realm or interface source of packets to match for static flow translation. This out-realm-id field value must be a valid identifier for a configured realm. This required entry must follow the Name Format.

out-source
Enter the outgoing source IP address and port of packets to translate to for static flow translation. IP address of 0.0.0.0 translates to any source address. Port 0 translates to packets sent on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The out-source parameter takes the format: `out-source <ip-address>[:<port>]`

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0.0.0.0
- Values: Port: Min: 0 / Max: 65535

This parameter accepts an IPv6 value.

out-destination
Enter the outgoing destination IP address and port of packets to translate to for static-flow translation. An IP address of 0.0.0.0 matches any source address. Port 0 translates to packets sent on any port. The port value has no impact on system operation if either ICMP or ALL is the selected protocol. The out-destination parameter takes the format: `out-destination <ip-address>[:<port>]`

- Default: 0.0.0.0
- Values: Port: Min: 0 / Max: 65535

This parameter accepts an IPv6 value.

protocol
Select the protocol for this static-flow. The protocol selected must match the protocol in the IP header. The protocol remains the same for the inbound and outbound sides of the packet flow.

- Default: UDP
- Values:
  - UDP—UDP used for this static-flow element
  - TCP—TCP used for this static-flow element
  - ICMP—ICMP used for this static-flow element
  - ALL—Static-flow element can accept flows via any of the available protocols.

alg-type
Select the type of NAT ALG to use

- Default: none
- Values:
  - none—No dynamic ALG functionality
  - NAPT—Configure as NAPT ALG

    Note

    out-source/port range overlapping with other ALG definitions is not allowed and can cause a port overlapping error during configuration verification.

  - TFTP—Configure as TFTP ALG

    Note

    Neither in-destination/port range overlapping or out-source/port range overlapping with other ALG definitions are allowed and can cause a port overlapping error during configuration verification.

average-rate-limit
This parameter is unsupported.

Copyright © 2024, 2026, Oracle and/or its affiliates.

start-port
Enter the internal starting ALG ephemeral port

- Default: 0
- Values: Min: 1025 / Max: 65535

end-port
Enter the internal ending ALG ephemeral port

- Default: 0
- Values: Min: 1025 / Max: 65535

flow-time-limit
Enter the time limit for a flow, measured in seconds

- Values: Min: 0 / Max: 999999999

initial-guard-timer
Enter the initial flow guard timer, measured in seconds

- Values: Min: 0 / Max: 999999999

subsq-guard-timer
Enter the subsequent flow guard timer, measured in seconds

- Values: Min: 0 / Max: 999999999

average-rate-limit
Set the average rate limit of RTP flows.

- Default: 0
- Values: 0 - 125000000

Path

static-flow is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **static-flow.**

> **Note**
>
> This is a multiple instance configuration element.

sti-config

The sti-config object configures server connection control parameters the Oracle Communications Session Border Controller uses to manage STIR/SHAKEN server availability.

Parameters

circuit-breaker-window-duration
Specifies the time in seconds the system uses to establish the window it uses to establish the circuit breakers timing. The default is 10 seconds. The range is from 10 to 30.

circuit-breaker-error-threshold
Specifies the number of errors the system counts before it marks the server as out of service. The default is 5 errors. The range is from 3 to 10.

Copyright © 2024, 2026, Oracle and/or its affiliates.

circuit-breaker-retry-time
Specifies the time in seconds the system uses to retry connecting to the server. The default is 15 seconds. The range is from 5 to 900.

circuit-breaker-half-open-frequency
Specifies the number of times the system skips this server while it is marked half open. The default is 6, which causes the system to re-use the server once every 6th retry. The range is from 5 to 100.

sti-signaling-attest-info-mandatory
When enabled, causes the system to check whether the mandatory headers P-Attestation-Info (or Attestation-Info) header and P-Origination-ID or (Origination-ID) header are present in received INVITE. If either of these headers are missing, the system does not sent an attestation request to the STI server.

- Default: disabled
- Values: enabled | disabled

anonymous-uri-add-verstat-to-hostpart
This parameter determines the system's placement of the verstat parameter when the received INVITE does not contain a P-Asserted-IDentity header, but does contain a Privacy header and an anonymous URI in the FROM. When enabled, the system adds the verstat parameter after the hostpart of the anonymous From URI. When disabled, the system adds the verstat parameter after the user-part of the anonymous From URI.

- Default: disabled
- Values: enabled | disabled

use-identity-header
When enabled in conjunction with STI verification, this parameter causes the SBC to add a Reason header to 18x, 19x responses and 3xx, 4xx, 5xx, 6xx final responses that it sends to a callee with a cause value of “428” and the text “Use Identity Header” for all received INVITEs that did not contain an identity header.

- Default: disabled
- Values: enabled | disabled

check-duplicate-passports
Enables the system to check for duplicate SHAKEN or DIV passports in a received INVITE. If it finds duplicates, the system deletes one of the duplicates from the INVITE.

- Default: disabled
- Values: enabled | disabled

tn-retargeting
Enables the system to perform DIV authentication request, based on the received INVITE.

- Default: disabled
- Values: enabled | disabled

verstat-comparison
To support authentication processes, determines whether and how the system compares the verstat value present in FROM and PAI headers with the values present in this parameter. If a value matches, then the system accepts the validation and performs only DIV authentication processes. If the value is empty, the system does not perform the comparison.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: Empty
- TN-Validation-Passed
- TN-Validation-Passed
- No-TN-Validation
- TN-Validation-Failed

dest-comparison
Specifies whether and on which header the system compares its stored TN with either the Request-URI or the To header in received INVITEs with the {dest} value in the SHAKEN passport. If the value is empty, the system does not perform the comparison.

- Default: Empty
- Request-URI
- To

sti-as-correlation-id
When enabled, the system adds the SipCallId parameter to REST authentication requests to the STI-AS. This parameter contains the information from the corrID parameter in the P-NokiaSiemens.Session-Info SIP header.

Values include:

- Default: disabled
- Values: enabled | disabled

reason-json-sip-translation
When enabled, the system creates a Reason header from the parameters reasoncode and reasontext, if received from the STI-VS. The system also adds this Reason header to the egress INVITE.

sti-header-mapping-ruleset-name
Name of this STI Header Mapping Ruleset you want to use as default across all sti-servers. A ruleset name configured against a sti-server takes precedence for that server over this ruleset.

flip-tn-lookup-order
When enabled, the system prioritizes the FROM header over the PAI header as the source from which it retrieves a TN for use during authentication and verification procedures.

- Default: disabled
- Values: enabled | disabled

sti-response-treatment-config-name
Specifies the name of the sti-response-treatment-config to apply to this sti-config with which the system can attempt to match the contents of each received sti-vs response for the purpose of rejecting the associated call.

max-retry-attempts
The number of attempts the system tries sending a request to a new sti-server within the sti-server-group unless a server responds or sip transaction times out.
Values include:

- Default: 0 (disabled)
- Values: 0 to 30

Copyright © 2024, 2026, Oracle and/or its affiliates.

sti-reason-header-config-name
Name of the STI Reason header config configured under **sti-reason-header-config**.

Path

sti-config is an element under the session-router branch. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-config**.

sti-header-mapping-ruleset

The sti-header-mapping-ruleset element allows you to set up the header mapping feature. You can apply a configured sti-header-mapping-ruleset to sti-server.

Parameters

name
Enter a unique identifier for this sti-header-mapping-ruleset. You use this name when you apply the ruleset to either a sti-server or the sti-config.

mapping-rules
Multi-instance element from which you create rules for manipulating headers within Stir/Shaken traffic.

Path

sti-header-mapping-ruleset is an element under the session-router path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sti-header-mapping-ruleset.

> **Note**
>
> This is a multiple instance configuration element.

sti-header-mapping-ruleset > mapping-rules

The mapping-rules is a multi-instance sub-element that resides within the sti-header-mapping-ruleset. This element allows you to set up the header mapping feature. You can apply a configured sti-header-mapping-ruleset to sti-server.

Parameters

id
Specifies a unique identifier for this mapping-rule.

source-header
Specifies the header within a SIP INVITE that uses Stir/Shaken architecture for validating the call.

target-header
Specifies the header you modify, based on this rule's source-header parameter, within an HTTP request that the system sends to the Stir/Shaken architecture.

Copyright © 2024, 2026, Oracle and/or its affiliates.

source-param
When configured, the system uses this referenced source-param to fetch the mapping details between the SIP header parameter and the HTTP header parameters in the HTTP request/response to or from an STI server.

> **Note**
>
> If the source-header is null and the direction is inbound, the system identifies this value as a key from the key-value pair from the HTTP Body JSON claim.

target-param
When configured, the system uses this referenced target-param to insert the mapping details between the SIP header parameter and the HTTP header parameters present in HTTP request/response to or from an STI server.

direction
Specifies the direction that this rule affects. Outbound causes the system to modify headers traffic to the applicable sti-server. Inbound affects headers from the sti-server.

- Default: outbound
- Values: outbound | inbound

role
Specifies the role, Stir/Shaken authentication or verification, within which this rule applies.

- Default: STI-AS
- Values: STI-AS | STI-VS

Path

mapping-rules is an element under the sti-header-mapping-ruleset path. The full path from the topmost ACLI prompt is: configure terminal > session-router > sti-header-mapping-ruleset > mapping-rules.

> **Note**
>
> This is a multiple instance configuration element.

sti-heartbeat-config

You use the sti-heartbeat-config configuration element to define the operational parameters for the heartbeat that monitors STIR/SHAKEN servers' availability.

Parameters

sti-heartbeat-state
Enables/disables the heartbeat functionality for all STIR/SHAKEN servers at the system level. Values include:

- Disabled (default)
- Enabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

sti-heartbeat-msg-interval-time
Specifies, in seconds, the time-interval to send the heartbeat message to STIR/SHAKEN servers. Values include:

- 5 seconds (default)
- Range 1 - 3600 seconds

> **Note**
>
> The value of this parameter should be more than the timeout value of each sti-server.

sti-orig-tn-number
Specifies the calling party TN number when sending heartbeat messages to STIR/SHAKEN servers, using a string value.

- Default: 9999999999
- Range is any 10 digits

sti-dest-tn-number
Specifies the called party TN number when sending heartbeat messages to STIR/SHAKEN servers, using a string value.

- Default: 7777777777
- Range is any 10 digits

sti-div-tn-number
Specifies the called party diverted TN number when sending heartbeat messages to STIR/SHAKEN servers, using a string value.

- Default: 3333333333
- Range is any 10 digits

Path

sti-heartbeat-config is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-heartbeat-config**.

> **Note**
>
> This is a multiple instance configuration element.

sti-response-treatment-config

You use the sti-response-treatment-config configuration element to create containers for response-treatment-entry sub-elements. These elements also contain the name used to apply the rules to a sti-server or the sti-config.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

name
Specifies the name of this sti-response-treatment-config, which you apply to sti-response-treatment-name parameters in either a sti-server or the sti-config.

sti-response-treatment-entry
Provides access to this sub-element, within which you configure the rules the system uses to match sti-vs response contents for the purpose of rejecting the associated call. If you have configured the system to perform STI verification and the sti-vs response contains an Identity header with reasoncode and reasontext that matches this entry, the system rejects the call.

Path

sti-response-treatment-config is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-response-treatment-config**.

> **Note**
>
> This is a multiple instance configuration element.

sti-response-treatment-config > sti-response-treatment-entry

You use sti-response-treatment-entry sub-elements to define global or specific sti-server rules. The system uses these rules to match the contents of sti-vs responses for the purpose of rejecting the associated call.

Parameters

verstat
Specifies the actionable verstat value returned in the STI-VS response. This field is mandatory. Allowed values include:

- TN-Validation-Passed
- TN-Validation-Failed
- No-TN-Validation
- custom (A value that you define)

reason-code
Specifies the reason code as returned in the STI-VS response. Allowed values include:

- Default: 0
- 403
- 428
- 436
- 437
- 438

Copyright © 2024, 2026, Oracle and/or its affiliates.

- custom (A value that you define within the range of 1xx to 5xx)

role
Specifies the function to which this rule applies. Allowed values include:

- Default: STI-VS

sip-reason-code
Specifies the reason text to match in the JSON response.

- Default: 403
- 403 / 428 / 436 / 437 / 438
- custom (A 3-digit value that you define within the range 4xx to 6xx)

sip-reason-text
Specifies the SIP reason text the system uses to generate the SIP response. Allowed values include:

- Default: Forbidden
- custom (A string that you define)

Path

sti-response-treatment-entry is an element of the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-response-treatment-config**, and then **sti-response-treatment-entry**.

> **Note**
>
> This is a multiple instance configuration element.

sti-server

The sti-server object configures target servers the Oracle Communications Session Border Controller communicates with during STIR/SHAKEN processes.

Parameters

name
Specifies the name of this sti-server configuration. This name can be up to 128 characters and must not begin with a period (.) or a dash (-) character.

description
Specifies a brief description for this sti-server element.

state
Enables or disables the operational state of this sti-server configuration.

- Default: enabled
- Values: enabled | disabled

role
Identify the role of the STIR/SHAKEN server.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: BOTH
- Values: STI-AS | STI-VS | BOTH

http-rest-type
The type of the STIR/SHAKEN implementation.

- Default: ATIS
- Values: 3GPP | ATIS

as-server-root
Specifies the IP Address or FQDN of the STIR verification server, with optional port and base path. Entry format is as a standard URL.

vs-server-root
Specifies the IP Address or FQDN of the STIR authentication server, with optional port and base path. Entry format is as a standard URL.

div-as-server-root
The STI-AS Server root URL for div authentication requests. This attribute accepts a hostname (starting with http:// or https://), an IPv4 address, or an IPv6 address. The port is optional.

div-vs-server-root
The STI-VS Server root URL for div verification requests. This attribute accepts a hostname (starting with http:// or https://), an IPv4 address, or an IPv6 address. The port is optional.

orig-id
This field specifies a UUID v4 to be added to STI-AS requests. Entry format is the standard UUID4 format, as in RFC 4122. You can enter a specific UUID or configure the system to generate a random UUID. The system generates a random UUID if you either:

- Configure the parameter with consecutive quotes ("")
- Configure the parameter with the All-Zero UUID in all interfaces (ACLI, REST, GUI): "00000000-0000-0000-0000-000000000000"

sti-attest
Specifies an attestation value that is sent in AS request. You must enter a value for this field to properly configure the sti-server.

- **A**—Sets the parameter to full-attestation
- **B**—Sets the parameter to partial-attestation
- **C**—Sets the parameter to gateway-attestation

timeout
Specifies amount of time (in milliseconds) to wait for a REST response from a STIR server.

- Default: 2000
- Values: Valid Range: 100-30000

http-client
Specifies the name of a http-client configuration that has information for making connection to the sti-server. This name can be up to 128 characters and must not begin with a period (.) or a dash (-) character

max-burst-rate
Specifies the maximum sending burst rate for STIR requests (per second). Valid values are:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Valid Range: 0-999999999

max-sustain-rate
Specifies the maximum sending sustained rate for STIR requests (per second). Valid values are:

- Default: 0
- Values: Valid Range: 0-999999999

burst-rate-window
Specifies the time period (in seconds) used to calculate burst rate. Valid values are:

- Default: 0
- Values: Valid Range: 0-999999999

sustain-rate-window
Specifies the time period (in seconds) used to calculate sustained rate. Valid values are:

- Default: 0
- Values: Valid Range: 0-999999999

options
Allows the configuration of applicable options to this sti-server.

sti-header-mapping-ruleset-name
Name of the STI ruleset you want to use for this sti-server. This ruleset takes precedence over any ruleset configured in the sti-config.

sti-response-treatment-config-name
Specifies the name of the sti-response-treatment-config to apply to this sti-server with which the system can attempt to match the contents of each received sti-vs response for the purpose of rejecting the associated call.

Path

sti-server is an element under the session-router branch. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-server**.

sti-server-group

The sti-server-group is used for configuring load balancing between servers accessed during STIR/SHAKEN processes on the Oracle Communications Session Border Controller.

Parameters

name
Specifies a name for the sti-server-group. This name can be up to 128 characters and must not begin with a period (.) or a dash (-) character

description
Specifies a brief description for the sti-server-group.

strategy
Specifies a strategy for sti-server selection. The default value is **hunt**. The values `LeastBusy` and `PropDist` are deprecated and not applicable for sti-servers.

Copyright © 2024, 2026, Oracle and/or its affiliates.

The valid values are:

- Hunt
- RoundRobin
- LowSusRate

sti-servers
Specifies the sti-server names that are members of the group. The server names can be specified as a space-separated list enclosed in double quotes. Alternatively, individual sti-server name can be added or removed by prefix the name with a plus (+) or minus (-) character, respectively.

Path

sti-server-group is an element under the session-router branch. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **sti-server-group**.

steering-pool

The steering-pool element defines sets of ports that are used for steering media flows through the Oracle Communications Session Border Controller. The Oracle Communications Session Border Controller can provide packet steering in order to ensure a determined level of quality or routing path.

Parameters

ip-address
Enter the target IP address of the steering pool. This required entry must follow the IP Address Format. The combination of entries in the ip-address, start-port, and realm-id fields must be unique. No two steering-pool elements can have the same entries in the ip-address, start-port, and realm-id fields.

An IPV6 address is valid for this parameter.

start-port
Enter the port number that begins the range of ports available to this steering pool element. This is a required entry. The steering pool will not function properly unless this entry is a valid port.

- Default: 0
- Values: Min: 0 / Max: 65535

end-port
Enter the port number that ends the range of ports available to this steering-pool element. This is a required field. The steering-pool element will not function properly unless this field is a valid port value.

- Default: 0
- Values: Min: 0 / Max: 65535

realm-id
Enter the steering-pool element's realm identifier used to restrict this steering pool to only the flows that originate from this realm. This required entry must be a valid identifier of a realm.

Copyright © 2024, 2026, Oracle and/or its affiliates.

network-interface
Enter the name of network interface this steering pool directs its media toward. A valid value for this parameter must match a configured name parameter in the network-interface configuration element. This parameter applies only to realms with multiple interfaces.

port-allocation-strategy
Select the appropriate strategy for this steering pool based on media type support in this realm. You can create multiple steering pools using different strategies to support multiple media types, per your deployment. Settings include:

- Default: mixed—The system can allocate these ports for any calls
- single— The system only allocates these ports for calls that require a single port
- pair— The system only allocates these ports for calls that require multiple ports

Path

steering-pool is an element under the media-manager path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **media-manager** , and then **steering-pool.**

> **Note**
>
> This is a multiple instance configuration element.

surrogate-agent

The surrogate-agent configuration element allows you to configure the SBC for surrogate registration. This feature lets the SBC explicitly register on behalf of Internet Protocol Branch Exchange (IP-PBX).

Parameters

register-host
Enter the registrar's hostname to be used in the Request-URI of the REGISTER request

register-user
Enter the user portion of the Address of Record

state
Enable or disable this surrogate agent

- Default: enabled
- Values: enabled | disabled

realm-id
Enter the name of the realm where the surrogate agent resides

description
Describe the surrogate agent. This parameter is optional.

customer-host
Enter the domain or IP address of the IP-PBX, which is used to determine whether it is different than the one used by the registrar. This parameter is optional.

Copyright © 2024, 2026, Oracle and/or its affiliates.

customer-next-hop
Enter the next hop to this surrogate agent

> **Note**
>
> Even though the customer-next-hop field allows specification of a SAG or FQDN, the functionality will only support these values if they resolve to a single IP address. Multiple IP addresses, via SAG, NAPTR, SRV, or DNS record lookup, are not allowed.

register-contact-host
Enter the hostname to be used in the Contact-URI sent in the REGISTER request. This should always point to the SBC. If specifying a IP address, use the egress interface's address. If there is a SIP NAT on the registrar's side, use the home address in the SIP NAT.

register-contact-user
Enter the user part of the Contact-URI that the SBC generates

password
Enter the password to be used for this agent

register-expires
Enter the expire time in seconds to be used in the REGISTER

- Default: 600,000 (1 week)
- Values: Min: 0 / Max: 999999999

replace-contact
Specify whether the SBC needs to replace the Contact in the requests coming from the surrogate agent

- Default: disabled
- Values: enabled | disabled

route-to-registrar
Enable or disable requests coming from the surrogate agent being routed to the registrar if they are not explicitly addressed to the SBC

- Default: enabled
- Values: enabled | disabled

aor-count
Enter the number of registrations to do on behalf of this IP-PBX

- Default: 1
- Values: Min: 0 / Max: 999999999

auth-user
Enter the authentication user name you want to use for the surrogate agent

max-register-attempt
Enter the number of times to attempt registration; a 0 value means registration attempts are unlimited

- Default: 3

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 0 / Max: 10

register-retry-time
Enter the amount of time in seconds to wait before reattempting registration

- Default: 300
- Values: Min: 30 / Max: 3600

count-start
Enter the number of registrations to do on behalf of this IP-PBX

- Default: 1
- Values: Min: 0 / Max: 999999999

register-mode
Enter the registration mode.

- Default: automatic
- Values:
  - automatic - Send automatically
  - triggered - Send upon trigger from Private Branch Exchange.

triggered-inactivity-interval
Enter the maximum time in seconds without any traffic from corresponding Private Branch Exchange. This is valid only if registered-mode is triggered.

- Default: 30
- Values: Min: 5 / Max: 300

triggered-oos-response
Specifies the response by the SBC to the Private Branch Exchange on detecting a failure.

- Default: 503
- Values:
  - 503 - Response for core network failure.
  - dropresponse - No response sent to Private Branch Exchange for core network failure.

source-ip-prefix
Can contain a list of IP address/prefixes that specify the source addressing of endpoints for which the system can authenticate calls using this surrogate-agent. Valid entries include any number of IP addresses and IP address prefixes in the format <ip>/<subnet>. If you set multiple values, separate them with a space and enclose them with parenthesis (). Addressing can be IPv4, IPv6 or a combination of both.

- Default: Empty
- Values: List of entries

options
Enter non-standard options or features

Copyright © 2024, 2026, Oracle and/or its affiliates.

un-register
Enable or disable whether the system generates register requests from this surrogate agent that specify Expires:0 and removes each of this surrogate agent's entries from the registration cache.

- Default: Disabled
- Enabled

auth-user-lookup
Enter the name of an auth-user-lookup in a realm's auth-attributes list so that the SBC uses those credentials to authenticate challenged register requests.

- Default: Empty
- string

proxy-name
Enter the name of the session agent you have configured as the Registrar that validates this surrogate agent's register requests for the purpose of routing to that session agent.

- Default: Empty
- string

un-register
Set the de-registration state

- Default: disabled
- Values: enabled | disabled

source-ip-prefix
Enter the list of IP address (with optional prefix) to validate the source IP. Multiple entries should be surrounded with parentheses. For example:

```
ORACLE(surrogate-agent)# source-ip-prefix (172.16.0.9 192.168.4.5/16)
```

Path

surrogate-agent is an element under the session-router path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **session-router** , and then **surrogate-agent.**

system-access-list

The system-access-list configuration element allows you to configure system access control of the management interface on your Oracle Communications Session Border Controller. Once configured, any access from hosts that are not part of the system access IP address or subnet are denied. When this element is not configured, any host can access management ports.

Parameters

source-address
Enter the network source address. An IPv4 or IPv6 address is valid for this parameter.

netmask
Enter the source subnet mask. An IPv4 or IPv6 address is valid for this parameter.

Copyright © 2024, 2026, Oracle and/or its affiliates.

description
Provide a brief description of this system-access-list configuration.

protocol
Enter a specified protocol or the special value all that specifies by protocol the type of management traffic allowed to access the system. The default value (all) matches all supported transport layer protocols.

- Default: all
- Values: all | icmp | ssh | snmp

An alternate means of configuring values supported by this parameter is the format IP protocol/well-known port. For example, the value 6/22 specifies protocol 6 (TCP) targeting port 22 (ssh). In addition, you can specify multiple entries using this format. The example (6/22 1/0 17/162) configures multiple entries.

Path

system-access-list is an element of the system path. The full path from the topmost ACLI prompt is: **configure terminal > system> system-access-list**

system-config

Use the **system-config** element to configure general system information and system parameters.

Parameters

hostname
Enter the main hostname that identifies the SBC. Entries must follow either the Hostname (or FQDN) Format or the IP Address Format.

description
Describe the SBC. Entries must follow the Text Format

location
Enter the physical location of the SBC used for informational purposes. Entries must follow the Text Format.

mib-system-contact
Enter the contact information for this SBC for SNMP purposes. This field value is the value reported for MIB-II when an SNMP GET is issued by the NMS. Entries must follow the Text Format.

mib-system-name
Enter the identification of the SBC for SNMP purposes. This value has no relation to the **system-config > hostname** field. By convention, this is the node's FQDN. If this field remains empty, the SBC name that appears in SNMP communications will be the target name configured in the boot parameters and nothing else.

mib-system-location
Enter the physical location of the SBC for SNMP purposes. This parameter has no direct relation to the location field identified above. Entries must follow the Text Format.

acp-tls-profile
Enter the TLS profile name the system uses to encrypt ACP traffic, to and from the SEM management system.

Copyright © 2024, 2026, Oracle and/or its affiliates.

> **Note**
>
> This parameter is not RTC supported.

disable-garp-out-of-subnet
When enabled, prevents the system from sending out any GARP or ND query for sip-interfaces that are not in the same subnet of each network-interface.

- Default: disabled
- Values: enabled | disabled

This parameter is Real Time Configurable.
This parameter does not apply to the Subscriber Aware Load Balancer (SLB).

snmp-enabled
Enable or disable SNMP is enabled. If SNMP is enabled, then the system will initiate the SNMP agent. If SNMP is disabled, then the SNMP agent will not be initiated, and the trap-receiver and snmp-community elements will not be functional.

- Default: enabled
- Values: enabled | disabled

enable-snmp-auth-traps
Enable or disable the SNMP authentication traps

- Default: disabled
- Values: enabled | disabled

enable-snmp-syslog-notify
Enable or disable sending syslog notifications to an NMS via SNMP; determines whether SNMP traps are sent when a SBC generates a syslog message

- Default: disabled
- Values: enabled | disabled

enable-snmp-monitor-traps
Determine whether traps are sent out in ap-smgmt.mib trap. (See MIB Reference Guide for more information)

- Default: disabled
- Values: enabled | disabled

enable-snmp-tls-srtp-traps
This parameter is reserved for future use. Ensure it remains disabled.

- Default: disabled
- Values: enabled | disabled

enable-env-monitor-traps
Determine whether the environmental monitoring MIB is sent from the SBC. This trap will be sent any time there is a change in state in fan speed, temperature, voltage (SD 2 only), power supply (SD 1 for rev 1.32 or higher, SD 2 w/QoS for rev 1.32 or higher, SD II no QoS for rev 1.3 or higher), phy-card insertion, or I2C bus status. If this parameter is set to enabled, fan speed, temperature, and power supply notifications are not sent out in other traps.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

enable-mblk_tracking
Enabled Mblk tracking.

- Default: disabled
- Values: enabled | disabled

enable-l2-miss-report
When this attribute is disabled, the L2 Miss Report is written to log.octData if the ETC debug level is set to NORMAL. By default, this attribute does not generate a log.

- Default: enabled
- Values: enabled | disabled

peak-concurrent-license
Enables the peak-concurrent-license feature for operation on the system.

- Default: enabled
- Values: enabled | disabled

snmp-syslog-his-table-length
Enter the maximum entries that the SNMP Syslog message table contains. The system will delete the oldest table entry and add the newest entry in the vacated space when the table reaches maximum capacity.

- Default: 1
- Values: Min: 0 / Max: 500

snmp-syslog-level
Set the log severity levels that send syslog notifications to an NMS via SNMP if snmp-syslog-notify is set to enabled. If the severity of the log being written is of equal or greater severity than the snmp-syslog-level value, the log will be written to the SNMP syslog history table. If the severity of the log being written is of equal or greater severity than the snmp-syslog-level field value and if enabled-snmp-syslog-notify field is set to enabled, the system will send the syslog message to an NMS via SNMP. If the severity of the log being written is of lesser severity than the snmp-syslog-level value, then the log will not be written to the SNMP syslog history table and it will be disregarded.

- Default: warning
- Values:
  - emergency
  - critical
  - major
  - minor
  - warning
  - notice
  - info

Copyright © 2024, 2026, Oracle and/or its affiliates.

  - trace
  - debug
  - detail

syslog-servers
Access the syslog-servers subelement

system-log-level
Set the system-wide log severity levels to write to the system log. When you set log levels through system-config, the settings take effect only after you Save and Activate and the settings will persist through a reboot.

> **Note**
>
> For some threads, such as **anthqueue**, **sshd**, and **tLFMiBd**, the log level is set when they are created at startup. Changing **system-log-level** will not change their log level until the system is rebooted.

- Default: warning
- Values:
  - emergency
  - critical
  - major
  - minor
  - warning
  - notice
  - info
  - trace
  - debug
  - detail

process-log-level
Set the default log level that processes running on the SBC start. When you set log levels through system-config, the settings take effect only after you Save and Activate and the settings will persist through a reboot.

> **Note**
>
> For some threads, such as **anthqueue**, **sshd**, and **tLFMiBd**, the log level is set when they are created at startup. Changing **process-log-level** will not change their log level until the system is rebooted.

- Default: notice
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- emergency
- critical
- major
- minor
- warning
- notice
- info
- trace
- debug
- detail

process-log-ip-address
Enter the IP address of server where process log files are stored. Entries must follow the IP Address Format. The default value of 0.0.0.0 causes log messages to be written to the local log file.

- Default: 0.0.0.0

process-log-port
Enter the port number associated with server IP address where process log files are stored. The default value of 0 writes log messages to the local log file.

- Default: 0
- Values: Min: 0; 1025 / Max: 65535

collect
Accesses the collect subelement.

schedule-backup
Accesses the schedule-backup subelement.

comm-monitor
Access the comm-monitor subelement.

call-trace
Enable or disable protocol message tracing for sipmsg.log for SIP

- Default: disabled
- Values: enabled | disabled

internal-trace
Enable or disable internal ACP message tracing for all processes

- Default: disabled
- Values: enabled | disabled

log-filter
Set to logs or all to send the logs to the log server

- Default: all
- Values:

Copyright © 2024, 2026, Oracle and/or its affiliates.

- none
- traces
- traces-fork
- logs
- log-fork
- all
- all-fork

default-gateway
Enter the IP address of the gateway to use when IP traffic sent by the SBC is destined for a network other than one of the LANs on which the 10/100 Ethernet interfaces could be. Entries must follow the IP Address Format. A value of 0.0.0.0 indicates there is no default gateway.

- Default: 0.0.0.0

fault-recovery
Enable or disable a clean reboot of the SBC when a fatal hardware fault is detected. This recovery mechanism is limited to the Acme Packet 4600.

restart
Enable or disable the SBC rebooting when a task is suspended. When set to enabled, this field causes the SBC to reboot automatically when it detects a suspended task. When this field is set to disabled and a task is suspended, the SBC does not reboot.

- Default: enabled
- Values: enabled | disabled

exceptions
Select system tasks that have no impact on system health or cause the system to restart. This field contains the name(s) of the task(s) surrounded by quotation marks. If there are multiple entries, they should be listed within quotation marks, with each entry separated by a <Space>.

telnet-timeout
Enter the time in seconds the SBC waits when there is no Telnet activity before an administrative telnet session, or SSH connection, is terminated. A value of 0 disables this functionality, meaning no time-out is being enforced.

- Default: 0
- Values: Min: 0 / Max: 65535

> **Note**
>
> This parameter is deprecated. Any value set here is ignored.

console-timeout
Enter the time in seconds the SBC waits when there is no activity on an ACLI administrative session before it terminates the session. The ACLI returns to the User Access Verification login sequence after it terminates a console session. A value of 0 disables this functionality.

- Default: 0
- Values: Min: 0 / Max: 65535

Copyright © 2024, 2026, Oracle and/or its affiliates.

http-timeout
Inactivity timeout in minutes for HTTP connections.

- Default: 5
- Values: 0 - 20

reserved-nsep-session-capacity
Sets the percentage value for the amount of NSEP sessions the system reserves from the pool of total session capacity for use by NSEP calls. The system monitors the remaining, general pool of sessions (total minus reserved NSEP) and serves NSEP calls from this reserved session pool if the number of sessions in the general pool becomes exhausted.

- Default: 0
- Values: 0 - 100

remote-control
Enable or disable listening for remote ACP config and control messages before disconnecting

- Default: enabled
- Values: enabled | disabled

alarm-threshold
Access the alarm-threshold subelement.

cli-audit-trail
Enable or disable the ACLI command audit trail. The cli-audit-trail outputs to cli.audit.log.

- Default: enabled
- Values: enabled | disabled

source-routing
This parameter / feature has been deprecated.

cli-more
Enable this parameter to have the ACLI “more” paging feature working consistently across console or SSH sessions with the SBC. When this parameter is disabled, you must continue to set this feature on a per session basis.

- Default: disabled
- Values: enabled | disabled

terminal-height
Set the SBC terminal height when the more prompt option is enable

- Default: 24
- Values: Minimum: 5 / Maximum: 1000

debug-timeout
Enter the time, in seconds, you want to the SBC to timeout log levels for system processes set to debug using the ACLI notify and debug commands. A value of 0 disables this parameter.

- Default: 0
- Values: Min: 0 / Max: 65535

trap-event-lifetime
Set this parameter to the number of days you want to keep the information in the alarm synchronization table; 0 turns alarm synchronization off

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0
- Values: Min: 0 / Max: 7

ids-syslog-facility
Enter a syslog facility, as entered in the syslog-config configuration element, facility parameter to send IDS-type syslog messages to that syslog server. The default value of -1 disables selective message transfer.

- Default: -1

ecc-chk-pkt
Enable ECC packet checks.

- Default: disabled
- Values: enabled | disabled

options
Enter any customer-specific features and/or parameters for this global system configuration. This parameter is optional.

default-v6-gateway
Set the IPv6 default gateway for this SBC. This is the IPv6 egress gateway for traffic without an explicit destination. The application of your SBC determines the configuration of this parameter.

An IPV6 address is valid for this parameter.

ipv6-signaling-mtu
This sets the system-wide, default IPv6 MTU size.

- Default: 1500
- Values: 1280-4096

ipv4-signaling-mtu
This sets the system-wide, default IPv4 MTU size.

- Default: 1500
- Values: 576-4096

cleanup-time-of-day
Enter the local time the SBC begins inspecting directories to perform the clean up process. directory-cleanup—Enters the directory-cleanup subelement.

- Default: 00:00

directory-cleanup
Access the directory-cleanup subelement.

snmp-engine-id-suffix
Sets a unique suffix for the SNMPEngineID. This value is entered as a string.

snmp-agent-mode
Determines which version of SNMP is supported on this system.

- Default: v3
- Values: v1v2 | v3

Copyright © 2024, 2026, Oracle and/or its affiliates.

snmp-rate-limit
Specifies the maximum number of SNMP packets per second the system accepts.

- Default: 0 (no rate limiting)
- Values: 0 - 9999

forwarding-cores
Specifies the number of CPUs to use for traffic forwarding.
The available cores depend on your system.

- Default: 1
- Values: 1 - 128

dos-cores
Specifies the number of CPUs to use for DoS processing.
The available cores depend on your system.

- Default: 0
- Values: 0 - 1

transcoding-cores
Specifies the number of CPUs to use to perform transcoding processes.
The available cores depend on your system.

- Default: 0
- Values: 0 - 128

use-sibling-core-datapath
Enables or disables the use of hyperthreading on your hypervisor.

- Default: disabled
- Values: enabled | disabled

httpclient-max-total-conn
The total number of TCP connections allowed by HTTP clients. Set to 0 to disable a limit.

- Default: 500
- Values: 0 - 2147483647

httpclient-max-cpu-load
The maximum CPU percentage for HTTP clients.

- Default: 70
- Values: 30 - 90

httpclient-cache-size-multiplier
Specifies the multiplier used to calculate the size of the HTTP client connection cache. The system calculates this cache size using the formula:
client connection cache = (number of pending transactions * httpclient-cache-size-multiplier)

- Default: 16
- Values: 4 - 50

http-clearDead-conn-timer
Specifies the number of seconds the system waits before it closes connections to HTTP servers that are in the half closed state.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: 0 (disabled)
- Values: 300 - 84600

resource-monitoring
Enable or disable the Resource Monitor. The Resource Monitor is configured in the **resource-monitor-profile** element under **system**.

- Default: disabled
- Values: enabled | disabled

Path

system-config is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **system-config.**

> **Note**
>
> Under the system-config element, options are not RTC supported. This is a single instance configuration element.

system-config > alarm-threshold

The alarm-threshold configuration element allows you to configure custom alarms for certain system conditions based on those conditions reaching defined operating levels.

Parameters

type
The type of custom alarm-threshold this object creates. Values:

- cpu — Alarm based on CPU usage
- space — Alarm based on used space on an identified disk volume
- memory — Alarm based on memory usage
- sessions — Alarm based on percentage of licensed sessions in use
- rfactor — unused
- deny-allocation — Alarm based on remaining number of reserved deny entries
- cpu-sipd — Alarm based on CPU used for sip process
- cpu-atcpd — Alarm based on CPU used for atcpd process
- cpu-mbcd — Alarm based on CPU used for mbcd
- cpu-datapath — Alarm based on CPU used for forwarding cores
- memory-datapath — Alarm based on datapath memory usage (mbuf)
- reserved-nsep-sessions — Alarm based on percentage of sessions set aside for NSEP sessions

volume
Identifies the disk volume that this alarm threshold monitors. This parameter is only configured when the type parameter is set to space.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Values for the volume parameter include active volume names on your system, such as "opt" and "boot".

severity
The system severity of this alarm.

- Default: minor
- Values: major | minor | critical

value
The percentage usage of the resource identified in the type parameter that triggers this alarm.

- Default: 0
- Values: 1 - 100

> **Note**
>
> When type is set to cpu-datapath or memory-datapath, you must set this to a number greater than 30.

Path

alarm-threshold is a subelement of the **system-config** element. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > alarm-threshold**

system-config > collect

The collect configuration element allows you to configure general collection commands for data collection on the Oracle Communications Session Border Controller.

Parameters

sample-interval
Enter the data collection sampling interval, in minutes

- Default: 5
- Values: Min: 1 / Max: 120

push-interval
Enter the data collecting push interval, in minutes

- Default: 15
- Values: Min: 0 / Max: 120

start-time
Enter the date and time to start data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m-minutes; s=seconds)

- Default: now

end-time
Enter the date and time to stop data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hours; m-minutes; s=seconds)

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: never

boot-state
Enable or disable group collection on reboot

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported

red-collect-state
Enable or disable HA support for the collection function

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

red-max-trans
Enter the maximum number of redundancy sync transactions to keep on active

- Default: 1000
- Values: Min: 0 / Max: 50000

red-sync-start-time
Enter the time to start redundancy sync timeout, in milliseconds.

- Default: 5000
- Values: Min: 0 / Max: 999999999

red-sync-comp-time
Enter the time to complete a redundancy sync, in milliseconds

- Default: 1000
- Values: Min: 0 / Max: 999999999

push-receiver
Access the push-receiver subelement

group-settings
Access the group-settings subelement

push-success-trap-state
Enable this parameter if you want the Oracle Communications Session Border Controller to send a trap confirming successful data pushes to HDR servers.

- Default: disabled
- Values: enabled | disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

Constraints

This element is not visible if the product is set to Subscriber-Aware Load Balancer.

Path

The **collect** is a subelement of the **system-config** element.

```
ORACLE# conf term
ORACLE(configure)# system
ORACLE(system)# system-config
ORACLE(system-config)# collect
ORACLE(collect)#
```

system-config > collect > push-receiver

The push-receiver configuration subelement allows you to configure the Oracle Communications Session Border Controller to push collected data to a specified node.

Parameters

address
Enter the hostname or IP address to which the Oracle Communications Session Border Controller pushes collected data

user-name
Enter the hostname or IP address to which the Oracle Communications Session Border Controller pushes collected data

password
Enter the login password for the specified server used when pushing collected data

data-store
Enter the absolute path on the specified server in which to put collected data

protocol
Set the protocol with which to send HDR collection record files.

- Default FTP
- Values FTP | SFTP

Path

push-receiver is a subelement of the **system-config>collect** subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect >** push-receiver.

system-config > collect > group-settings

The group-settings subelement allows you to configure and modify collection parameters for specific groups.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

group-name
Enter the name of the object the configuration parameters are for. There can only be one object per group.

- Values:
  - system
  - interface
  - session-agent
  - session-realm
  - voltage
  - fan
  - temperature
  - sip-sessions
  - sip-ACL-oper
  - sip-ACL-status
  - sip-client
  - sip-server
  - sip-policy
  - sip-errors
  - sip-status
  - sip-invites
  - sip-rate
  - sip-rate-per-inf
  - sip-rate-per-agent
  - sip-srvcc (Only supported for enterprise products)
  - sip-codec-per-realm
  - enum-stats
  - enum-rate
  - enum-rate-per-name
  - enum-rate-per-addr
  - dnsalg-rate
  - dnsalg-rate-per-realm
  - dnsalg-rate-per-addr
  - h323-stats
  - ike-stats

Copyright © 2024, 2026, Oracle and/or its affiliates.

- radius-stats
- diameter-stats
- msrp-stats
- dos-threshold-counters
- stir-stats
- stir-stats-session-agent
- stir-stats-sip-interface
- stir-stats-realm
- stir-stats-system
- network-util
- space
- registration-realm
- thread-usage
- thread-event
- survivability-sip-errors (Only supported for enterprise products)
- survivability-sip-status (Only supported for enterprise products)
- survivability-sip-invites (Only supported for enterprise products)
- survivability-sip-registration (Only supported for enterprise products)
- sobjects
- ext-rx-policy-server
- sa-ike
- sa-imsaka (Only supported for enterprise products)
- sa-srtp
- xcode-session-gen-info
- xcode-codec-util
- xcode-tcm-util
- sip-method
- sip-realm-method
- sip-interface-method
- sip-agent-method
- latest-peak-license-usage
- sip-invites-detail

sample-interval
Enter the group data collection sampling interval, in minutes

- Default: 5
- Values: Min: 1 / Max: 120

Copyright © 2024, 2026, Oracle and/or its affiliates.

start-time
Enter the date and time to start group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hour; m=minute; s=second)

- Default: now
- Values:
  - now - Start data collection now.
  - <date&time> - Date and time to start data collection.

end-time
Enter the date and time to stop group data collection. Enter in the form of: yyyy-mm-dd-hh:mm:ss (y=year; m=month; d=day; h=hour; m=minute; s=second)

- Default: never
- Values:
  - never - Never end data collection .
  - <date&time> - Date and time to end data collection.

boot-state
Enable or disable data collection for this group.

- Default: disabled
- Values: enabled | disabled

Path

group-settings is a subelement of the **configure terminal > system > system-config > collect >** subelement. The full path from the topmost ACLI prompt is: **configure terminal > system > system-config > collect > group-settings**

system-config > syslog-servers

The syslog-servers subelement configures multiple syslog servers.

Parameters

address
Enter the syslog server's IPv4 address.

port
Enter the port number on the syslog server that the Oracle Communications Session Border Controller sends log

- Default 514

facility
Enter the user-defined facility value sent in every syslog message from the Oracle Communications Session Border Controller to the syslog server. This value must conform to IETF RFC 3164.

- Default 4

Copyright © 2024, 2026, Oracle and/or its affiliates.

Path

syslog-servers is a subelement under the system-config element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **system-config** , and then **syslog-servers.**

> **Note**
>
> We recommend configuring no more than 8 syslog-config subelements.
> This is a multiple instance configuration subelement.

system-config > directory-cleanup

This element is unsupported.

Path

directory-cleanup is a subelement under the **system-config** element. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **system-config** , and then **directory-cleanup.**

tcp-media-profile

The **tcp-media-profile** configuration element allows you to enter individual tcp media profile entry elements. These are used for MSRP functionality.

Parameters

name
Set the name of this tcp media profile.

profile-list
Enter individual tcp media profiles.

Path

tcp-media-profile is an element of the media-manager path. The full path from the topmost ACLI prompt is:**configure terminal**, and then **media-manager**, and then **tcp-media-profile**.

tcp-media-profile > profile-list

The **profile-list** or **profile-entry** configuration element allows you to enter individual tcp media profile entry elements. These are used for MSRP functionality.

Parameters

media-type
A string used to match with the media type <media> in the SDP message's media description (m=). For example: "message" for MSRP.

- Default: message

Copyright © 2024, 2026, Oracle and/or its affiliates.

transport-protocol
The string used to match with the transport protocol <proto> in the media description (m=). For example: "TCP/TLS" for MSRP over TCP/TLS.

listen-port
The listening port on which the system listens for incoming connections to establish a TCP connection for a media session. If the value of this field is 0, the listening port will be chosen automatically by the system from the steering pool of the realm (which the tcp-media-profile belongs to).

- Default: 0
- Values: 0-65535

prefered-setup-role
The value used by the system for the a=setup attribute when negotiating the setup role, regardless of whether the Oracle Communications Session Border Controller is an offer or answer in the SDP offer/answer exchange.

- Default: passive
- Values: active | passive | actpass

require-fingerprint
If transport-protocol is TCP/TLS/MSRP, use the require-fingerprint parameter to enable or disable endpoint authentication using the certificate fingerprint methodology defined in RFC 4572. This parameter can be ignored if transport-protocol is TCP/MSRP.

- Default: disabled
- Values: enabled | disabled

msrp-cema-support
Enable or disable the system to negotiate Connection Establishment for Media Anchoring (CEMA) support with parties in a given realm.

- Default: disabled
- Values: enabled | disabled

msrp-sessmatch
Enable or disable whether or not the URI comparison of the To-Path header in the MSRP messages received from the respective realm includes the authority part.

- Default: disabled
- Values: enabled | disabled

msrp-message-size-enforce
Set to enable or disable the system to reject of messages that exceed the negotiated maximum size or to stop file transfers that exceed the maximum negotiated size.

- Default: disabled
- Values: enabled | disabled

msrp-message-size
Set the maximum size negotiated for the MSRP messages.

- Default: 0 (no size limit enforced)
- Values: 0 - 4194304

Copyright © 2024, 2026, Oracle and/or its affiliates.

msrp-message-size-file
Set the maximum size negotiated for the MSRP file transfer.

- Default: 0 (no size limit enforced)
- Values: 0 - 4294967295.

msrp-types-allowlist
Use to set a list of media types and sub-types that you want the system to accept. You can leave the parameter empty or you can set one or more entries. Each entry represents one media type and sub-type. When the parameter contains a valid value, the system checks that incoming MSRP SEND requests contain only the media types specified in the SDP a=accept-types attribute resulting from applying R5725_0220 to intersect the request and the allowlist. Leave the **msrp-types-allowlist** parameter empty to tell the system not to perform any media types filtering.

- Default: empty
- Values: empty | MsrpMediaTypeList | * (star indicates that all MSRP media types or subtypes are allowed)

Path

tcp-media-profile-entry is a subelement of **tcp-media-profile**. The full path from the topmost ACLI prompt is:**configure terminal**, and then **media-manager**, and then **tcp-media-profile**, and then **tcp-media-profile-entry**.

tdm-config

Use the **tdm-config** configuration element to enable and configure Time Division Multiplexing.

Constraints

Only platforms with Digium cards running the E-SBC support **tdm-config**.

Path

The **tdm-config** configuration element is in the **system** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# tdm-config
ORACLE(tdm-config)#
```

Parameters

The **tdm-config** configuration element contains the following parameters:

state
Enable or disable TDM.

- Default: enabled
- Values: enabled | disabled

logging
Enable or disable TDM logging.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

line-mode
(platforms with Digium PRI cards)
Set either T1 or E1.

- Default: t1
- Values: t1 | e1

line-mode
(platforms with Digium BRI cards)
Set either T1 or E1.

- Default: bri
- Values: bri

line-mode
(platforms with Digium analog cards)
Set either T1 or E1.

- Default: analog
- Values: analog

tone-zone
(platforms with Digium PRI cards)
Set the tone zone value according to the line mode that you specified for this configuration.

- Default: us
- Values: us | us-old | au | fr | nl | uk | fi | es | jp | no | at | nz | it | gr | tw | se | be | sq | il | br | hu | lt | pl | za | pt | ee | mx | in | de | ch | dk | cz | cn | ar | my | th | bg | ve | ph | ru | pa | mo | cr | ae

For T1, use US; for E1, use ES.

tone-zone
(platforms with Digium BRI cards)
Set the tone zone value according to the line mode that you specified for this configuration.

- Default: es
- Values: us | us-old | au | fr | nl | uk | fi | es | jp | no | at | nz | it | gr | tw | se | be | sq | il | br | hu | lt | pl | za | pt | ee | mx | in | de | ch | dk | cz | cn | ar | my | th | bg | ve | ph | ru | pa | mo | cr | ae

For T1, use US; for E1, use ES.

tone-zone
(platforms with Digium analog cards)
Set the tone zone value according to the line mode that you specified for this configuration.

- Default: us
- Values: us | us-old | au | fr | nl | uk | fi | es | jp | no | at | nz | it | gr | tw | se | be | sq | il | br | hu | lt | pl | za | pt | ee | mx | in | de | ch | dk | cz | cn | ar | my | th | bg | ve | ph | ru | pa | mo | cr | ae

For T1, use US; for E1, use ES.

Copyright © 2024, 2026, Oracle and/or its affiliates.

calling-Pres
(platforms with Digium PRI cards or Digium BRI cards)
Enable or disable call IP presentation for a SIP device.

- Default: allowed_not_screened
- Values: allowed | allowed_not_screened | allowed_passed_screen | allowed_failed_screen | prohib | prohib_not_screened | prohib_passed_screen | prohib_failed_screen | unavailable

When you set a value for **calling-pres**, you must also set a value for **caller-ID**.

caller-ID
Enable or disable caller ID for CLIP and COLP.

- Default: no
- Values: no | rpid | pai

When you set a value for **caller-ID**, you must also set a value for **calling-pres**.

tdm-profile
(platforms with Digium PRI cards or Digium BRI cards)
Access the **tdm-profile** configuration element.

fxo-profile
(platforms with Digium analog cards)
Access the **fxo-profile** configuration element.

fxs-profile
(platforms with Digium analog cards)
Access the **fxs-profile** configuration element.

tdm-profile

Use **tdm-profile** to specify one or more profiles for Time Division Multiplexing (TDM) behavior on the SBC. The single-port TDM card supports only one profile, while the quad-port TDM card supports up to four TDM profiles.

Constraints

Only platforms with Digium PRI cards or Digium BRI cards support **tdm-profile**.

Path

The **tdm-profile** configuration element is in the **tdm-config** element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# tdm-config
ORACLE(tdm-config)# tdm-profile
ORACLE(tdm-profile)#
```

Parameters

The **tdm-profile** configuration element contains the following parameters:

name
Set the name for this TDM profile.

Copyright © 2024, 2026, Oracle and/or its affiliates.

signalling
(platforms with Digium PRI cards)
Set the timing source for the TDM card.

- Default: pri_cpe
- Values: pri_cpe | pri_net
- bri_net—the TDM card uses the internal clock as the timing source.
- bri_cpe—the TDM card uses an external clock as the timing source.

signalling
(platforms with Digium BRI cards)
Set the timing source for the TDM card.

- Default: bri_cpe
- Values: bri_cpe | bri_net
- bri_net—the TDM card uses the internal clock as the timing source.
- bri_cpe—the TDM card uses an external clock as the timing source.

switch-type
(platforms with Digium PRI cards)
Set a switch type for this configuration.

- Default: national
- Values: national | dms100 | 4ess | 5ess | euroisdn | ni1 | qsig

switch-type
(platforms with Digium BRI cards)
Set a switch type for this configuration.

- Default: euroisdn
- Values: euroisdn

b-channel
(platforms with Digium PRI cards)
Set the B channel value according to the line mode specified for this configuration.

- Default: 1-23
- Values: 1-23 | 1-15,17-31
- For T1, select 1-23.
- For E1, select 1-15,17-31.

b-channel
(platforms with Digium BRI cards)
Set the B channel value according to the line mode specified for this configuration.

- Default: 1-2
- Values: 1-2
- For T1, select 1-23.
- For E1, select 1-15,17-31.

d-channel
(platforms with Digium PRI cards)

Copyright © 2024, 2026, Oracle and/or its affiliates.

Set the D channel value according to the line mode specified for this configuration.

- Default: 24
- Values: 24 | 16
- For T1, select 24.
- For E1, select 16.

d-channel
(platforms with Digium BRI cards)
Set the D channel value according to the line mode specified for this configuration.

- Default: 3
- Values: 3
- For T1, select 24.
- For E1, select 16.

span-number
Set the TDM span number.

- Default: 1

For example

- 1
- 1,2
- 1,2,3,4

route-group
Configure the route group the profile belongs to.()

- Default: 0
- Min: 0 | Max: 63

line-build-out
Configure the TDM Line Build Out (LBO) value (Line Build Out is a decibel value used on a per length basis.

- Default: 0
- Values:
  - 0: 0db / 0-133 feet
  - 1: 266-399 feet
  - 2: 266 -399 feet
  - 3: 399 -533 feet
  - 4: 533 -655 feet
  - 5: -7.5 db
  - 6: -15 db
  - 7: -22.5 db

line-build-out
(Available only on platforms that have the Wanpipe driver installed.)

Copyright © 2024, 2026, Oracle and/or its affiliates.

Configure the TDM Line Build Out (LBO) value (Line Build Out is a decibel value used on a per length basis.

- Default: 0DB
- Values:
  1. 0DB
  2. 7.5DB
  3. 15DB
  4. 22.5DB
  5. 0-110FT
  6. 110-220FT
  7. 220-330FT
  8. 330-440FT
  9. 440-550FT
  10. 550-660FT
  11. 75OH
  12. 120OH

framing-value
(platforms with Digium PRI cards)
Configure TDM framing value(TDM Framing value)

- Default: esf
- Values: esf | d4 | ccs | cas

framing-value
(platforms with Digium BRI cards)
Configure TDM framing value(TDM Framing value)

- Default: ccs
- Values: ccs

coding-value
(platforms with Digium PRI cards)
TDM coding value()

- Default: b8zs
- Values: b8zs | ami | hdb3

coding-value
(platforms with Digium BRI cards)
TDM coding value()

- Default: ami
- Values: ami

crc4-checking
(platforms with Digium PRI cards)
Enable CRC-4 checking over E1 interface()

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Default: disabled
- Values: enabled | disabled

term-resistance
(platforms with Digium BRI cards)
BRI termination resistance()

- Default: disabled
- Values: enabled | disabled

timing-source
Configure TDM timing source value()

- Default: 1
- Min: 0 | Max: 4

rx-gain
(Decibel value that increases or decreases the TDM receive channel volume Valid value range is 0.0 - 9.9)

- Default: 0.0

tx-gain
(Decibel value that increases or decreases the TDM transmit channel volume Valid value range is 0.0 - 9.9)

- Default: 0.0

echo-cancellation
enable tdm echo cancellation()

- Default: enabled
- Values: enabled | disabled

overlap-dial
Configure overlap dial()

- Default: no
- Values: no | incoming

incoming-pattern
A list of extension numbers or match patterns.(List of extension numbers or match patterns. Single extension numbers are separated with the vertical bar (|) symbol. A pattern starts with the underscore symbol (_). In an extension pattern, the following characters have special meanings: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9) . wildcard, matches one or more characters ! wildcard, matches zero or more characters immediately)

- Default: _X.

options
Configure TDM options()

Copyright © 2024, 2026, Oracle and/or its affiliates.

test-policy

The test-policy element tests and displays local policy routes from the ACLI.

Parameters

source-realm
Enter the name set in the source-realm field of a configured local policy. Entering an “*” in this field matches for any source realm. Leaving the field empty indicates that only the “global” realm will be tested.

from-address
Enter the “from” address of the local policy to look up/test. From addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

to-address
Enter the “to” address of the local policy to look up/test. To addresses should be entered as SIP-URLs in the form of `sip:19785551212@netnetsystems.com`.

time-of-day
Enable or disable use of the time of day value set in the start-time and end-time fields you set in configured local-policy elements

- Values: enabled | disabled

carriers
Enter the names of permitted carriers set in the carriers fields set in configured local-policy elements. This field is formatted as a list of comma separated text strings enclosed in quotation marks.

media-profile
Enter a list of media profiles

show
Show the next hop and the associated carrier information for all routes matching the “from” and “to” addresses entered

Path

test-policy is available under the session-router path.

Notes

Type the show command to perform the actual test lookup after parameters have been entered.

The test-policy element can also be configured in Superuser mode as a command.

test-sip-manipulation

The test-sip-manipulation element allows you to test and validate a sip-manipulation. Navigate to the test-sip-manipulation element.

```
ORACLE# test-sip-manipulation
ORACLE(test-sip-manipulation)#
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

Parameters

debugging
Enable or disable debugging mode.

- Default: disabled.
- Values: enabled | disabled

direction
Set the direction of the SIP message.

- Default: out.
- Values: in | out

display-sip-message
Display on screen the SIP message that will be manipulated.

execute
Execute the referenced sip-manipulation against the SIP message.

load-sip-message
Paste a new SIP message into the ACLI to use as a test. Press Ctrl + D to end the message.

local-ip
Set the IP and port for the $LOCAL_IP variable.

manipulation-pattern
Set the manipulation pattern, used in $MANIP_PATTERN.

manipulation-string
Set the manipulation string, used in $MANIP_STRING.

refresh-manipulations
Reload any newly configured sip-manipulations.

remote-ip
Set the IP and port for the $REMOTE_IP variable.

sip-manipulation
Identify the name of the sip-manipulation you want to test.

tgrp-context
Set the trunk group context, used in the $TRUNK_GROUP_CONTEXT variable.

loop
This hidden command executes the sip-manipulation N number of times.

> **Warning**
>
> Never run the loop command on a production system. Running the loop command degrades system performance.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Example

```
ORACLE(test-sip-manipulation)# sip-manipulation rmHeaders
ORACLE(test-sip-manipulation)# execute
```

> **Note**
>
> This command exists both as a command and as a configuration element.

test-translation

The test-translation element tests translation rules configured for the Address Translation feature.

> **Note**
>
> Although you can use the **test-translation** command to test the address translation feature, you can only use it for rules configured with specific **input-header-type** and **output-header-type** values. Applicable rules include those configured with the **called-header** or **calling-header** values for both the input and output header type.

Parameters

called-address
Enter the address on which the called rules will be applied. This entry is required.

calling-address
Enter the address on which the calling rules will be applied. This entry is required.

translation-id
Enter the translation rules to test. This entry is required.

show
Show results of translation

Path

test-translation is available under the session-router path.

> **Note**
>
> The test-translation element can also be configured in Superuser mode as a command.

Copyright © 2024, 2026, Oracle and/or its affiliates.

tls-global

The tls-global configuration element allows you to configure global TLS parameters.

Parameters

session-caching
Enable or disable the SBC's session caching capability. When disabled, the SBC does not send new session tickets.

- Default: disabled
- Values: enabled | disabled

> **Note**
>
> This parameter is not RTC supported.

session-cache-timeout
Enter the session cache timeout in hours

- Default: 12
- Values: Min: 0 (disabled) / Max: 24

diffie-hellman-key-size
Enter the size of the Diffie-Hellman key offered by the SBC when negotiating TLS on a SIP interface.

- Default: DH_KeySize_1024
- Values: DH_KeySize_1024 | DH_KeySize_2048

Setting the key size to 2048 bits significantly decreases performance.

Path

tls-global is an element of the security path. The full path from the topmost ACLI prompt is: **configure terminal**, and then **security**, and then **tls-global**.

tls-profile

The tls-profile configuration element holds the information required to run SIP over TLS.

Constraints

This configuration element is not RTC supported for MSRP Online Certificate Status Protocol. To support MSRP OCSP, you must reboot after configuring **cert-status-check** and **cert-status-profile-list**.

Parameters

name
Enter the name of the TLS profile

Copyright © 2024, 2026, Oracle and/or its affiliates.

end-entity-certificate
Enter the name of the entity certification record

trusted-ca-certificates
Enter the names of the trust CA Certificate records

global-trusted-root-ca-list
Enter one or more trusted-root-ca element names for use on this tls-profile.
Enter multiple entries by listing entries within parenthesis, (), and separating them with a space. You can also add or remove a single entry to an existing list by prefixing the applicable name with a plus sign (+) to add, and a minus sign (-) to remove.

cipher-list
Enter a list of supported ciphers or retain the default value, **DEFAULT**. For a comprehensive list of ciphers supported by the OCSBC, see the *Oracle Communications Session Border Controller Release Notes*.

- Default: DEFAULT

verify-depth
Enter the maximum depth of the certificate chain that will be verified

- Default: 10
- Values: Min: 0 / Max: 10

mutual-authenticate
Enable or disable the mutual authentication of clients that connect to the SBC.

- Default: disabled
- Values: enabled | disabled

tls-version
Enter the TLS version you want to use with this TLS profile

- Default: tlsv13
- Values:
  - tlsv12
  - tlsv13
  - compatibility — When the OCSBC negotiates on TLS, it starts with the highest TLS version and works its way down until it finds a compatible version and cipher that works for the other side.

> **Note**
>
> The **security-config > sslmin** option works in conjunction with the tls-profile's **tls-version** parameter when it is set to **compatibility**. For profiles that negotiate to compatible versions, the **sslmin** option specifies the lowest TLS version allowed.

cert-status-check
Enable or disable OCSP in conjunction with an existing TLS profile.

- Default: disabled

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: enabled | disabled

cert-status-profile-list
Select an object from the cert-status-profile parameter. In order to enable this parameter, this list must not be empty. If multiple cert-status-profile objects are assigned to cert-status-profile-list, the Oracle Communications Session Border Controller will use a hunt method beginning with the first object on the list.

- Values: Any valid certificate status profile from cert-status-profile parameter

ignore-dead-responder
Allows local certificate based authentication by the Oracle Communications Session Border Controller in the event of unreachable OCSRs

- Default: disabled
- Values: enabled | disabled

allow-self-signed-cert
Allows self-signed certificate for Message Session Relay Protocol.

- Default: disabled
- Values: enabled | disabled

Path

tls-profile is an element under the security path. The full path from the topmost prompt is: **configure terminal** , and then **security** , and then **tls-profile**

translation-rules

The translation-rules element creates unique sets of translation rules to apply to input headers. See the Session Translation chapter in the Configuration Guide.

Parameters

id
Enter the identifier or name for this translation rule. This field is required.

description
A brief description of what this translation rule accomplishes.

input-header-type
Select the input header which this translation rule will modify.
The translation rule will check for the existence of this header, user part, or parameter. If a particular SIP message doesn't contain it, the rule won't modify that message.

input-header-value
Enter the regular expression that defines the modification of the input header.
If the regex pattern does not match, no modification happens. If the regex pattern does match, the whole output header will be set to the value of output-header-value. When entering regex patterns on the ACLI, wrap the pattern in double quotes if it includes spaces.

output-header-type
Select the header type which this translation rule will output to.
When the input-header-type and output-header-type are the same, the translation rule modifies a single header. When the input-header-type and output-header-type are different,

Copyright © 2024, 2026, Oracle and/or its affiliates.

the translation rule can capture values from the input header and insert them into the output header.

output-header-value
Enter the regular expression that defines the new value of the output header.
If your input-header-value includes regex capture groups, use the **$<group number>** syntax to identify the captured content.
When using capture groups that are followed by numbers, use the **$0<group number>** syntax for single-digit capture groups. For example, the SBC will read $1781 as capture group 17 followed by the literal digits 81. The SBC will read $01781 as capture group 1 followed by the literal digits 781. Capture groups that are followed by a letter, such as $3a, are not affected by this rule.

Path

The **translation-rules** element is under the session-router path.

```
ORACLE# conf term
ORACLE(configure)# session-router
ORACLE(session-router)# translation-rules
ORACLE(translation-rules)#
```

This is a multiple instance configuration element.

trap-receiver

The trap-receiver element defines the NMSs to which the Oracle Communications Session Border Controller sends SNMP traps for event reporting.

> **Note**
>
> The trap-receiver element is not used if the session delivery SNMP agent operates in SNMPv3 mode.

Parameters

ip-address
Enter the IP address and port for an NMS. If no port value is specified, the Oracle Communications Session Border Controller uses a default port of 162. This required field must follow the IPv4 or IPv6 address format.

filter-level
Set the filter level for the NMS identified within this trap-receiver element

- Default: critical
- Values:
  - **All**—All alarms, syslogs, and other traps will be trapped out. That is, the corresponding NMS will receive informational, warning, and error events.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- **Minor**—All syslogs generated with a severity level greater than or equal to MINOR and all alarms generated with a severity level greater than or equal to MINOR will be trapped out
- **Major**—All syslogs generated with a severity level greater than or equal to MAJOR and all alarms generated with a severity level greater than or equal to MAJOR will be trapped out
- **Critical**—Syslogs generated with a severity level greater than or equal to CRITICAL and all alarms generated with a severity level greater than or equal to CRITICAL will be trapped out

community-name
Enter the name of the community to which a particular NMS belongs. This required entry must follow the Name format. The community-name field values must be unique. The community-name must be 1-32 characters long and must not contain """

user-list
This parameter is configured with the name of one or more snmp-user-entry configuration element user-names for authorizing access to SNMPv3 functionality.

Path

trap-receiver is an element under the system path. The full path from the topmost ACLI prompt is: **configure terminal** , and then **system** , and then **trap-receiver.**

> **Note**
>
> This is a multiple instance configuration element.

tunnel-orig-params

The tunnel-orig-params configuration element defines a single remote IKEv2 peer.

Parameters

name
Enter the name of this instance of the **tunnel-orig-params** configuration element

- Default: None
- Values: A valid configuration element name, that is unique within the **tunnel-orig-params** namespace

remote-addr
Enter the IPv4 address of a remote IKEv2 peer

- Default: None
- Values: Any valid IPv4 address

retry-limit
Set the number of times IKEv2 tries to initiate the tunnel. If this value is exceeded, IKEv2 abandons the initiation attempt and issues an SNMP trap.

- Default: 3

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Values: Min: 1 | Max: 5

retry-time
Set the interval (in seconds) between initiation attempts.

- Default: 30 seconds
- Values: Min: 5 | Max: 60

Path

tunnel-orig-params is a subelement under the ike element. The full path from the topmost ACLI prompt is: **configure-terminal**, and then **security**, and then **ike**, and then **tunnel-orig-params**

> **Note**
>
> This is a multiple instance configuration element.

two-factor-authentication

The **two-factor-authentication** configuration element is used for configuring two-factor authentication. This element is only visible if you have the Admin Security entitlement installed.

Parameters

two-factor-auth-access-method-list
Enumerated list of the authentication access methods that require two-factor authentication.

- Default: None
- Values: SSH | GUI | SSH,GUI

common-name-list
List of the authorized Common Names (CN)

Path

two-factor-authentication is an element under the security path. The full path from the topmost prompt is: **configure terminal**, then **security**, then **authentication.**, then **two-factor-authentication**.

web-server-config

The **web-server-config** configuration element has been deprecated. See the **http-server** configuration element instead.

Copyright © 2024, 2026, Oracle and/or its affiliates.