Oracle® Enterprise Communications Broker

Maintenance Release Guide

Release PCZ20

February 2018

Oracle Enterprise Communications Broker Maintenance Release Guide, Release PCZ20

Copyright © 2014, 2018, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

Contents

About this Guide

1 PCZ2.0 M1

Content Map 1-1
GUI Appearance 1-2
Agent Groups 1-2
Multi-Hop Header Manipulation Rules (HMRs) 1-3
Multi-Hop Agent Ping 1-4
Replacing the Calling Number in the FROM Header 1-5
Deny Patterns in Route Parameter Syntax 1-5
Route Policy 1-6
RADIUS Authentication 1-7
Management Protocol Behavior 1-9
RADIUS Authentication Configuration 1-9
Global Authentication Settings 1-10
RADIUS Server Settings 1-10
Forcing an HA Switchover 1-12
Setting Your Login Banner 1-12
Displaying and Clearing Alarms 1-13
Displaying Users 1-13
Displaying Log Files 1-14
Displaying System Health 1-14
Obtaining Support Information 1-15
The User Menu 1-15
Issues Resolved 1-15

2 PCZ2.0 M2

Content Map 2-1
Memory Requirement 2-2
Using Policy to Refine Routing 2-2
The Redirect Action 2-3

Defining a Custom Policy 2-4
Applying a Policy to a Route 2-6
Applying a Policy to the Registrar 2-6
Configurations Using Policy 2-6
Priority Call Handling 2-6
Transcoding and the Oracle Enterprise Communications Broker 2-7
Multiple Outbound Translations 2-8
Routing Action Configurations 2-10
Resolving to the Longest Match in the User Database 2-12
Fork Groups 2-13
Fork Group Assignment 2-14
Additional Targets 2-15
Configuring Fork Groups 2-15
Configuring Fork Groups on Agents 2-15
Configuring Additional Target Groups 2-16
Configuring Fork Groups on a Registrar 2-16
Configuring LDAP for Fork Groups 2-16
Configuring the Global Fork Group Timer 2-17
LDAP Client Configuration 2-17
LDAP Configuration Options 2-17
Making Settings 2-18
LDAP Groups 2-18
Matching Criteria in LDAP Groups 2-19
Configuring LDAP Groups 2-19
SIP REFER on the Oracle Enterprise Communications Broker 2-20
SIP REFER Method Call Transfer for ECB 2-20
Unsuccessful Transfer Scenarios 2-21
Call Flows 2-21
SIP REFER Method Configuration 2-23
180 & 100 NOTIFY in REFER Call Transfers for ECB 2-24
Sample Messages 2-26
180 and 100 NOTIFY Configuration 2-27
TOS Marking 2-28
Syslog Settings 2-28
Early Media Inhibit 2-29
Command Line Interface (CLI) Widgets 2-29
CLI Display Timeouts 2-30
Issues Resolved 2-31

3 PCZ2.0 M3

Content Map 3-1
Behavioral Changes 3-2
Configuring CNAM Replacement 3-2
Using Policy to Normalize SIP Headers 3-3
ANI Masking 3-3
ANI Masking Configurations 3-4
Restricting Session Initiation 3-5
Proxy Registrations 3-5
Synchronizing the Registration Cache 3-5
Audit Logs 3-6
Secure FTP Push Configuration 3-8
Configure Secure FTP Push with Public Key Authentication 3-8
Generate an RSA Public Key 3-9
Generate a DSA Public Key 3-9
Import a DSA Public Key 3-10
Copy the RSA Public Key to the SFTP Server 3-10
Configure Audit Logging 3-11
License Widget 3-12
Issues Resolved 3-13

4 PCZ2.0 M4

Content Map 4-1
64-bit Upgrade 4-2
Platform Boot Loaders 4-2
Apply a Policy to the User Table 4-2
SIP Monitor and Trace Filter Configuration 4-3
SIP Session Summary Changes 4-5

A Known Issues and Caveats

Known Issues and Caveats - M1 A-1
Known Issues A-1
Caveats A-2
Limitations A-3
Known Issues and Caveats - M2 A-3
Known Issues A-3
Caveats A-5
Limitations A-5
Known Issues and Caveats - M3 A-6

Known Issues (M3) A-6
Caveats (M3) A-9
Known Issues and Caveats - M4 A-9
Known Issues (M4) A-10
Caveats (M4) A-10

B CLI Portal Reference

About this Guide

This Oracle Enterprise Communications Broker Maintenance Guide supports Release PCZ2.0 and the corresponding documentation set. This guide provides an overview of new features and functions in PCZ2.0 maintenance releases. This guide also documents issues fixed since PCZ2.0 GA, as well as known issues and caveats associated with the latest maintenance release.

The information contained in this Maintenance Guide pertains to Enterprise Customers, and the following Oracle Enterprise Communications Broker distributions:

- Netra ISO — Designed for distributed medium to large enterprises, runs on a certified Netra server.
- Software Only — Designed for distributed medium to large enterprises, runs on a generic server within a virtual OVM environment.

Refer to the Oracle Enterprise Communications Broker PCZ2.0 documentation set for more information about each platform.

Audience

This Maintenance Guide is for enterprise users who want to know about new features, fixed issues, known issues, and caveats.

Licensing

The PCZ2.0 releases are an aggregation of software from various sources and organizations. These include Oracle software, third-party commercial software used under license, and publicly available software packages distributed under various open source licenses. For full details of the applicable licenses and how to obtain the corresponding source code for the open source components, click About on the Web GUI software User menu or ask your Oracle representative.

Revision History

Date	Revision Number	Description
December, 2014	1.00	Initial Release
December, 2014	1.10	• Adds known issue on behavior when the system attempts to forward an ACK request. • Removes defect indicating Oracle ECB would not recover from an OVM kernel crash. • Adds section on RADIUS authentication support via GUI configuration.
January, 2015	1.20	• Adds the ability to use multiple DNS servers to the Issues Resolved section.
June, 2015	1.30	• Adds M2 content.

Date	Revision Number	Description
July, 2015	1.40	• Corrects fixed issues lists. • Adds note warning users not to have duplicate phone numbers in LDAP database.
February, 2016	1.50	• Adds M3 content. • Removes the Local Route Table entries from the Command Line Portal Reference Appendix.
March 2016	1.60	• Adds M4 content.
April 2016	1.70	• Updates the procedure for configuring High Availability with NTP in the Known Issues section.
July 2016	1.80	• Adds updated hardware requirements for virtual systems to the 64-bit Upgrade topic. • Adds instructions for Virtual Machines to the HA with NTP Known Issue in M3. • Adds behavioral information to the Redirect Action topic in the M2 chapter about how system handles a redirect route.
February 2018	1.90	Adds the "Early Media Inhibit" item to the Known Issues table in the M4 chapter.

1

PCZ2.0 M1

This chpater provides descriptions, explanations, and configuration information for the contents of Maintenance Release PCZ2.0.0M1. Maintenance Release content supercedes that distributed with the previous point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.7
- P1.0.0

Current patch baseline: PCZ2.0.0p2

Content Map

The following table identifies the new content in this PCZ2.0 M1 Maintenance Release documentation.

Content Type	Description
Adaptation	GUI Appearance
Adaptation	Agent Group Support
Adaptation	Multi Hop HMR
Adaptation	Multi Hop Agent Ping
Adaptation	Replace Calling Number in From header with a Number from an LDAP Response
Adaptation	Deny Dial Pattern within Route Entries
Adaptation	Route Policy: Stop Recursion and Deny Route
Adaptation	Configure RADIUS Authentication from the GUI
Adaptation	Force a Switchover from the GUI
Adaptation	Create and Display Login Banner Text

Content Type	Description
Adaptation	Show and Clear Alarms from the GUI
Adaptation	Show Users
Adaptation	View a Log File
Adaptation	Show the System Health
Adaptation	Create Support Info File
Adaptation	The User Menu
Defect Tracking	Issues Resolved

GUI Appearance

The Oracle Enterprise Communications Broker GUI no longer displays the Acme Packet logo on any dialogs. Instead the GUI displays the Oracle logo. There are also subtle changes to the GUI layout. For example, the splash page's layout includes non-functional changes, such as its use of the color red. The majority of functional controls remain the same as the previous version; those that are changed are documented herein.

Agent Groups

Agent groups contain multiple agents. Members of an agent group are logically equivalent (although they might vary in their individual constraints) and can be used interchangeably as transit targets for SIP traffic. For one reason or another, a given agent may not be able to service traffic. Users configure agent groups to establish multiple transit destinations for purposes such as redundancy.

Examples of agent groups include the following:

- Application Server cluster
- Media Gateway cluster
- Softswitch redundant pair
- SIP Proxy redundant pair
- Gatekeeper redundant pair

Agent group members do not need to reside in the same domain, network, or realm. The Oracle Enterprise Communications Broker can allocate traffic among member agents regardless of their location. It uses the allocation strategies configured for an agent group to allocate traffic across the group members.

The user configures agent groups from the GUI's Agent configuration dialog. This configuration consists of simply naming the group, selecting the allocation strategy, selecting recursion preference and adding the agent group members.

Having configured the group, the user then configures agent group names as:

- A `Dest agent` in a routing table entry
- A `Route` in a routing table entry
- A user's `Home agent` in the user database
- A `Default home agent` within an LDAP query

The syntax for these entries appears as the word 'group' followed by a colon (:) and the group name.

```
group:MyGroupName
```

When configuring the group, the user selects between the following allocation strategies to define the method of selecting the next member of the group for a connection attempt if the previous connection attempt fails:

Allocation Strategy	Description
Hunt	Oracle Enterprise Communications Broker selects the agents in the order in which they are configured in the agent group. If the first agent is in service, and has not exceeded any defined constraints, all traffic is sent to the first agent. If the first agent is out of service, or is in violation of constraints, all traffic is sent to the second agent. And so on for all agents in the agent group. When the first agent returns to service, the new traffic is routed back to it.
Round robin	Oracle Enterprise Communications Broker selects each agent in the order in which it is configured, routing a session to each agent in turn.

To summarize, agent group operation requires the following configuration:

- Two or more agents
- An agent group containing those agents
- A route, user configuration or LDAP query that directs traffic to that group

Recursion

Agent groups use a recursive process to communicate with agent group members. This recursion behavior is specified by the allocation strategy. The user can optionally configure the Oracle Enterprise Communications Broker to attempt communications with only a single member of the agent group by leaving the **Try All** control unchecked (disabled).

The agent group performs its agent selection rotation process independently of this recursion setting. Each allocation strategy rotates agent selection as a means of selecting the first agent to try. This ensures that the system continues to use each agent in the group as a message target.

Routing paths may traverse multiple agent groups. The system, however, only performs recursion on the last agent group in the path. This reduces what could otherwise become an inordinate number of connection attempts.

Multi-Hop Header Manipulation Rules (HMRs)

Oracle Enterprise Communications Broker HMR support includes allowing the user to specify that a manipulation be applied depending on an agent's location (hop) in a route. Applicable hops include the next and last hop of a route. Applying an HMR when an agent is the last hop in a route is referred to as 'multi-hop' HMR. The user configures this on session agents. HMRs themselves do not require any changes to their configuration to operate as multi-hop HMRs.

The user configures an agent's **Apply-outbound-manipulation-on** parameter to specify when the system applies the agent's outbound HMR. Syntax for this command is shown below.

Apply-outbound-manipulation-on [next-hop-only | last-hop-only | next-and-last-hop]

The default setting is **next-hop-only**. This configuration makes the system apply the outbound HMR only when the agent is the next hop in the route's path.

If there are multiple HMRs the Oracle Enterprise Communications Broker must apply for the route, it applies the HMR for the last hop first. If the same agent is both next and last hop for any given traffic, the Oracle Enterprise Communications Broker applies the HMR only once regardless of the `Apply-outbound-manipulation-on` setting.

Multi-Hop Agent Ping

The Oracle Enterprise Communications Broker's ping function can test connectivity to endpoints that are not directly adjacent to the source Oracle Enterprise Communications Broker. This multi-hop ping capability requires that the user configure special routes dedicated to sending SIP options pings to these targets.

To enable ping tests to targets that are more than one hop from the Oracle Enterprise Communications Broker, they configure routes that have the string `"ping:"` in the **Called number** field. These routes also have first agent towards the target configured in the **Route** field, and the last agent toward the target configured in the **Destination Agent** field.

The system invokes these `ping:` routes for ping traffic only. In addition, the system prioritizes SIP signaling traffic over `ping:` route traffic.

An example of a multi-hop ping route is shown in the table below.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
*	*	Target_Agnt	ping:	Adja_Agnt	0	

Having configured this route, the user can then initiate a ping to a target, or configure agent pinging to `Target_Agnt`, via `Adja_Agnt`.

The user can also set up multi-hop ping recursion by creating multiple `ping:` routes that specify the complete path to the target. To create these paths, the user can configure `ping:` routes using the `Destination Agent` and `Route` fields to define each hop in a "ping path".

Based on the two routes entries below, for example, ping attempts to reach the device defined as `Target_Agnt` follow a two-hop path:

1. Oracle Enterprise Communications Broker to `Adja_Agnt`
2. `Adja_Agnt` to `Interim_Agnt`
3. `Interim_Agnt` to `Target_Agnt`

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
*	*	Interim_Agnt	ping:	Adja_Agnt	0	
*	*	Target_Agnt	ping:	Interim_Agnt	0	

The Oracle Enterprise Communications Broker uses an agent status, as determined by OPTIONS ping, to validate all routes using that agent. Specifying an agent's status, including in-service and out-of-service, is the same for agents using either single or multi-hop ping. The system does not use routes to out-of-service agents for any signaling traffic.

Replacing the Calling Number in the FROM Header

The Oracle Enterprise Communications Broker provides for replacement of the calling number in SIP messages' FROM headers. Applicable messages include INVITEs that match the query, and all messages sent by the Oracle Enterprise Communications Broker to those calls' callees. An example application is allowing recipient UEs to display a caller ID that would be recognized by the recipient, even during an enterprise's transition to new dialing schemes.

This calling number replacement function refers to LDAP resources as the source of the replacement calling number. The user configures a lookup query from the **Modify LDAP config** dialog to specify this source. Configured lookup queries become available in the **FROM header replacement** drop-down list, from which the user selects their query. This selection specifies and enables the replacement.

This feature piggybacks normal LDAP lookup procedures by collecting an additional value within the LDAP query request/response sequence. The Oracle Enterprise Communications Broker replaces the FROM header of the outgoing message with this value.

While processing this LDAP response for calling number, the Oracle Enterprise Communications Broker stores the result of the query and uses it to create the FROM header user parts for applicable outgoing messages. For traffic in which there is no match to the calling number, the Oracle Enterprise Communications Broker simply uses the original calling number.

The user can disable this replacement function by clearing the lookup query attribute name from the **FROM header replacement** field.

Deny Patterns in Route Parameter Syntax

The Oracle Enterprise Communications Broker allows the user to configure routes that refine the routing engine's behavior, based on the called and/or calling number. Specifically, this syntax prevents the routing engine from using that route entry as a member of the applicable route sets.

The user configures this behavior by creating a route that prepends the called and/or calling numbers with an exclamation point (!). An example of a route entry using a deny pattern is shown below. The user configures the digits following the exclamation point as the first digits in the string, not the entire string.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Agent_1	!123	*	*	Agent_2	0	

As configured, traffic that includes a calling number starting with the digits 123 does not match this route. The Oracle Enterprise Communications Broker, therefore, does not use this route in any applicable route set.

In addition, the user can configure both calling and called numbers with the deny format to establish an "and" condition to the route.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Agent_1	!123	*	!456	Agent_2	0	

As configured, traffic that includes a calling number starting with the digits 123 and a called number starting with the digits 456 does not match this route.

Conversely, the "and" condition allows the following traffic originating from `Agent_1` via `Agent_2` to match this route:

- From any calling number that does not start with the digits 123 to any called number.
- From any calling number that starts with the digits 123 to any called number other than one that starts with 456.
- To any called number that does not start with the digits 456.
- To any called number that starts with the digits 456 from any called number other than one that starts with 123.

Route Policy

The Oracle Enterprise Communications Broker includes a route configuration control called **Policy** that allows the user to alter the behavior of routes. As the Oracle Enterprise Communications Broker assembles hops together to create an complete route, it considers and acts on the policies configured on each route entry.

The user configures a route's **Policy** from the Modify Routing entry dialog. The parameter's values include:

Policy [Deny | StopRecurse]

The field's default setting is empty, which imposes no policy on the route.

The **Deny** policy in any resultant SIP routes to a destination prevents the Oracle Enterprise Communications Broker from forwarding a SIP request to the destination point in question. The user can use the **Deny** policy to prevent session between two endpoints for policy or cost reasons. Consider this route entry.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Class_B	*	Protect_Agnt	*	Transit_Agnt	0	Deny

The user has configured this route entry to prevent calls passing through the agent named `Class_B` from reaching any endpoint behind `Protect_Agnt`. This route entry may be installed as part of one or multiple routes that could potentially reach `Protect_Agnt`. Having assembled these routes, however, the routing engine recognizes the presence of this entry and rejects the call.

To expand upon the example, consider this route.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Class_A	*	Protect_Agnt	*	Transit_Agnt	0	StopRecurse

The user is allowing traffic to reach `Protect_Agnt` as long as it originates via the agent named `Class_A`.

The **StopRecurse** policy stops further attempts to forward a SIP request to a given destination if that route fails. The **StopRecurse** policy can prevent the system from forwarding calls on routes that are cost-prohibitive or could cause loops in SIP call flows.

For example, consider the case where an endpoint can be reached using two routes.

- Route 1: Agent_1 > Agent_2 (**StopRecurse**) > PBX
- Route 2: Agent_3 > PSTN

Route 1 has a **StopRecurse** policy defined on the hop between Agent_2 and PBX. The Oracle Enterprise Communications Broker stops processing the call if Route 1 does not receive a successful response. This configuration can prevent calls initially targeted for Route 1 from using the PSTN.

RADIUS Authentication

The User Authentication and Access control feature supports authentication using your RADIUS server(s). In addition, you can set two levels of privilege, one for all privileges and more limited set that is read-only.

User authentication configuration also allows you to use local authentication, localizing security to the Oracle Enterprise Communications Broker log-in modes. These modes are User and Superuser, each requiring a separate password.

The components involved in the RADIUS-based user authentication architecture are the Oracle Enterprise Communications Broker and your RADIUS server(s). In these roles:

- The Oracle Enterprise Communications Broker restricts access and requires authentication via the RADIUS server; the Oracle Enterprise Communications Broker communicates with the RADIUS server using either port 1812 or 1645, but does not know if the RADIUS server listens on these ports
- Your RADIUS server provides an alternative method for defining Oracle Enterprise Communications Broker users and authenticating them via RADIUS; the RADIUS server supports the VSA called ACME_USER_CLASS, which specifies what kind of user is requesting authentication and what privileges should be granted.
  The Oracle Enterprise Communications Broker also supports the use of the Cisco Systems Inc.™ Cisco-AVPair vendor specific attribute (VSA). This attribute allows for successful administrator login to servers that do not support the Oracle authorization VSA. While using RADIUS-based authentication, the Oracle Enterprise Communications Broker authorizes you to enter Superuser mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA. For this VSA, the Vendor-ID is 1 and the Vendor-Type is 9. The list below shows the values this attribute can return, and the result of each:
  - shell:priv-lvl=15—User automatically logged in as an administrator
  - shell:priv-lvl=1—User logged in at the user level, and not allowed to become an administrator
  - Any other value—User rejected

When RADIUS user authentication is enabled, the Oracle Enterprise Communications Broker communicates with one or more configured RADIUS servers that validates the user and specifies privileges. On the Oracle Enterprise Communications Broker, you configure:

- What type of authentication you want to use on the Oracle Enterprise Communications Broker
- If you are using RADIUS authentication, you set the port from which you want the Oracle Enterprise Communications Broker to send messages

- If you are using RADIUS authentication, you also set the protocol type you want the Oracle Enterprise Communications Broker and RADIUS server to use for secure communication

Although most common set-ups use two RADIUS servers to support this feature, you are allowed to configure up to six. Among other settings for the server, there is a class parameter that specifies whether the Oracle Enterprise Communications Broker should consider a specific server as primary or secondary. As implied by these designation, the primary servers are used first for authentication, and the secondary servers are used as backups. If you configure more than one primary and one secondary server, the Oracle Enterprise Communications Broker will choose servers to which it sends traffic in a round-robin strategy. For example, if you specify three servers are primary, the Oracle Enterprise Communications Broker will round-robin to select a server until it finds an appropriate one; it will do the same for secondary servers.

The VSA attribute assists with enforcement of access levels by containing one of the three following classes:

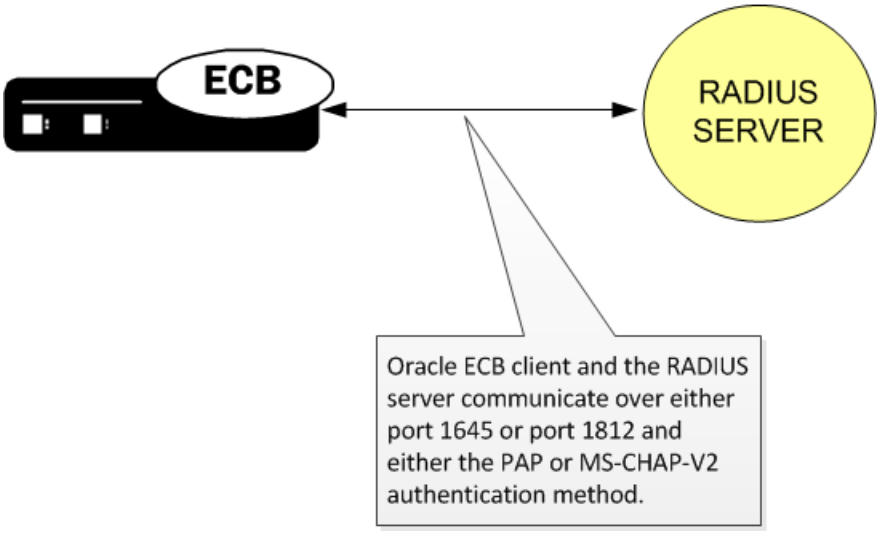
- None—All access denied
- User—Monitoring privileges are granted; your user prompt will resemble ORACLE>
- Admin—All privileges are granted (monitoring, configuration, etc.); your user prompt will resemble ORACLE#

Once it has selected a RADIUS server, the Oracle Enterprise Communications Broker initiates communication and proceeds with the authentication process. The authentication process between the Oracle Enterprise Communications Broker and the RADIUS server takes place uses one of three methods, all of which are defined by RFCs:

Protocol	RFC
PAP (Password Authentication Protocol)	B. Lloyd and W. Simpson, PPP Authentication Protocols, RFC 1334, October 1992
CHAP (Challenge Handshake Authentication Protocol)	B. Lloyd and W. Simpson, PPP Authentication Protocols, RFC 1334, October 1992 W. Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, August 1996
MS-CHAP-V2	G. Zorn, Microsoft PPP CHAP Extensions, Version 2, RFC 2759, January 2000

Note:

MS-CHAP-V2 support includes authentication only; password exchange is not supported or allowed on the Oracle Enterprise Communications Broker.



Management Protocol Behavior

When you use local authentication, management protocols behave the same way that they do when you are not using RADIUS servers. When you are using RADIUS servers for authentication, management protocols behave as described in this section.

- Telnet—The “user” or admin accounts are authenticated locally, not via the RADIUS server. For all other accounts, the configured RADIUS servers are used for authentication. If authentication is successful, the user is granted privileges depending on the ACME_USER_CLASS VSA attribute.
- FTP—The “user” or admin accounts are authenticated locally, not via the RADIUS server. For all other accounts, the configured RADIUS servers are used for authentication.
- SSH in pass-through mode—When SSH is in pass through mode, the Oracle Enterprise Communications Broker behaves the same way that it does for Telnet.
- SSH in non-pass-through mode—When you create an SSH account on the Oracle Enterprise Communications Broker, you are asked to supply a user name and password. Once local authentication succeeds, you are prompted for the ACLI user name and password. If your user ACLI name is user, then you are authenticated locally. Otherwise, you are authenticated using the RADIUS server. If RADIUS authentication is successful, the privileges you are granted depend on the ACME_USER_CLASS VSA attribute.
- SFTP in pass-through mode—If you do not configure an SSH account on the Oracle Enterprise Communications Broker, the RADIUS server is contacted for authentication for any user that does not have the user name user. The Oracle Enterprise Communications Broker uses local authentication if the user name is user.
- SFTP in non-pass-through mode—The “user” or admin accounts are authenticated locally, not via the RADIUS server. For all other accounts, the configured RADIUS servers are used for authentication.

RADIUS Authentication Configuration

To enable RADIUS authentication and user access on your Oracle Enterprise Communications Broker, you need to configure global parameters for the feature and then configure the RADIUS servers that you want to use.

Global Authentication Settings

To configure the global authentication settings:

1. Click the **Configuration** tab.

   The Oracle Enterprise Communications Broker displays the configuration panel.

2. Click the **Security** configuration icon.

   The Oracle Enterprise Communications Broker displays the security configuration panel.

3. Click the **Login authentication** link from the navigation panel on the left-hand side of the security configuration panel.

   The Oracle Enterprise Communications Broker displays the **Modify Authentication** dialog.

4. Set the number of the port you want to use from message sent from the Oracle Enterprise Communications Broker to the RADIUS server in the **Source port** field. The default value is 1812. The valid values are:

   - 1645 | 1812

5. Set the type of user authentication you want to use on this Oracle Enterprise Communications Broker using the **Type** drop-down list. The default value is **local**. The valid values are:

   - local | radius

6. If you are using RADIUS user authentication, set the protocol to use with your RADIUS server(s) from the **Protocol** drop-down list. The default is **pap**. The valid values are:

   - pap | chap | mschapv2

7. Set the **allow-local-authorization parameter** to **enabled** if you want the Oracle Enterprise Communications Broker to authorize users to enter Superuser (administrative) mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA. The default for this parameter is **disabled**.

8. Check the **Login as admin** checkbox if you want users to be logged automatically in Superuser (administrative) mode. The default for this parameter is disabled.

RADIUS Server Settings

The parameters you set for individual RADIUS servers identify the RADIUS server, establish a password common to the Oracle Enterprise Communications Broker and the server, and establish trying times.

Setting the class and the authentication methods for the RADIUS servers can determine how and when they are used in the authentication process.

To configure a RADIUS server to use for authentication:

1. Navigate to the Radius servers list box directly below the main authentication configuration controls. The list box displays all previously configured Radius servers, if any. You can Add, Edit, Copy and Delete existing servers using the control across the top of this list box.

2. Click the Add link.

   The Oracle Enterprise Communications Broker displays the Add Radius server dialog.

3. Set the remote IP address for the RADIUS server in the **Add** field. There is no default value, and you are required to configure this address.
4. Set the port at the remote IP address for the RADIUS server in the **Port** field. The default port is set to **1812**. The valid values are:
   - 1645 | 1812
5. Set the state of the RADIUS server in the **State** field. Enable this parameter to use this RADIUS server to authenticate users. The default value is **enabled**. The valid values are:
   - enabled | disabled
6. Set the password that the RADIUS server and the Oracle Enterprise Communications Broker share in the **secret** dialog, available when you click the **set** button. This dialog requires you to enter the secret twice and click **OK**. This password is transmitted between the two when the request for authentication is initiated; this ensures that the RADIUS server is communicating with the correct client.
7. Set the NAS ID for the RADIUS server in the **Nas id** field. There is no default for this parameter.
8. Set the number of times that you want the Oracle Enterprise Communications Broker to retry for authentication information from this RADIUS server in the **retry-limit** field. The default value is **3**. The valid range is:
   - Minimum—1
   - Maximum—5

     If the RADIUS server does not respond within this number of tries, the Oracle Enterprise Communications Broker marks is as dead.
9. Set the amount of time (in seconds) that you want theOracle Enterprise Communications Broker to wait before retrying for authentication from this RADIUS server in the **retry-time** field. The default value is **5**. The valid range is:
   - Minimum—5
   - Maximum—10
10. Set the amount of time in seconds before the Oracle Enterprise Communications Broker retries a RADIUS server that it has designated as dead because that server did not respond within the maximum number of retries in the **dead-time** field. The default is **10**. The valid range is:
    - Minimum—10
    - Maximum—10000
11. Set the maximum number of outstanding sessions for this RADIUS server. The default value is **255** in the **maximum-sessions** field. The valid range is:
    - Minimum—1
    - Maximum—255
12. Set the class of this RADIUS server as either primary or secondary in the **class** field. A connection to the primary server is tried before a connection to the secondary server is tried. The default value is **primary**. Valid values are:
    - primary | secondary

      The Oracle Enterprise Communications Broker tries to initiate contact with primary RADIUS servers first, and then tries the secondary servers if it cannot reach any of the primary ones.

If you configure more than one RADIUS server as primary, the Oracle Enterprise Communications Broker chooses the one with which it communicates using a round-robin strategy. The same strategy applies to the selection of secondary servers if there is more than one.

13. Set the authentication method you want the Oracle Enterprise Communications Broker to use with this RADIUS server from the in the **authentication-method** drop-down. The default value is **pap**. Valid values are:

    - all | pap | chap | mschapv2

      This parameter has a specific relationship to the global protocol parameter for the authentication configuration, and you should exercise care when setting it. If the authentication method that you set for the RADIUS server does not match the global authentication protocol, then the RADIUS server is not used. The Oracle Enterprise Communications Broker simply overlooks it and does not send authentication requests to it. You can enable use of the server by changing the global authentication protocol so that it matches.

14. Save your work and activate your configuration.

Forcing an HA Switchover

The Oracle Enterprise Communications Broker allows the user to cause an HA switchover manually. Executing this procedure forces the two Oracle Enterprise Communications Brokers in your HA node to trade roles. The active system becomes standby, and the standby becomes active.

To perform a successful manual switchover, the following conditions must be met:

- The Oracle Enterprise Communications Broker from which you trigger the switchover must be in one of the following states: active, standby, or becoming standby.
- A manual switchover to the active state is only allowed on a Oracle Enterprise Communications Broker in the standby or becoming standby state if it has achieved full media, signaling, and configuration synchronization.
- A manual switchover to the active state is only allowed on a Oracle Enterprise Communications Broker in the standby or becoming standby state if it has a health score above the value you configure for the threshold.

1. Click the **System** tab.

   The Oracle Enterprise Communications Broker displays the system navigation panel to the left of the window displaying the associated controls.

2. Click the **System** tab's **Force HA switchover** link.

   The Oracle Enterprise Communications Broker displays the **Force HA switchover** dialog, which includes a **Switch to standby** button.

3. Click the **Switch to standby** button.

   The Oracle Enterprise Communications Broker executes the HA role change.

Setting Your Login Banner

The Oracle Enterprise Communications Broker allows the user to create and edit the message displayed in the Login banner dialog, which appears upon successful login.

1. Click the **Configuration** tab.

The Oracle Enterprise Communications Broker displays the configuration panel.

2. Click the **Wizards** dropdown.

   The Oracle Enterprise Communications Broker displays the widget menu panel.

3. Click the **Set login banner** link.

   The Oracle Enterprise Communications Broker displays the **Set login banner** dialog, which includes a text box allowing the user to write a login message.

4. Type your banner text and click the **Save** button to set the banner.

   The Oracle Enterprise Communications Broker sets the login banner.

Displaying and Clearing Alarms

The Oracle Enterprise Communications Broker provides a widget that allows the user to see all current alarms that the system has triggered.

1. Click the **Widgets** tab.

   The Oracle Enterprise Communications Broker displays the widget navigation panel to the left of the associated controls.

2. Find and click the **Alarms** widget group in the **System** widget category.

   The Oracle Enterprise Communications Broker displays the **Alarms** widget display types, including the link to the **Table** display.

3. Click the **Table** link.

   The Oracle Enterprise Communications Broker displays the **Alarms** table.

4. To clear alarms, click either the **Clear** or **Clear All** links in the Alarms table's control bar.

   The **clear** link clears the selected alarm. The **Clear All** link clears them all.

Displaying Users

The Oracle Enterprise Communications Broker provides a widget that allows the user to see a list of other users currently logged into the system.

1. Click the **Widgets** tab.

   The Oracle Enterprise Communications Broker displays the widget navigation panel to the left of the associated controls.

2. Find and click the **User Management** widget group in the **System** widget category.

   The Oracle Enterprise Communications Broker displays the **Show users** widget display types, including the link to the **Table** display.

3. Click the **Table** link.

   The Oracle Enterprise Communications Broker displays the **Show users** table. Controls also include a button that allows the current user, assuming that user has administrator privileges, to disconnect another currently connected user.

Displaying Log Files

The Oracle Enterprise Communications Broker allows the user to view log files without having to download them.

1. Click the **System** tab.

   The Oracle Enterprise Communications Broker displays the system navigation panel to the left of the associated controls.

2. Click the **System** tab's **File management** link.

   The Oracle Enterprise Communications Broker displays the **File Management** dialog, which includes **File type** drop down control.

3. Select the **Log** file type.

   The Oracle Enterprise Communications Broker displays file list, displaying all log file categories.

4. Expand a log file category and select a log file by checking the file's check box.

   The Oracle Enterprise Communications Broker enables all applicable command links on the File Management control bar, including the **View** link.

5. Click the **View** link.

   The Oracle Enterprise Communications Broker displays the **Viewing log:[filename]** dialog with the log file's contents. This dialog includes **Close** and **Refresh** buttons.

Displaying System Health

The Oracle Enterprise Communications Broker provides a widget that allows the user to see your device's current health score and state.

1. Click the **Widgets** tab.

   The Oracle Enterprise Communications Broker displays the widget navigation panel to the left of the associated controls.

2. Find and click the **System health** widget group in the **System** widget category.

   The Oracle Enterprise Communications Broker displays the **System health** widget display types, including the link to the **Table** display.

3. Click the **Table** link.

   The Oracle Enterprise Communications Broker displays the **System health** table.

4. Click the Synchronization health button to show extended details on the system's current status.

   The system displays the popup Synchronization health table. The table's information is useful to determine the system's relative ability to act as primary in an HA configuration. If the system is deployed in an HA configuration, there is also a Switch over log button, which allows the user to display information about HA switchover events.

Obtaining Support Information

The Oracle Enterprise Communications Broker allows the user obtain a pre-defined file containing information that support personnel normally request.

1. Click the **System** tab.

   The Oracle Enterprise Communications Broker displays the system navigation panel to the left of the associated controls.

2. Click the **System** tab's **Support information** link.

   The Oracle Enterprise Communications Broker displays the **Support Information** dialog, which includes the **Support information** button allowing the user to generate support information output.

3. Click the **Support information** button.

   The Oracle Enterprise Communications Broker displays a **Progress** message box, which indicates the system is generating support information output. When complete, your browser displays a dialog allowing you to decide what to do with the support-info.log file.

4. Follow the dialog's instructions to select the application you want to use to display your support-info.log file or save the file locally.

The User Menu

Oracle Enterprise Communications Broker dialogs include a User menu. This menu is located in the upper right-hand corner of each Oracle Enterprise Communications Broker dialog, and is labeled with the currently logged in user's name.

Commands the user can execute from the User menu include:

- Screen help
- Help topics
- About
- Logout

Issues Resolved

Documented issues resolved between Release PCZ2.0 GA and Release PCZ2.0 M1 are listed below.

- The user may now configure multiple DNS server IP addresses as resources for the Oracle ECB.
- If the user presses the GUI's back button while working within the LST editor, the system now warns the user that changes are about to be lost.
- "Inner" configuration objects, such as dial patterns inside a dial context, are now searchable.
- The GUI Initial install wizard now performs error checking on invalid IP address entries. Furthermore, the wizard does not complete when configured with invalid IP addresses.
- An invalid search string no longer returns invalid results.

- The LST Editor no longer displays a blank screen when opening LST files that do not have well-formed XML syntax.
- The Verify config panel no longer keeps reappearing after being minimized.
- After adding an ECB sync peer and activating the configuration, the Web GUI no longer appears to hang, displaying a "Loading" message.
- When configured with LST/LDAP authentication, the system no longer exhibits a minimal memory leak during re-registrations. This became evident after days of running at high load.
- The Ping Widget no longer reports an error for agents that do not respond with a 200 OK to OPTION pings.
- The user can now configure Host Routes with the GUI.
- The Initial setup wizard now provisions a default gateway properly.
- Enabling LST or LDAP authentication is now dynamically configurable.
- The system now informs the user that the TLS license is not present when they attempt to configure it.
- The system now properly acquires a configuration lock when the user performs an upgrade to a standby system, regardless of upgrade method.

2

PCZ2.0 M2

This chapter provides descriptions, explanations, and configuration information for the contents of Maintenance Release PCZ2.0 M2. Maintenance Release content supercedes that distributed with the previous point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.7
- P1.0.0

Current patch baseline: PCZ2.0.0 M1p2

Content Map

The following table identifies the new content in this PCZ2.0 M2 Maintenance Release documentation.

Content Type	Description
Platform Resource Change	Memory Requirement
Adaptation	Policy-Based Routing
Application (Using Policy)	Priority Call Handling
Application (Using Policy)	Conditional Routing to Transcoders
Application (Using Policy)	Multiple Outbound Translations
Adaptation	User DB - Longest Match Resolution
Adaptation	Fork Groups
Adaptation	LDAP Server Enhancements
Adaptation	SIP REFER
Adaptation	TOS Marking
Adaptation	Syslog Setting Enhancement

Content Type	Description
Adaptation	Early Media Inhibit
GUI Adaptation	Command Line Interface Widgets
GUI Adaptation	Synchronize Configuration Files to Standby
Defect Tracking	Issues Resolved

Memory Requirement

The Oracle Enterprise Communications Broker version PCZ2.0.0 M2 requires 4G memory for proper operation. Note that any ugrades from prior versions also require memory upgrade to 4G. This requirement applies to all platforms.

Using Policy to Refine Routing

The Oracle Enterprise Communications Broker supports policy-based routing, allowing the user to select pre-defined policies or create their own policies and apply them to routes or the Registrar. In turn, these policies impact the behavior of the applicable routes when traffic matches user-defined conditions. The user configures new policies from the Oracle Enterprise Communications Broker's **Policy** icon (or uses pre-built policies) and applies them to routes and/or the Registrar. Routes support multiple policies.

Policy provides the Oracle Enterprise Communications Broker with a generic approach to configuring routing applications. Policy configuration assumes a desired behavior that has been identified by the user. The most common objectives include:

- Establish more specific routing decisions
- Apply additional services

The Oracle Enterprise Communications Broker abstracts policy behavior into three components including:

- Route
- Condition
- Action

The combination of route and condition define when the policy applies. The action refines the way in which the traffic uses the route. Note that possible actions may include not using the route.

This generic approach to route policy provides great flexibility in policy definition, but also imposes a level of complexity on the user, requiring them to:

- Identify the application they want to create.
- Determine how to identify the applicable traffic.
  - Use or create new routes specifically for the application.
  - Define the condition that causes the system to apply the policy to the route.
- Test traffic matching and application action.
- Ensure no overlapping configurations cause the system to use or not use the policy unexpectedly.

There are two components of a policy configuration:

- Conditions:
  - codec-condition—Tell the system to determine the presence of absence of specific codecs within an offer.
  - time-condition—Specify the day(s) of the week and time(s) of the day when the system uses the policy.
- Actions:
  - routing-action—Tells the system to modify how the route is applied.
  - redirect-action—Tells the system to direct traffic to the configured agent when the route and conditions match.
  - outbound-translation-action—Tells the system to perform the configured outbound translation when the route and conditions match.

Policies allow for both multiple conditions and actions. All conditions must be met for the condition to be true. Alternatively, the user can configure no conditions, meaning the policy's condition is always true. When a policy includes multiple actions, it performs all of the actions in the configured order.

The user may also need to create route(s) specific to the policy. Whether an existing or newly configured route, the user configures the route to use one or more policies to complete the application configuration.

The Redirect Action

The redirect action causes the Oracle Enterprise Communications Broker (ECB) to redirect the incoming call through a particular agent by way of policy. You can use redirect to send a call to an external resource or service, such as a transcoding Session Border Controller or a call-recorder.

When applied, the policy engine performs an additional routing lookup for the call to the specified redirect agent. The system pre-pends additional hops from the redirect to the hops that were already calculated for the current route. The redirect action adjusts the routes to send the call to the specified redirect agent first, and then to the call destination.

Redirect action configuration includes the**Hairpin signaling** field. When you enable **Hairpin signaling**, the ECB routes the call to the redirect agent first, then routes it back to the ECB before sending it to the original destination. Hairpin signaling ensures that the ECB can route the call even when the redirect agent cannot reach the final destination. Note that keeping **Hairpin signaling** disabled eliminates the extra hops and extra session required when the destination is reachable by the redirect agent.

The ECB uses the same source agent, calling number, and called number parameters as the original call to reach the redirect agent. Only the dest-agent parameter gets replaced with the redirect agent specified in the redirect policy action. Take special care with default routes or routes that use a wildcard in the dest-agent field because such routes can become part of the path to the redirect agent.

Note the following details when evaluating and configuring redirect action:

- Hops incurred by the redirect action do not affect the route cost. The system determines the route-set and order-set before the redirection takes place.
- The system does not evaluate policies applied to the redirect routes, which prevents redirection loops and other undesirable behavior.

- The system uses only the first (lowest cost) redirection path, which prevents the exponential increase of backup paths.
- You can configure redirection to agent groups, which operate normally.
- The system applies the same routing parameters of the call (source agent/number and dest number) to the redirection route lookup as the original route.
- The system does not use default routes ('*' for all match patterns) for redirection. When the ECB finds no valid routes for the redirect, the ECB rejects the call.

Defining a Custom Policy

The Policy icon, available from the Oracle Enterprise Communications Broker's Configuration screen, provides access to the policy list and configuration dialogs, allowing the user to define and manage policies.

The user must have clearly analyzed traffic patterns and message content before configuring a custom policy.

Prior to configuration, identify the traffic that requires conditional routing. In addition, identify the message contents and/or metadata that allows them to uniquely target the traffic. Having performed these tasks, follow the procedure below to define your policy.

1. Follow the path **Configuration** tab > **Policy** icon to navigate to the applicable dialogs.

   The Oracle Enterprise Communications Broker displays the policy list.

2. Select an existing policy for editing, or click the **Add** button to create a new custom policy.

   The Oracle Enterprise Communications Broker displays the **Add Policy entries** dialog.

3. **Name**—Enter a name for your policy.
4. **Description**—Enter descriptive text that adequately explains the purpose of your policy.
5. From the **Conditions** list box, select a condition for editing or click the **Add** button to create a condition for this policy. Choices include:

   - **codec-condition**
   - **time-condition**

   The Oracle Enterprise Communications Broker displays the appropriate condition configuration dialog.

6. If you selected **codec-condition**, the **Add Policy/codec-condition** dialog allows the user to set the following fields to define the condition.

   - **Name**—Enter a name for your codec condition.
   - The **Contains codecs** list box includes controls that allow the user to **Add**, **Edit** or **Delete** codecs. The user selects applicable codecs from the drop-down box on the ensuing dialogs or deletes the selected codec.
   - The **Missing codecs** list box includes controls that allow the user to **Add**, **Edit** or **Delete** codecs. The user selects applicable codecs from the drop-down box on the ensuing dialogs or delete the selected codec.

7. If you selected **time-condition**, the **Add Policy/time-condition** dialog allows the user to set the following fields to define the condition.

   - **Name**—Enter a name for your codec condition.

- The **Days** list box includes controls that allow the user to **Add**, **Edit** or **Delete** codecs. The user selects applicable day from the drop-down box on the ensuing dialogs or delete the selected codec.
- **Start time**—Specify the time of day in 24-hour format at which the condition begins to apply.
- **End time**—Specify the time of day in 24-hour format at which the condition no longer applies.

8. From the **Actions** list box, select an action for editing or click the **Add** button to create an action for this policy. Choices include:
   - **routing-action**
   - **redirect-action**
   - **outbound-translation-action**

   The Oracle Enterprise Communications Broker displays the appropriate condition configuration dialog.
9. If you selected **routing-action**, the **Add Policy/routing-action** dialog allows the user to set the following fields to define the action.
   - **Name**—Enter a name for your routing action.
   - **Routing mode**—The user selects the mode from the drop-down box. Applicable modes include:
     - deny
     - skip
     - stop-recurse
10. If you selected **redirect-action**, the **Add Policy/redirect-action** dialog allows the user to set the following fields to define the action.
    - **Name**—Enter a name for your redirect-action.
    - **Redirect to agent**—The user selects the applicable agent from the drop-down box.
    - **Hairpin signaling**—The user checks the checkbox to enable hairpin redirect.
11. If you selected **outbound-translation action**, the **Add Policy/outbound-translation action** dialog allows the user to set the following fields to define the action.
    - **Name**—Enter a name for your outbound-translation-action.
    - **Egress number translation mode**—Select the translation mode from the drop-down box. Applicable modes include:
      - E164
      - E164-no-plus
      - n-digit-dialing
      - no-country-code
      - pattern-only
    - **Number of digits for n-digit dialing**—If you selected n-digit-dialing as Number Translation Mode for this agent, use this field to specify how many digits the Oracle Enterprise Communications Broker must send to this agent.

- **Prepend prefix on egress**—Specify a prefix the Oracle Enterprise Communications Broker must send to this agent. An example of such a prefix is the digit 9, which may be required to allow outbound traffic.

12. Save and Activate your configuration.

The user must apply the policy to the Registrar and/or desired route(s) from the Oracle Enterprise Communications Broker's Registrar or route configuration dialogs.

Applying a Policy to a Route

The user configures an Oracle Enterprise Communications Broker route's Policy from the **Modify Routing entry** dialog. The dialog presents a list box titled **Policy**, with controls that allow the user to **Add**, **Edit** or **Delete** policies to the route. When the user clicks **Add**, the system presents a drop-down selection box displaying the names of all currently configured Policies. This list includes user-configured policies, as well as the system's pre-configured policies, Deny, Emergency and Stop-Recurse. The user selects the desired policy and clicks **OK**, **Add/Apply another** or **Cancel** to complete the procedure.

Applying a Policy to the Registrar

The user configures the Oracle Enterprise Communications Broker Registrar with a Policy from the **Modify Registrar settings** dialog. The dialog presents a list box titled **Policy**, with controls that allow the user to **Add**, **Edit** or **Delete** policies to the registrar. When the user clicks **Add**, the system presents a drop-down selection box displaying the names of all currently configured Policies. This list includes user-configured policies, as well as the system's pre-configured policies, Deny, Emergency and Stop-Recurse. The user selects the desired policy and clicks **OK**, **Add/Apply another** or **Cancel** to complete the procedure.

Configurations Using Policy

Application examples using policy as a primary construct are presented below. These application examples are valid for both the Small and Large Enterprise models as base configurations.

Configuration examples include:

- Priority Call Handling, Using Constraint Policy Action
- Transcoding, Using Redirect Policy Action
- Call Recording, Using Redirect Policy Action
- Domestic vs. International Call, Using Translation Action
- Deny Routes, Using Routing Action
- Stop Recurse Routes, Using Routing Action
- Skip Routes, Using Routing Action

Priority Call Handling

The Oracle Enterprise Communications Broker provides support for ensuring that high priority calls, such as 911 calls, are not constrained by system utilization thresholds. Non-priority calls are still subject to system constraint configuration. The user configures priority call behavior by creating a policy with the constraint-action, then applying that policy to the applicable routes.

The Oracle Enterprise Communications Broker applies this policy to the configured route, as well as every subsequent backup route, even if the backup routes are not configured with the policy.

The system ignores constraints, such as session and rate/burst limits, for calls that match the priority route. The **constraints-action** provides a built-in action called **IgnoreConstraints**. This action causes the policy to mark a call to ignore constraints. All conditions configured on the policy must be satisfied for the action to be applied. The constraints-action is special in that, when enabled, it sets the call to ignore constraints for ALL routes. This is necessary because backup routes may be utilized that are not specific to priority/emergency calls.

For example, an emergency call might first be routed to a 911 service, but on failure it would be sent to the PSTN. The call cannot be limited by constraints on the PSTN route.

The built-in **Emergency** policy is provided for user convenience, and uses the **IgnoreConstraints constraints-action**. This built-in policy can be edited, if desired.

Note that this setting does not affect the "Deny" and "StopRecurse" policies on routes. It is simply not known whether these policies are for constraining purposes or because the network infrastructure cannot support calls over those routes.

Priority Call Configurations

This example shows a policy configuration that excludes 911 calls from system constraints, ensuring that the system does not encumber the call delivery. The configuration below documents the built-in policy titled "Emergency" applied to a route for 911 calls.

Policy

Name	Description
Emergency	Built-in policy to ignore constraints for emergency or priority calls

Condition

Recall that the default condition, which requires no configuration, is to always apply the policy.

Action

Name	Enabled
IgnoreConstraints	Y

Example Route

In addition to the configurations above, the system needs this route.

Source Agent	Calling #	Destination Agent	Called #	Route	Cost	Policy
*	*	*	911	EmerSvc	0	Emergency

Transcoding and the Oracle Enterprise Communications Broker

Transcoding is the conversion of media streams' encoding between endpoints that use different codecs. The Oracle Enterprise Communications Broker allows the user to configure routing policies that identify session agents deployed for transcoding media sessions and redirect applicable signaling and media streams to those agents.

Transcoding Configurations

This example shows a policy configuration that identifies an offer that does not include PCMU or PCMA and routes the call to a Transcoding device, in this case an SBC, to ensure the media uses either PCMU or PCMA.

Policy

Name	Description
XcodePcmuPcma	Send calls that need transcoding to PCMU or PCMA to a transcoding SBC

Condition

Name	Contains Codecs	Missing Codecs
XcodePcmu		PCMU

Action

Name	Redirect to Agent	Hairpin signaling
XcodeRedirect	XcodeSBC	enabled

Example Route

In addition to the configurations above, the system includes this route.

Source Agent	Calling #	Destination Agent	Called #	Route	Cost	Policy
*	*	PBX	*	PBX	0	XcodePcmu

These configurations result in the system sending traffic that contains the PCMU codec to the PBX, and traffic without the PCMU codec to the XcodeSBC, back to the Oracle Enterprise Communications Broker and then to the PBX.

Multiple Outbound Translations

The Oracle Enterprise Communications Broker provides a means for refining outbound translation configurations using routing policy. Fixed outbound translation configuration is available at the agent level. Routing policy, however, includes an outbound translation action that takes precedence over agent and sip interface configuration and applies translation based on individual route matches.

Outbound Translation Configurations

This example shows an outbound translation configuration that configures E164 numbers for domestic calls, and E164-no-plus with 011 prepended for international calls. The example calls for two policies and two routes.

Policy

Name	Description
InternationalDialNA	North American international dialing
DomesticDialNA	North American domestic dialing

Condition

Recall that the default condition, which requires no configuration, is to always apply the policy.

Actions

Outbound Translation Action (InternationalDial)

Name	Egress number translation mode	Number of digits for n digit dialing	Prepend prefix on egress
InternationalDial	E164-no-plus	0	011

Outbound Translation Action (DomesticDial)

Name	Egress number translation mode	Number of digits for n digit dialing	Prepend prefix on egress
DomesticDial	E164	0	

Routes

In addition to the dial patterns above, the system needs two new routes.

Route#	Source Agent	Calling #	Destination Agent	Called #	Route	Cost	Policy
1	*	*	PSTN-NA	!1*	PSTN-NA	0	InternationalDialNA
2	*	*	PSTN-NA	1*	PSTN-NA	10	DomesticDialNA

Results

This configuration provides the results presented in the table below.

From	Dial String	Transformation	Result
*	15551234	15551234	Call is routed without dial string change
*	34555555	01134555555	Call is routed with dial string change

The system routes any call that includes a country code and does not begin with the digit "1" internationally, and with the applicable transformation.

Routing Action Configurations

The Oracle Enterprise Communications Broker includes three pre-configured **Policies** (based on the pre-configured **DenyAction**, **StopRecurseAction** and **IgnoreConstraints** routing actions) that the user can apply to routes. In addition, the pre-configured **Skip** routing action mode is available for easy Policy configuration, which the user can then apply to routes.

Modes for routing actions include:

- **Deny**—The Oracle Enterprise Communications Broker should not forward the call at all.
- **StopRecurse**—Stop trying backup routes if the current route fails.
- **Skip**—Do not try this route, based on condition; proceed to any backup options.

Deny Route Policy Configurations

This example shows a policy configuration that prevents the system from allowing the request's source to reach the destination. The configuration below documents the built-in policy titled "Deny" applied to an example route.

The **Deny** policy in any resultant SIP routes to a destination prevents the Oracle Enterprise Communications Broker from forwarding a SIP request to the destination point in question. The user can use the **Deny** policy to prevent sessions between two endpoints for policy or cost reasons.

The Oracle Enterprise Communications Broker includes a pre-configured deny route policy that can be used without modification.

Policy

Name	Description
Deny	Built-in policy to deny the incoming session

Condition

Recall that the default condition, which requires no configuration, is to always apply the policy.

Action

Name	Routing Mode
DenyAction	deny

Example Route

In addition to the configurations above, consider the policy applied against this route.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Class_B	*	Protect_Agnt	*	Transit_Agnt	0	Deny

The user has configured this route entry to prevent calls passing through the agent named `Class_B` from reaching any endpoint behind `Protect_Agnt`. This route entry may be installed as part of one or multiple routes that could potentially reach `Protect_Agnt`.

Having assembled these routes, however, the routing engine recognizes the presence of this entry and rejects the call.

In addition, the system applies this Deny regardless of the backup route on which it is specified.

Stop Recurse Route Policy Configurations

This example shows a policy configuration that prevents the system from recursing through ensuing backup routes if the route configured with this policy fails. The configuration below documents the built-in policy titled "StopRecurse" applied to an example route.

A Stop-Recurse hop stops further attempts to forward a SIP request to a destination once the system has tried the route with the Stop-Recurse hop. The Stop-Recurse hop can be used to prevent calls from being forwarded on certain routes that are cost-prohibitive or could cause loops in SIP call flows.

The Oracle Enterprise Communications Broker includes a pre-configured stop recurse policy, with Routing Action being applied.

Policy

Name	Description
StopRecurse	Built-in policy to prevent further backup route attempts

Condition

Recall that the default condition, which requires no configuration, is to always apply the policy.

Action

Name	Routing Mode
StopRecurse	stop-recurse

Example Route

To expand upon the example, consider this route.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Class_A	*	Protect_Agnt	*	Transit_Agnt	0	StopRecurse

The user is allowing traffic to reach `Protect_Agnt` as long as it originates via the agent named `Class_A`.

For example, consider the case where an endpoint can be reached using two routes.

- Route 1: Agent_1 > Agent_2 (**StopRecurse**) > PBX
- Route 2: Agent_1 > PSTN

Route 1 has a **StopRecurse** policy defined on the hop between Agent_2 and PBX. The Oracle Enterprise Communications Broker stops processing the call if Route 1 does not receive a successful response. This configuration can prevent calls initially targeted for Route 1 from using the PSTN.

Skip Route Policy Configurations

This example shows a policy configuration that prevents the system from using this route based on condition. The policy contrasts with StopRecurse in that the routing engine is free to recurse through other routing options after skipping.

The Oracle Enterprise Communications Broker includes a pre-configured Skip Action, which the user can select to define their policy.

Policy

Name	Description
MySkip	Do not use this route, depending on condition.

Condition

The Time Condition Fields set below invoke the skip policy on weekdays from 9am to 5pm.

Name	Days	Start Time	End Time
When to enforce MySkip	Monday, Tuesday, Wednesday, Thursday, Friday	09:00:00	16:59:59

Action

Name	Routing Mode
SkipRoute	skip

Example Route

In addition to the configurations above, the user applies the policy against target routes.

Source Agent	Calling Number	Destination Agent	Called Number	Route	Cost	Policy
Class_B	*	Protect_Agnt	*	Transit_Agnt	0	MySkip

The resultant configuration prevents the system from using this route to **Transit_Agnt** as a means of reaching **Protect_Agnt** on weekdays from 9 to 5.

Resolving to the Longest Match in the User Database

The Oracle Enterprise Communications Broker user database supports resolution of overlapping numbers during lookups by selecting entries that have the longest matches.

Flexibility within the means of creating user database records allows for overlapping records, which can create ambiguity when the Oracle Enterprise Communications Broker looks for a match. To resolve this ambiguity, the Oracle Enterprise Communications Broker selects the entry that matches the most digits. This flexibility imposes the requirement on the administrator to manage user database entries that take advantage of this matching as well as prevent ambiguity.

The table shows a set of overlapping user number entries in the user database. The corresponding match length for each is determined by how many digits can match exactly. Number ranges and wildcards are not part of the match length.

Pattern	Match Length
17815551111	11
17815551[000-999]	8
17815551[111-999]	8
17815551xxx	8
1781555(x)xxx	7
xxxxxxxxxxx	0

When performing a user database lookup, the system uses the entry that matches the pattern with the longest match length. The table below provides an explanation on how different dialed numbers match the numbers configured in the user database.

Dialed Number	Matching Pattern	Reason
17815551111	17815551111	This number matches all patterns, however, this is an exact match and has the highest match length (11).
17815551112	17815551[000-999] or 17815551[111-999] or 17815551xxx	This number matches all but the first pattern. Three patterns have the longest match length of 8. The selection between them is ambiguous, and therefore undefined.
17815552111	1781555(x)xxx	This number matches only the last two patterns, but this pattern has a higher match length (7).
22222222222	xxxxxxxxxxx	This number only matches the last pattern.

As shown above, if multiple entries have the same match length, the selection between them is undefined and causes the lookup to fail. This ambiguity must be resolved by careful user database entry configuration.

Fork Groups

Fork-groups on the Oracle Enterprise Communications Broker are sets of one or more contacts that the system attempts to reach simultaneously. The system uses fork group order to specify when it tries to reach each fork group's contacts. This results in a hybrid of serial and parallel forking operation. The user can configure fork groups on agents, the registration cache and within the LDAP database. The user can also configure a global fork group timer with a value from 0 to 32 seconds on the sip-interface. If the system does not receive a response from any contact within that time, it tries the next fork group. Parallel forking must be enabled.

By default, the Oracle Enterprise Communications Broker assigns all contacts to fork group 1 and attempts to contact them serially, using the order in which it learns them. If desired, the user can enable parallel forking. By itself, parallel forking causes the system to attempt to reach all contacts simultaneously. Fork groups refine parallel forking, allowing the system to try all contacts in a group, and then move on to the next group.

The user names fork groups using decimal numbers between 1 and 100. This naming defines fork group order, with the system using fork group 1 first. The user configures objects with fork group numbers, based on a forking plan they devise.

The user can also configure a lookup query to LDAP databases to retrieve individual contacts' fork groups. The user must have previously modified the LDAP database to include a custom fork group field in contact records.

A use case for this feature could include the system attempting to reach a user's BYOD and desk phone simultaneously, then forwarding to an enterprise-preferred voicemail server if neither answers. For this to work, the BYOD and desk phone would be in the same fork group. The voicemail server would be a member of a higher numbered fork group. To ensure this order, the system assigns lower numbered fork groups with a higher precedence.

After establishing a session, other contacts may respond to try and start the session themselves. The Oracle Enterprise Communications Broker replies to these messages with a CANCEL.

Fork group operation does not exclude the use of primary and backup routes. The Oracle Enterprise Communications Broker still creates route sets for all contacts. If a contact fails via a primary route, the system attempts to reach the contact using all backup routes, based on cost.

If the Oracle Enterprise Communications Broker receives a redirect from an endpoint, the system adds the redirect target to the current fork-group and tries to contact it before attempting the next fork-group. If the global fork group timer expires before the system receives a redirect, however, the system proceeds to the next fork group.

The flexibility inherent in fork group operation requires the user to carefully plan forking prior to configuration. For each call, the system creates an ordered contact list, based on fork group configuration. Because the fork group assignment may affect multiple contacts, such as agent configuration, the user must be careful not to configure a sequence that would adversely affect calls to different end stations behind that agent.

Fork Group Assignment

The user configures fork groups to specify call attempt order for a given call. The Oracle Enterprise Communications Broker creates these call attempt lists based on each contact's fork group assignment.

Upon configuration, the system assigns fork groups to target endpoints as follows:

- User database—Each user database entry is assigned to the home-agent's fork-group.
- Registration cache—Each registration cache entry is assigned to the SIP registrar's fork-group.
- LDAP server—Each contact retrieved from an LDAP server is assigned to the a fork-group specified in the server's user record. If no fork-group was configured for the user in the Active Directory, the system assigns the target endpoint to the fork-group of the user's home-agent, as configured on the LDAP server.

Recall the contact source order used by the Oracle Enterprise Communications Broker:

1. Registration cache contact(s)
2. User database contact
3. LDAP contact(s)
4. LDAP AORs generating subsequent contact dips for additional registration cache contact(s)

By default, the Oracle Enterprise Communications Broker collects contacts from these sources and creates a contact list that follows the order in which the system learns them. This behavior is in accordance with default fork group operation, wherein all contacts are in fork group 1 and the mode is to fork serially only. As soon as the system finds differentiation between contact fork groups, however, it arranges contact lists using the fork group order.

Additional Targets

The user may want to include forking targets to stations that are not resolved as original call targets. Examples of these scenarios include directing calls to a preferred enterprise voice mail server if they are not picked up. The Oracle Enterprise Communications Broker provides for this using Additional target configurations. The user manually configures these devices within **Additional target groups**, which include one or more end stations. Agent and registrar configuration allows the user to select these groups as additional forking targets for all calls that use that agent or registrar's entries.

An additional target group is a list of agents (or endstations) that the Oracle Enterprise Communications Broker uses as candidates for either parallel or serial forking. The user configures these groups with fork group numbers, which the system then uses to define fork group order. The system adds additional target contacts to the forking sequence the same way it adds contacts for other objects with fork group configurations.

Configuring Fork Groups

Fork Group configuration requires that the user establish a clear plan prior to any configuration. Configurations established by this planning may include:

- The user may identify or create new agents as fork group targets.
- The user may identify usage and precedence policy for forking via the Registrar.
- The user may adjust fork group identification and precedence based on preferred LDAP lookup scenarios.

Coordinating the use of these sources and configuring the applicable objects establishes and refines fork group configuration. Applicable configuration objects include:

- Agent—The user creates new agents specifically for use in a fork group, or uses existing agents. The user configures an agent with a single fork group number, which the system applies to every call using that agent as a route.
- Additional targets—The user creates sets of targets to manually establish forking targets.
- Registrar—The user sets the registrar to a single fork group, which the system applies to every contact in the registrar.
- LDAP—The user defines a lookup query that pulls the pre-configured fork group assignment defined for the queried contact. The query must pull this fork group assignment from a custom attribute established on the LDAP database.

Configuring Fork Groups on Agents

The **Configuration tab** > **Agent** navigation sequence brings the user to the **Configure Agent** list. Each list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.

1. Click **Add** to create a new agent or **Edit** to add the agent to a fork group.

   The system displays the **Modify Agents** dialog.

2. **Additional target group**—Select and existing target group from the drop down list.
3. **Fork group**—Enter a digit (1-100) to specify this agent's fork group assignment.

Configuring Additional Target Groups

Additional targets are agents (or endstations) that are not contacts already targeted by a given call.

The user assigns additional target groups on a per-agent and a per-registrar basis.

The **Configuration tab** > **Agents** > **Additional Target Group** navigation sequence brings the user to the **Additional Target** list. This list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.

1. Click the **Add** link.

   The system displays the **Add Additional Target** dialog.
2. **Name**—Enter a name for this target. Use this name to assign this group to an agent or the registrar.
3. Note the Additional target group list.

   This list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.
4. Click the **Add** link.

   The system displays the subsequent **Add Additional Target** dialog. This list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.
5. **Additional session agent**—Select and existing target group from the drop down list, or enter an IP address of a target station.
6. **Fork group**—Enter a digit (1-100) to specify this agent's fork group assignment.

Assign your Additional Target Groups to the appropriate agent(s) and/or the registrar.

Configuring Fork Groups on a Registrar

The **Configuration tab** > **Registrar** > navigation sequence brings the user to the Registrar configuration dialog, which includes the Fork Group configuration fields.

1. **Additional target group**—Select and existing target group from the drop down list.
2. **Fork group**—Enter a digit (1-100) to specify the fork group for every contact in the registrar.

Configuring LDAP for Fork Groups

This procedure assumes the user has already defined and populated the custom LDAP attribute for specifying a user's fork group.

The **Configuration tab** > **LDAP** > navigation sequence brings the user to the LDAP server list. The list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.

1. Click **Edit**.

   The system displays the **Add LDAP config** dialog.
2. Scroll to the **Lookup queries** list. The list includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links.

3. Click **Add** to create a new lookup query.

   The system displays the **Add lookup query** dialog.

4. Referring to the **Fork group attribute** field, enter the name of the custom attribute in the LDAP database that includes fork group assignments.

Configuring the Global Fork Group Timer

The **Configuration tab** > **SIP Interface** > navigation sequence brings the user to the SIP Interface configuration dialog, which includes the global Fork Group timer configuration field.

1. **Fork group timer**—Enter a time in seconds (0-32) to specify the timeout the system uses to wait for responses from a fork group before it begins to try contacts the 'next' fork group. The default is zero (0). When set to default, the system waits for the standard SIP INVITE transaction timeout to expire before proceeding with the next group.

   After this timeout, the system drops responses received from contacts in the expired fork group.

LDAP Client Configuration

The Oracle Enterprise Communications Broker supports LDAP as a communications mechanism for interaction with one or more LDAP servers. For many enterprises, this means utilizing Active Directory, a common LDAP-based service, to request information used in SIP session routing and authentication. The Oracle Enterprise Communications Broker's LDAP client requires configuration on the Oracle Enterprise Communications Broker and the LDAP server.

Configuration aspects of LDAP client configuration include:

- LDAP server access—The user specifies LDAP server location and access preferences.
- Routing queries—The user specifies the conditions wherein the Oracle Enterprise Communications Broker performs an LDAP dip to obtain location information (home agent) for FROM and REQUEST-URIs.
- AoR queries—Optionally searches for additional AoR matches in Active Directory so that it can create additional routes to target users that have contacts stored in separate records.
- SIP Authentication queries—As an optional registration authentication mechanism, LDAP client configuration can utilize domain authentication or customized authentication server configuration on the LDAP server, as follows:
  - The use of domain authentication requires an application be installed on the domain controller.
  - Customized authentication requires the specification of compatible authentication fields on both client and server.

LDAP Configuration Options

The Oracle Enterprise Communications Broker provides options for LDAP configuration. These options provide the user with the flexibility to implement lookup precedence and preference on a per-agent and global basis.

An overall LDAP configuration on the Oracle Enterprise Communications Broker can include the following types of configurations.

- LDAP Config—A configuration that reaches one or multiple LDAP servers that refer to the same search base, use the same credentials, and typically service the same domain. The user can apply these configuration to agents.
- Global Config—A special LDAP configuration that the system uses as a default LDAP Config. When enabled, the system uses this LDAP Config for agents that are not configured with an LDAP Config or LDAP Group. The user cannot rename or delete the Global Config.
- LDAP Group—Multiple LDAP configs grouped together that allow the user to refine LDAP lookups across disparate LDAP domains.

The Oracle Enterprise Communications Broker's operational precedence for using your LDAP configuration on a per call basis is as follows:

1. If the applicable agent has an LDAP group applied, calls from that agent use the group configuration.
2. If the applicable agent does not have an LDAP group configuration, but does have an LDAP Config applied, calls from that agent use the LDAP Config.
3. If the call arrives on an agent without any LDAP configuration, calls from that agent use the Global LDAP configuration.

The Global LDAP configuration is disabled by default. This, in conjunction with the absence of any LDAP Configs, excludes the use of LDAP.

Making Settings

The Oracle Enterprise Communications Broker provides access to configuration fields via lists on the GUI.

When the user clicks the LDAP icon, the system displays a navigation pane on the left side of the screen, which includes the following links:

- LDAP
- Groups

When the LDAP link is selected, they system displays the list of currently configured LDAP Configs, including the Global Config. See the *Oracle® Enterprise Communications Broker User's Guide*, Release P-CZ2.0.0 for instructions on configuring LDAP Config fields.

Clicking the Groups link displays the LDAP Groups list, from which the user configures LDAP Groups.

LDAP Groups

LDAP groups on the Oracle Enterprise Communications Broker group **LDAP configs** together, allowing the user to refine lookups to multiple LDAP servers. The user configures **LDAP groups**, defines the matching criteria by which the system selects servers to query, and applies LDAP groups as profiles to agents.

When the system determines that it may find information it needs in the LDAP database, it checks to see if there is an **LDAP group** configured on the applicable agent. If there is no group, the system uses the LDAP configuration to control its lookups. This configuration can include a single LDAP Config configured on the agent or a Global LDAP config. If there is a group, the system:

1. Checks the matching criteria in the group to identify relevant LDAP servers, and

2. Performs lookups to relevant servers `using the order that the administrator has configured in the group.

If there is no match with any of the group's servers, the system does not perform an LDAP lookup and proceeds with the process sequence is uses to find information.

Matching Criteria in LDAP Groups

The Oracle Enterprise Communications Broker uses user-configured **Matching Criteria** to determine whether it should perform a lookup to each server in an **LDAP Group**. The Oracle Enterprise Communications Broker supports regex expressions within matching criteria configuration.

The system evaluates matching criteria for all LDAP servers listed in the group. If there are no matches, the system proceeds without querying LDAP. If there are any matches, the system initiates lookups to servers in the order listed in the group. If there is no match, the system skips those servers entirely.

Consider the example wherein the system performs a lookup for an phone number in LDAPGroup1. Recall that the **LDAP Group** selection is based on the agent configuration of the applicable end station. In this case, the LDAP1 agent configuration specifies LDAPGroup1 as its **LDAP group**.

The user has configured the first lookups within LDAPGroup1 to be directed to LDAP1 itself. If the number matches a criteria entry, the system adds that server to the lookup list. If not, the system skips to the next servers in the group, evaluating their **Matching Criteria**.

Matching criteria for LDAPGroup1 could include these entries.

Matching Criteria	LDAP Server
+1*	LDAP1
*@Div1.com	LDAP1
.*	LDAP2
+44*	LDAP3
+34555*	LDAP3

For LdapGroup1, the system queries LDAP1 only if the number starts with a +1 or has a host of Div1.com. The system queries LDAP2 in all cases based on its wildcard criteria. The system queries LDAP3 if the called number has a UK area code or has a Spain area code, then starts with 555.

Configuring LDAP Groups

The user must have configured LDAP configs before they can configure LDAP groups.

Follow the procedure below to create a new LDAP group:

1. Navigate to the LDAP group configuration dialogs using the sequence **Configuration** tab > **LDAP** icon > **Groups** link.

   The Oracle Enterprise Communications Broker displays the Modify LDAP group list, which includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links

2. Click the **Add** button to create a new custom policy.

The Oracle ECB displays the **Add LDAP group** dialog.

3. **Group name**—Type a name for this group into the field. The name must be between 1 and 128 alpha-numeric characters without spaces, and can include the underscore, comma, period and dash characters, as long as those are not the first characters in the name.

   The system makes this name available within all LDAP group drop-down selection boxes.

4. **Description**—Type a description for this monitor in the text box.
5. **State**—Check this checkbox to enable your LDAP group
6. The system includes the LDAP agents listbox along with the fields. This listbox includes standard **Add**, **Edit**, **Copy**, **Delete** and **Delete All** command links from which the user can access the LDAP agent dialog. Click the **Add** link to create a new group.

   The system displays the **LDAP Agents** dialog.

7. Select the desired LDAP configuration from the **LDAP config** dropdown selection box.
8. **Matching criteria**—Define the criteria the system must use to determine whether it should perform a lookup in the associated server for end station information. Regex is supported as a means of configuring matching strings.
9. Click OK to complete this configuration.
10. Save and activate your configuration.

Apply your LDAP group to the applicable Agent(s) from the **LDAP** dropdown list under the Agent's controls.

SIP REFER on the Oracle Enterprise Communications Broker

SIP REFER provides the Oracle Enterprise Communications Broker with the ability to terminate SIP REFER messages and perform attended or unattended call transfers. The user can enable REFER termination at both the agent and SIP interface, with agent configuration taking precedence. In addition the user can configure SIP interface with support for sending NOTIFY messages for provisional responses.

The following sections explain in detail the components of SIP REFER implemented on the Oracle Enterprise Communications Broker.

SIP REFER Method Call Transfer for ECB

The Oracle Enterprise Communications Broker supports a handling mode for the REFER method that automatically converts a received REFER method into an INVITE method. This allows the Oracle Enterprise Communications Broker to transfer a call without having to proxy the REFER back to the other UA.

The Oracle Enterprise Communications Broker has a configuration parameter giving it the ability to provision the handling of REFER methods as call transfers. The parameter is called **Enable REFER termination**. When this feature is enabled, the Oracle Enterprise Communications Broker creates an INVITE message whenever it receives a REFER. The Oracle Enterprise Communications Broker sends this INVITE message to the address in the Refer-To header. Included in the INVITE message is all the unmodified information contained in the REFER message. The previously negotiated SDP is used in the new INVITE message. NOTIFY and BYE messages are sent to the UA upon call transfer completion. The user

configures this function at the SIP interface or agent with agent configuration taking precedence.

If a REFER method is received containing no Referred-By header, the Oracle Enterprise Communications Broker adds one, allowing the Oracle Enterprise Communications Broker to support all call agent screen applications.

This SIP REFER method call transfer feature supports the following:

- Both unattended and attended call transfers.
- Both successful and unsuccessful call transfers.
- Early media from the Referred-To party to the transferee.
- REFER method transfer from different sources.
- The REFER event package as defined in RFC 3515. This applies for situations where multiple REFER methods are used within a single dialog.
- Third party initiated REFER method signalling the transfer of a call by associating the REFER method to the dialogue via the REFER TargetDialog.

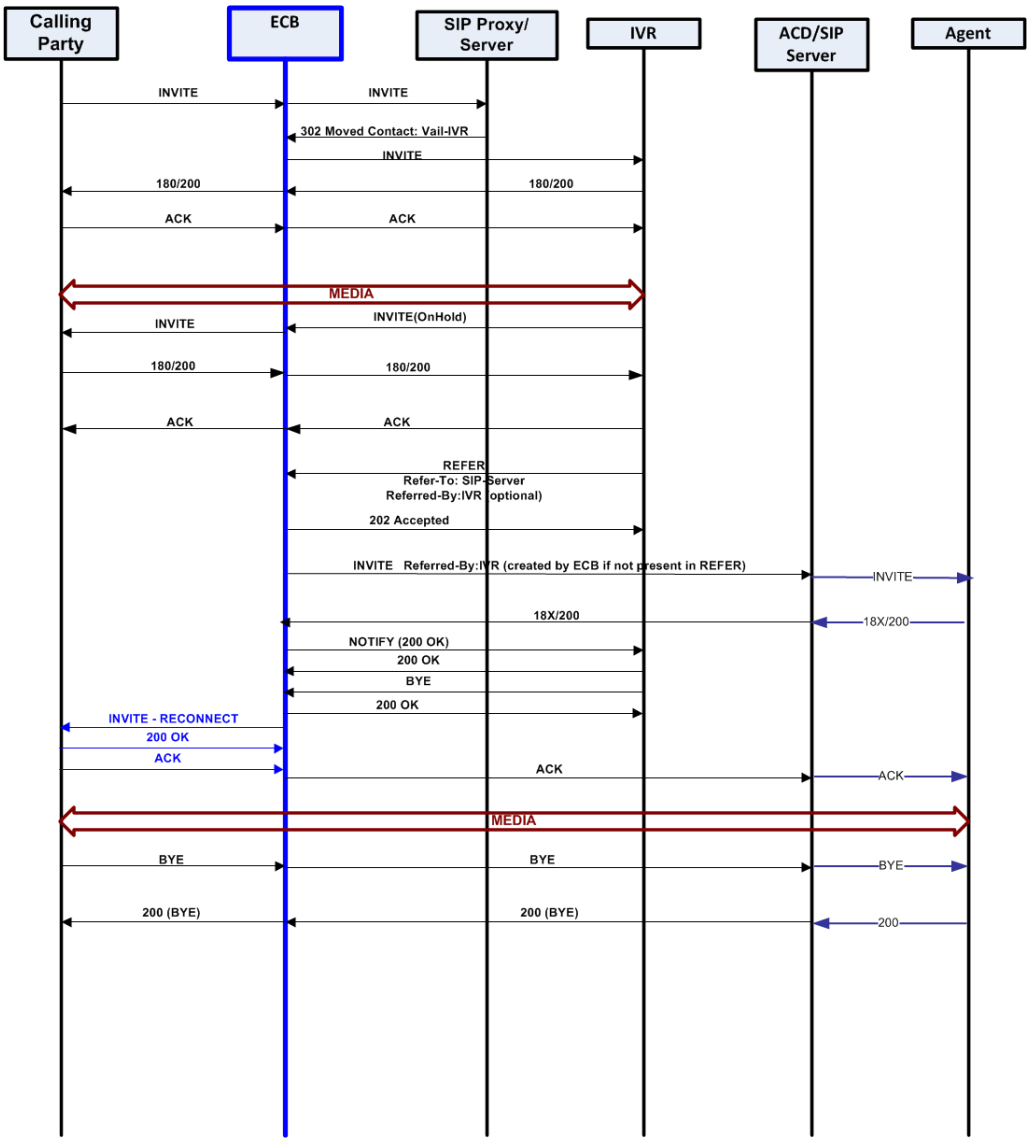
Unsuccessful Transfer Scenarios

The Oracle Enterprise Communications Broker does not successfully handle the following failed, unusual, and unexpected transfer scenarios:

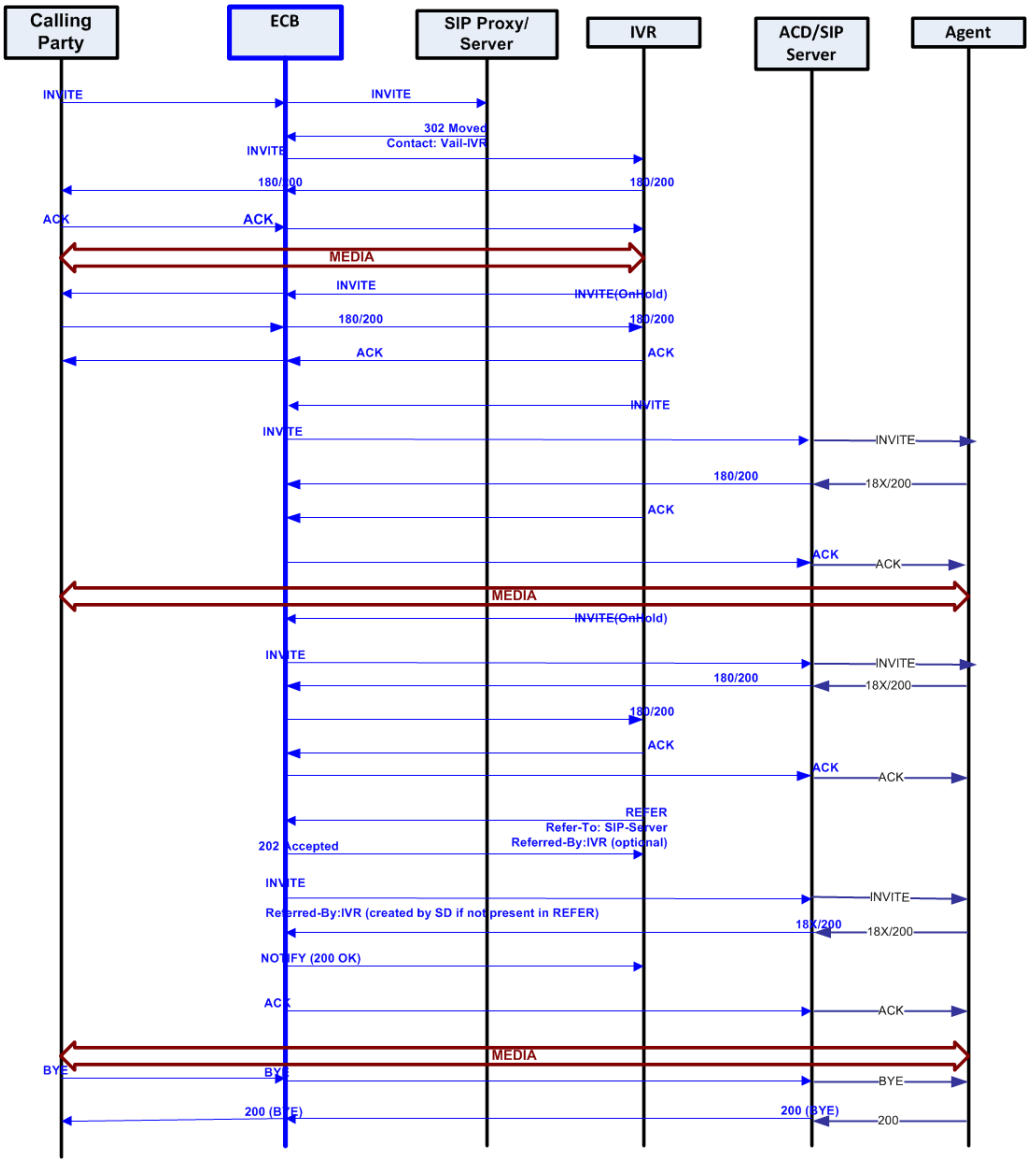
- The new INVITE to the Referred-To party gets challenged, the Oracle Enterprise Communications Broker does not answer the challenge. It is treated with the 401/407 response just as any other unsuccessful final response.
- The header of the REFER message contains a method other than INVITE or contains URI-parameters or embedded headers not supported by the Oracle Enterprise Communications Broker.
- The Oracle Enterprise Communications Broker shall allow the Referred-To URI that happens to resolve to the same next-hop as the original INVITE went to, to do so.
- The Oracle Enterprise Communications Broker ignores any MIME attachment(s) within a REFER method.
- The Oracle Enterprise Communications Broker recurses (when configured to do so) when the new INVITE sent to the Referred-To party receives a 3xx response.
- The transferee indicated support for 100rel, and the original two parties agreed on using it, yet the Referred-To party does not support it.
- The original parties negotiated SRTP keys.
- The original parties agreed on a codec using a dynamic payload type, and the Referred-To party happens to use a different dynamic payload number for that codec.

Call Flows

The following is an example call flow for an unattended call transfer:



The following is an example call flow of an attended call transfer:



SIP REFER Method Configuration

The Oracle Enterprise Communications Broker allows the user to set REFER termination on a per-agent and/or SIP interface basis. Agent configuration takes precedence over SIP interface configuration.

SIP Interface configuration includes the **Enable REFER termination** checkbox. The user checks the **Enable REFER termination** checkbox to allow this agent to support SIP REFER method call transfers.

Follow the procedure below to enable SIP REFER termination support, setting the SIP interface first, if applicable to your deployment:

1. Navigate to the SIP Interface's SIP REFER configuration fields using the sequence **Configuration** tab > **SIP Interface** icon.

   The Oracle Enterprise Communications Broker displays the **Modify Interface settings** dialog.

2. Locate and check the **Enable REFER termination** checkbox.
3. Navigate to the SIP REFER configuration fields using the sequence **Configuration** tab > **Agent** icon > **Edit** link.

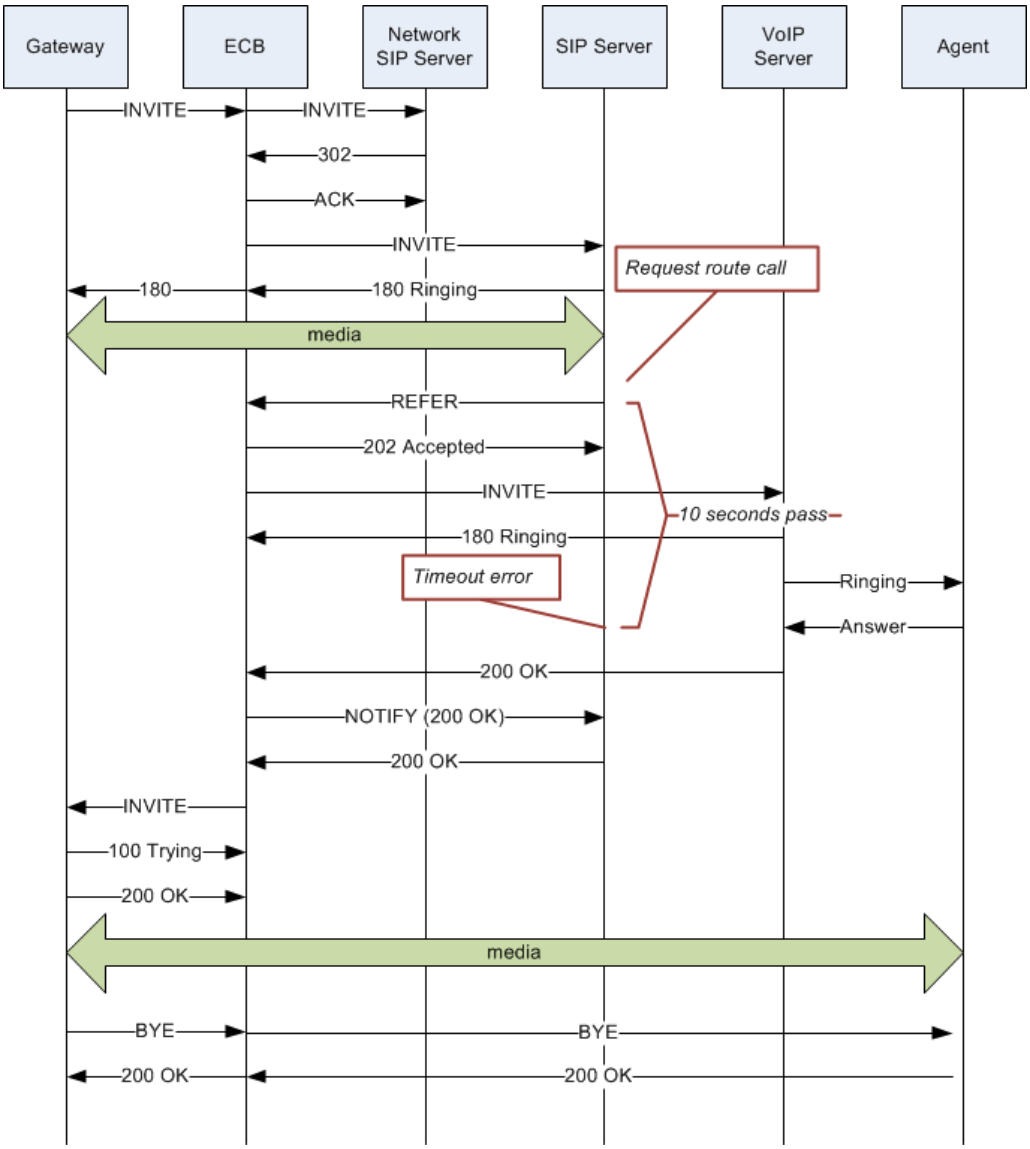
   The Oracle Enterprise Communications Broker displays the **Modify Agents** dialog.
4. Locate and check the **Enable REFER termination** checkbox.
5. Save and activate your configuration.

180 & 100 NOTIFY in REFER Call Transfers for ECB

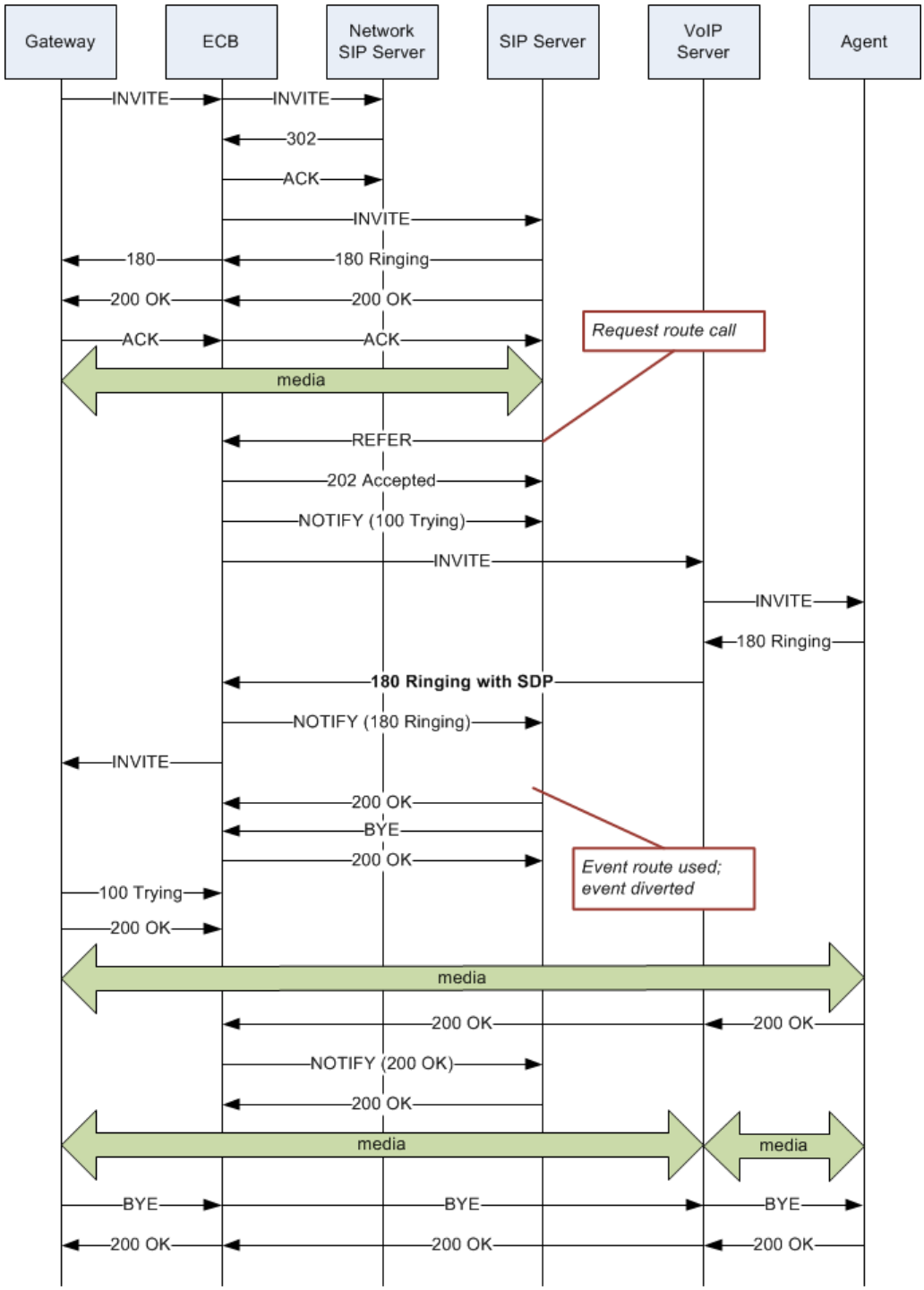
When you configure your Oracle Enterprise Communications Broker to support REFER call transfers, you can enable it to send a NOTIFY message after it has sent either a 202 Accepted or sent a 180 Ringing message. If your network contains elements that comply with RFC 5589, and so expect the NOTIFY message after the 202 Accepted and each provisional 180 Ringing, you want to set the **Send NOTIFY messages for REFER Provisional Responses** to either **initial** or **all**, according to your needs.

Without this parameter changed from its default (**none**), the Oracle Enterprise Communications Broker does not return send the NOTIFY until it receives the 200 OK response from the agent being called. If the time between the REFER and the NOTIFY exceeds time limits, this sequencing can cause the Oracle Enterprise Communications Broker's NOTIFY to go undetected by devices compliant with RFC 5589. Failures during the routing process can result.

You can see how a sample call flow works without setting the **Send NOTIFY messages for REFER Provisional Responses** parameter.



When you compare the call flow above to the one depicting the scenario when the Oracle Enterprise Communications Broker has the **Send NOTIFY messages for REFER Provisional Responses** changed from its default, you can see that the Oracle Enterprise Communications Broker now response with a NOTIFY in response to the 202 Accepted and it sends another after the 180 Ringing. This causes the event to be diverted successfully.



Sample Messages

In compliance with RFC 5589, the NOTIFY message with 100 Trying as the message body looks like the sample below. Note that the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
```

```
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 100 Trying
```

Also in compliance with RFC 5589, the NOTIFY message with 180 Ringing as the message body looks like the sample below. Again, the expires value in the subscription state header is populated with a value that equals 2* TIMER C, where the default value of TIMER C is 180000 milliseconds.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=360
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 180 Ringing
```

Also in compliance with RFC 5589, the NOTIFY message with 200 OK as the message body looks like the sample below.

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 74 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: terminated;reason=noresource
Content-Type: message/sipfrag
Content-Length: ...
SIP/2.0 200 OK
```

180 and 100 NOTIFY Configuration

You can apply the **Send NOTIFY messages for REFER Provisional Responses** setting to the sip-interface. By default, the Oracle Enterprise Communications Broker only sends the final result NOTIFY message.

To enable 100 and 180 NOTIFY messages in REFER call transfers:

1. Navigate to the SIP Interface's SIP REFER configuration fields using the sequence **Configuration** tab > **SIP Interface** icon.

   The Oracle Enterprise Communications Broker displays the **Modify Interface settings** dialog.

2. Locate the **Send NOTIFY messages for REFER Provisional Responses** and choose from one of the following settings, where the Oracle Enterprise Communications Broker:

   - **None**—Disable NOTIFY for REFER provisional responses.
   - **initial**—Sends an immediate 100 Trying NOTIFY, and the final result NOTIFY.
   - **all**—Sends an immediate 100 Trying NOTIFY, plus a notify for each non-100 provisional messages the Oracle Enterprise Communications Broker receives; and the final result NOTIFY.

3. Save and activate your configuration.

TOS Marking

The Oracle Enterprise Communications Broker provides RFC 2474 compliant Type of Service (TOS) marking as a mechanism to prioritize traffic. The user configures a single TOS marking for all traffic (SIP signaling) on a SIP interface, which the Oracle Enterprise Communications Broker inserts into all of this interface's egress traffic. Upstream devices use these markings to prioritize traffic. Configuration consists of the user enabling TOS marking and setting the value that the Oracle Enterprise Communications Broker inserts in all traffic.

The user sets the following parameters from the Configuration tab's **SIP Interface** icon to configure TOS marking on that interface.

- **Enable TOS marking**—Checking this checkbox enables the function, causing the system to insert RFC 2474 compliant TOS marking in all of this interface's egress traffic.
- **TOS value**—The user manually types the TOS value for traffic in decimal or hexadecimal format. This determines the RFC 2474 compliant value that the Oracle Enterprise Communications Broker inserts in all of this interface's egress traffic.

The Oracle Enterprise Communications Broker's **TOS value** setting is agnostic to the RFC 2474-specified means of determining the value. The field allows the user to enter any hex value, requiring the user to ensure that it is correct.

Syslog Settings

Set the following parameters from the Configuration tab's **General** icon to configure system-wide Syslog functionality.

1. Syslog server IP address—Set the IP address of the server to which you are sending syslog messages from the Oracle Enterprise Communications Broker. Note that Syslog message log level is always **Warning**.

2. Syslog server port—Enter the port number on the syslog server to which the Oracle Enterprise Communications Broker sends log messages.

   - Range: 0 to 65535
   - Default: 514

3. Syslog facility—Enter the user-defined facility value sent in every syslog message from the Oracle Enterprise Communications Broker to the syslog server. This value must conform to IETF RFC 3164.
   - Range: 0 to 99999999
   - Default: 4
4. Process log level—Set the severity level of the process log messages. Debug is most verbose. Both Debug and Trace can adversely impact system performance; configure these levels temporarily and only when required.
   - Critical (2)
   - Minor (4)
   - Warning (5)
   - Notice (6)
   - Info (7)
   - Trace (8)
   - Debug (9)

Early Media Inhibit

The Oracle Enterprise Communications Broker's early media inhibit function extracts SDP from provisional responses and stores it. If the dialog's final 200OK does not include SDP, the Oracle Enterprise Communications Broker inserts the stored SDP into that 200 OK before forwarding. If the final 200 OK includes SDP, the Oracle Enterprise Communications Broker forwards the message unchanged. The user configures early media inhibit on a global (sip-interface) or per-agent basis.

An example call flow targeted by the early media inhibit function is forking. If end stations present SDP in provisional responses for call flows that include forking, this can result in an SDP negotiation between end stations that ultimately do not handle the call. Early media inhibit prevents this from happening.

The user sets **Early media inhibit** from the Configuration tab's **SIP Interface** or **Agent** icon to configure early media inhibit globally or on that agent.

- **Early media inhibit**—Checking this checkbox enables the function, causing the system to manage SDP insertion.

Command Line Interface (CLI) Widgets

Like many devices, the Oracle Enterprise Communications Broker includes an underlying management interface called the Command Line Interface (CLI). Support technicians use this CLI to display detailed information about the system in text format. Oracle makes this information available from the graphical user interface (GUI) with CLI Widgets, available from the Oracle Enterprise Communications Broker's widget tab. These widgets can provide useful troubleshooting information as well as insight into system operation.

The CLI portal is available from the Oracle Enterprise Communications Broker's Widgets tab. The navigation sequence from the left panel's widget list is **Command** > **CLI** > **CLI portal**. When the user clicks the CLI portal link, the Oracle Enterprise Communications Broker displays the Command line portal. The portal includes **Settings** and a **Results** panel.

CLI portal settings include:

Field Name	Description
Command	A pull-down selection box allowing the user to choose the CLI command. Available commands are presented below.
Parameter	A text box allowing the user to enter additional parameter text to refine the command output with a command argument.
Auto-refresh interval	A pull-down selection box allowing the user to specify how often the system refreshes the widget's data. Available settings, in seconds, include: • never • 30 • 40 • 50 • 60

The portal includes an OK and a Cancel button. When the user clicks OK, the system adds a CLI command output window into the **Results** panel below the **Settings**. Each CLI widget provides standard widget controls on their menu bar, including a button to make the widget visible on the dashboard.

The system produces two types of CLI widgets, depending on the command invoked:

- Text Display—The system displays the output of the command in an all-text format.
- Tabular Display—The system displays the output of these commands in a table.

The user can run additional CLI commands after the first one. The CLI portal stacks widgets in the **Results** panel, minimizing previous widgets below the new widget sequentially. By maximizing widgets, the user can scroll through the **Results** panel, effectively monitoring multiple command output information simultaneously.

The portal includes a **Remove All** button that allows the user to clear all widgets from the portal at the same time.

For command and output descriptions, see the CLI Portal Reference Appendix in this document.

CLI Display Timeouts

The Oracle Enterprise Communications Broker GUI provides configuration fields under the general icon that allows the user to set timeout values to both serial (console) and telnet sessions to the device. These sessions provide CLI management access to the Oracle Enterprise Communications Broker. If there is no activity on these sessions within the timeout period, the system closes the session.

The use of telnet and serial sessions to manage theOracle Enterprise Communications Broker is not recommended. There are troubleshooting and other procedures that may, however, include the use of CLI management sessions. The **console-timeout** and **telnet-timeout** configuration fields provide a means of securing those sessions by terminating them when they are not in use.

Navigate to the **console-timeout** and **telnet-timeout** configuration fields from the Configuration tab's **General** icon.

console-timeout—Enter the time in seconds the Oracle Enterprise Communications Broker 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
- ValuesMin: 0 / Max: 65535

telnet-timeout—Enter the time in seconds the Oracle Enterprise Communications Broker 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
- ValuesMin: 0 / Max: 65535

Issues Resolved

Documented issues resolved between Release PCZ2.0 M1 and Release PCZ2.0 M2 are listed below.

- The Broker widget now shows outbound translation information.
- When the user completes a record editing procedure from a live multi-instance table, the system now sets focus (item selection) to that record in the table.
- The system now generates Interim-Update records for Accounting.
- The **Set boot parameters** wizard no longer displays a reboot information dialog box whenever the user clicks the Complete button and the user has not made any changes.
- The Oracle ECB now forwards an in-dialog ACK request when the host part of the request-uri is a configured SIP registrar domain.
- The system now synchronizes LST files across Oracle ECBs in HA configurations.

3

PCZ2.0 M3

This chapter provides descriptions, explanations, and configuration information for the contents of Maintenance Release PCZ2.0 M3. Maintenance Release content supercedes that distributed with the previous point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.7
- P1.0.0

Current patch baseline: PCZ2.0.0 M2p1

Content Map

The following table identifies the new content in this PCZ2.0 M3 Maintenance Release documentation.

Content Type	Description
Behavioral Changes	Widget, Commands Menu, non-E.164 Number Normalization
Adaptation (Using Policy)	Configuring CNAM Replacement
Adaptation	Using Policy to Normalize SIP Headers
Application (Using Policy)	ANI Multi-header
Adaptation	Restricting Session Initiation
Adaptation	Proxy Registrations
Adaptation	Synchronizing the Registration Cache
GUI Adaptation	Audit Logs
Adaptation	License Widget
Defect Tracking	Issues Resolved

Behavioral Changes

Please review the following sections prior to using this software release.

Widget Layout Change

The **All Widgets** list and the widget tree now include the commands presented in the **CLI portal** widget.

Commands Menu

The **Configuration** tab now includes a **Commands** menu accompanying the **Save** and **Wizards** menus.

Non-E.164 Number Normalization

If a call comes from a non E164 number, the Oracle Enterprise Communications Brokerstrips all special (non-numeric) characters from the header, with the exception of the plus sign. In addition, the Oracle Enterprise Communications Broker does not perform outbound translations on non E164 numbers. Previously, the system also removed the + character.

Widgets Removed

This release no longer includes the following widgets:

- Answer and Seizure ratio line graph
- Answer and Seizure ratio table
- Established sessions line graph
- Established sessions table
- Requests per second line graph
- Requests per second table
- Response bar graph
- Response pie graph
- Response table
- Session duration bar graph
- Session duration table

Configuring CNAM Replacement

The Oracle Enterprise Communications Broker provides the user with the ability to specify the value of the caller name (CNAM) in the FROM header. A simple use case would consist of an enterprise inserting the name of their company into the FROM value, in place of the original caller name. The user configures the system to use other policy or routing configurations to determine when to replace a CNAM. The system applies this policy action on SIP requests immediately prior to egress.

To configure CNAM replacement, add the **cnam-masking-action** action to the desired policy. The **Modify Policy / cnam masking action** dialog includes two fields.

- **Name**—Assigns a name as an identifier to your action.

- **Display name**—Defines the text the Oracle Enterprise Communications Broker inserts as the CNAM value in the FROM header.

Note that, if no user name is in the original FROM, the Oracle Enterprise Communications Broker inserts text configured via the CNAM mask and encloses it in brackets per RFC 2822.

Using Policy to Normalize SIP Headers

The Oracle Enterprise Communications Broker supports policy-based SIP Header Normalization, allowing the user to copy and change information in headers when their user parts are Tel-URIs or SIP URIs composed of numbers. The system writes header changes caused by policy after any inbound and before any outbound manipulation performed by header manipulation rules. These policies work for registered users and targets derived from the user database or LDAP. The user configures header normalization policies from the Oracle Enterprise Communications Broker's **Policy** icon and applies them to routes and/or the Registrar. Routes support multiple policies.

The header normalization policy works with the existing outbound translation policy. Each policy consists of one or more rules by which the system changes headers to messages that match the routes or registrar to which the policy is configured. Multiple rules can be defined for the same SIP header. The system evaluates and executes rules in the configured order and changes the header values with each rule that has a valid **New value** field.

Header normalization configuration fields include:

- **SIP header name**—The name of the SIP header to be normalized. This field cannot be empty.
- **Dialing context**—Name of dialing context that defines the dialing rules to be applied to the phone number in this SIP header. An empty value in this field indicates that no dialing rules need to be applied to the corresponding SIP header in the rule.
- **Result name**—A temporary variable name to store the result of the dialing rules on the SIP header. This name has to be unique within this policy action. The value is saved between policy rule evaluation, but is not saved after the policy is fully evaluated.
- **New value**—The **Result name** whose value will be used as the new value of the SIP header. If this field is left empty, the system does not change the value of the SIP header.

If a rule specifies a SIP header name that is absent in the SIP request and the **New value** field has a valid **Result name**, the system adds the SIP header and set it to the value of **Result name**.

ANI Masking

The Oracle Enterprise Communications Broker provides a means for ensuring that the automatic number identification (ANI) presented to a service provider be recognized as a valid screened telephone number (STN) and, therefore, is not dropped by that service provider. The user configures this function as a Header Normalization policy that rewrites the applicable header with a recognizable STN. Applicable headers are DIVERSION, P-ASSERTED-IDENTIFY or FROM, depending on the service provider's requirements.

ANI Masking Configurations

This example shows a header normalization policy that ensures that the system presents an ANI as a valid STN. This assumes the user has created a dialing context from which the system can determine an STN.

Policy

Name	Description
ANI_Mask1	North American international dialing

Condition

The default condition, which requires no configuration, is to always apply the policy.

Actions

The example below configures the action named ANI_MaskforSP1, which is of the header-normalization-action element type with two actions.

SIP header name	Dialing context	Result Name	New value
From	find_Verizon_STN	STN	
Diversion		original_diversion	STN

The results of these actions follow.

1. Use the value of the "from" header and run it through a dialing context called "find_Verizon_STN" and store the result in a variable called "stn". Since new value field is empty the value of the "from" header is unaltered.
2. Since the dialing context is empty, copy value of the "Diversion" header to the variable called "original_diversion". If the incoming SIP request did not have a "Diversion" header "original_diversion" will be set to an empty string. Lastly, copy the value of the variable "STN" into the "Diversion" header.

Routes/Registrars

Configure either routes or registrars as triggers by setting their **Policy** fields to the **ANI_Mask1** policy.

Results

This configuration provides the results presented in the table below.

SIP Message Text	Mask Function	Result SIP Message Text
To: sip: 781.630.1111@oracle.com From: sip: 781.630.2222@oracle.com	Use Dialing context titled "find_Verizon_STN" to create new value titled "STN"	To: sip: 781.630.1111@oracle.com From: sip: 781.630.2222@oracle.com Diversion: sip: 978.528.1234@oracle.com

Restricting Session Initiation

The Oracle Enterprise Communications Broker can restrict the set of end stations that can initiate sessions to those originating via active session agents and previously registered users. By default, the Oracle Enterprise Communications Broker does not restrict session initiation. The user enables this functionality within the **sip-port**.

The Oracle Enterprise Communications Broker's **sip-port** configuration includes a checkbox titled **Allow session agents and registered end-points** with which the user can restrict session initiation. When checked, the Oracle Enterprise Communications Broker responds to session initiation by endpoints that are not behind an agent or not already registered with a **403: Unauthorized** message.

Proxy Registrations

The Oracle Enterprise Communications Broker can proxy registrations when it receives REGISTERs for domains for which it is not a registrar. The user enables this functionality within the **sip-interface**. By default, the Oracle Enterprise Communications Broker rejects the registration.

The Oracle Enterprise Communications Broker's **sip-interface** configuration includes a checkbox titled **Proxy Registrations**, with which the user can enable this function. When checked, the Oracle Enterprise Communications Broker proxies the registration towards the intended registrar. When unchecked, the Oracle Enterprise Communications Broker responds with a **403: Unauthorized** message.

Synchronizing the Registration Cache

ECB Sync data includes the Oracle Enterprise Communications Broker's registration cache. The user can enable registration cache sync via a checkbox within the Sync config settings under the ECB Sync icon.

When enabled, the Oracle Enterprise Communications Broker presents its registration cache to all ECB Synch agents every nine minutes. Each ECB Sync agent uses this data to create a separate, ECB Sync-only registration cache table that includes contacts and the ECB from which it learned the cache entry.

When a call comes for a contact found in the ECB Sync-only registration cache, the Oracle Enterprise Communications Broker receiving the call adds a URI parameter to the request URI of the TO header and forwards the message to the Oracle Enterprise Communications Broker in the table. This URI parameter informs the target Oracle Enterprise Communications Broker that is must only use its registration cache for routing this call. This parameter appears as follows.

```
TO sip:user2@server2.com;orcl-regonly=true
```

In these cases, both Oracle Enterprise Communications Brokers forward the call. The Oracle Enterprise Communications Broker receiving the call uses all other routing sources to route the call, including LDAP, LST and UserDB. The Sync agent Oracle Enterprise Communications Broker routes the call using its registration cache, and skips all other routing sources, including LDAP, LST and UserDB.

Audit Logs

The Oracle Enterprise Communications Broker (ECB) can record user actions in audit logs. The audit logs record the creation, modification, and deletion of all user-accessible configuration elements, as well as attempted access to critical security data such as public keys. For each logged event, the system provides the associated user-id, date, time, event type, and success or failure data.

You can specify how the system records audit log information, but not which information it records. You can configure the system to record in either verbose or brief mode. Verbose mode captures the system configuration after every change, and displays both the previous and new settings in addition to the event details. Brief mode displays only the event details.

As the ECB records audit log data, users with admin privileges can read, copy, and download that information from the Web GUI. No one can delete or edit the original log.

The audit log records the following actions:

Source	Actions Recorded
Global	• Log on and log off. • Save a template configuration. • Click **Complete** in a Wizard.
Home tab	• Add, reset, and save. • Change Widget settings.
Configuration tab	• Save and activate a configuration. • Discard a configuration. • Add, edit, delete, and copy configuration changes. • Run the generate and import certificate commands.
Widgets tab	• Export from a Widget. • Add a Widget to favorites. • Clear, clear all on alarm, add, and delete license.
System tab	• Add audit entries to the system file management actions, such as upload, download, restore, backup, add, edit, and delete. • Force an HA switch over. • Run the Show Support Information command. • Run the Upgrade Software wizard. • Download and view an audit log.
Monitor and Trace tab	• Export the summary. • Export the session detail.

Audit log events are Comma Separated Values (CSV) lists written in the following format:

```
{TimeStamp,
src-user@address:port,Category,EventType,Result,Resource,Prev,
Detail}
```

The following table describes each value written to an audit log event.

Log Element	Information Provided
TimeStamp	Shows the time when the system wrote the event to the audit log.
src-user@address:port	Identifies the system that wrote the audit log line.
Category	Classifies the event as: • Configuration • Security • System
EventType	Identifies the action that caused the event as: • Activate-config • Acquire-config • Create • Data-access • Delete • Halt • Login • Logout • Modify • Reboot • Save-config
Result	Identifies the outcome of the event as: • Failure • Success
Resource	Describes the action within the event. Some of the numerous actions that the system can log include: • Authentication • Banner (Means that someone edited the log on banner text.) • Download <filename> • Generate public key • Reboot • Upload <filename>
Prev—Displays only in verbose mode.	Displays the setting prior to this change.
Details	Displays additional information about the change, depending on the following event types: • Create—displays “New = element added." • Data-access—displays “Element = accessed element.” • Delete—displays “Element = deleted element.” • Modify—displays “Previous = oldValue New = newValue.”

Note that you can configure the system to transfer audit log files to an SFTP server by way of secure FTP push, when conditions satisfy one of the following specifications.

- The specified amount of time since the last transfer elapsed.
- The size of the audit log reached the specified threshold. (Measured in Megabytes)
- The size of the audit log reached the specified percentage of the allocated storage space.

The ECB transfers the audit logs to a designated directory on the target SFTP server. The audit log file is stored on the target SFTP server with a filename in the following format: **audit<timestamp>**. The timestamp is a 12-digit string the YYYYMMDDHHMM format.

Use the following configuration process:

1. Configure secure FTP push. See "Secure FTP Push Configuration."
2. Configure audit logging. See "Configure Audit Logging."

Secure FTP Push Configuration

You can configure the Oracle Enterprise Communications Broker (ECB) to securely send audit log files to an SFTP push receiver for storage. Configure secure FTP push before you configure audit logging.

You can configure the Oracle Enterprise Communications Broker (ECB) to log on to a push receiver using one of the following authentication methods to create a secure connection.

Password
Configure a username and password, and leave the **public-key** parameter blank. Note that you must also import the host key from the SFTP server to the ECB for this type of authentication.

Public key
Set the **public-key** parameter to a configured public key record name including an account **username**, and configure the SFTP server with the public key pair from the ECB.

It is also common for the SFTP server to run the Linux operating system. For Linux, the command ssh-keygen-e creates the public key that you need to import to the ECB. The ssh-keygen-e command sequence requires you to specify the file export type, as follows.

```
[linux-vpn-1 ~]# ssh-keygen -e
Enter file in which the key is (/root/.ssh/id_rsa/): /etc/ssh/
ssh_host_rsa_key.pub
```

If you cannot access the SFTP server directly, but you can access it from another Linux host, use the ssh-keyscan command to get the key. An example command line follows.

```
root@server:~$ssh-keyscan -t dsa sftp.server.com
```

Configure Secure FTP Push with Public Key Authentication

For increased security when sending files from the Oracle Enterprise Communications Broker (ECB) to an SFTP server, you can choose authentication by public key exchange rather than by password. To use a public key exchange, you must configure public key profiles on both devices and import the key from each device into the other.

The following list of tasks shows the process for configuring authentication by public key between the ECB and an SFTP server. For each step in the process, see the corresponding topic for detailed instructions.

1. Generate an RSA public key on the ECB. See "Generate an RSA Public Key."
2. Create a DSA public key on the SFTP server. See "Generate a DSA Public Key."
3. Import the DSA public key from the SFTP server into the ECB using the **known-host** option in the Import Key dialog. See "Import a DSA Public Key."
4. Add the RSA public key to the authorized_keys file in the .ssh directory on the SFTP server. See "Copy the RSA Public Key to the SFTP Server."

Generate an RSA Public Key

Add a public key profile on the Oracle Enterprise Communications Broker (ECB) and generate an RSA key. You will later import the RSA key into the SFTP server to enable authentication by way of public key exchange with the ECB.

To add a public key profile and generate an RSA public key:

1. Log on to the ECB and click **Configuration** > **Security** > **Public key**.
2. On the Public Key page, click **Add**.
3. In the Add Public Key dialog, do the following:

Attributes	Instructions
Name	Enter the name of this profile.
Type	Select RSA.
Size	Enter one of the following: • 1024 (default) • 2048 • 512

4. Click **OK** to create the public key profile.

   The system displays the Public Key list box including the new profile.
5. Save and activate the configuration.
6. Select the newly created profile, and click **Generate key**.

   The ECB displays the key in the Generate Key text box for you to copy to the SFTP server.
7. Save and Activate the configuration.

Next Steps

- Generate a DSA public key.

Generate a DSA Public Key

Generate and save a DSA public key on the SFTP server. You will later import the DSA key into the Oracle Enterprise Communications Broker (ECB) to enable authentication by way of public key exchange with the SFTP server.

To generate and save a DSA public key:

1. Run the following command on the SFTP server:
   ssh-keygen -e -f /etc/ssh/ssh_host_dsa_key.pub | tee sftp_host_dsa_key.pub
2. Save the key to the authorized_keys file in the .ssh directory on the SFTP server.

Next Steps

- Import the DSA key into the ECB.

Import a DSA Public Key

Import a DSA public key from the SFTP server into the Oracle Enterprise Communications Broker (ECB).

- Generate and save a DSA public key on the SFTP server.

Perform the following procedure on the ECB and select "known-host" for type.

To import the DSA public key:

1. Access the SSH file system on the SFTP server by way of a terminal emulation program.
2. On the SFTP server, copy the base64 encoded public file. Be sure to include the Begin and End markers, as specified by RFC 4716 *The Secure Shell (SSH) Public Key File Format*.

   For OpenSSH implementations host files are generally found at `/etc/ssh/ssh_host_dsa_key.pub`, or `/etc/ssh/sss_host_rsa.pub`. Other SSH implementations can differ.
3. On the ECB, click **Configuration** > **Security** > **Public Key**.
4. On the Public key page, click **Import key**, and do the following.

Attributes	Instructions
Type	Select known-host.
Name	Enter a name for your profile, which the ECB displays in public key drop-down lists.
SSH public key	Paste the DSA public key from the SFTP server into the text box. Ensure that the text of the key ends with a semi-colon.

5. Click **Import**.

   The ECB imports the key and makes it available for configuration as the public key on an external device.

Next Steps
Copy the RSA public key to the SFTP server.

Copy the RSA Public Key to the SFTP Server

Copy the RSA public key from the from the Oracle Enterprise Communications Broker (ECB) to the authorized_keys file in the .ssh directory on the SFTP server.

- Confirm that the .ssh directory exists on the SFTP server.
- Confirm the following permissions: Chmod 700 for .ssh and Chmod 600 for authorized_keys.

When adding the RSA key to the authorized_keys file, ensure that no spaces occur inside the key. Insert one space between the ssh-rsa prefix and the key. Insert one space between the key and the suffix. For example, ssh-rsa <key> root@1.1.1.1.

To copy the RSA key to the SFTP server:

1. Access the SSH file system on a configured SFTP server with a terminal emulation program.

2. Copy the RSA key to the SFTP server, using a text editor such as vi or emacs, and paste the RSA key to the end of the authorized_keys file.

Configure Audit Logging

The Oracle Enterprise Communications Broker (ECB) provides a means of tracking user actions through Audit Logs. You can specify how the system records audit log information, and where to send the logs for archiving. You can configure the system to record in either brief or verbose mode. Verbose mode captures the system configuration after every change, and displays both the previous and new settings in addition to the event details. Brief mode displays only the event details.

- Configure one or more push receivers to receive the audit logs. See the documentation for the receiver.
- If you want to use public keys for authentication between the ECB and the push receiver, configure public key profiles on both devices before configuring audit logging. See "Configure Secure File Transfer with Public Keys."

To configure audit logging:

1. Log on to the ECB, and click **Configuration** > **Security** > **Audit logging**.
2. On the Audit Logging page, do the following:

Attributes	Instructions
State	Select to enable event recording in the audit log.
Detail level	Select brief (default) or verbose output.
File transfer time	Specify the amount of time, in hours, from the completion of the last transfer to the beginning of the next transfer. This determines when a file transfer occurs unless the Max storage space or Max file size triggers the transfer first. • Minimum: 0, which disables this file transfer time function. • Maximum: 65535 • Default: 720
Max storage space	Specify the maximum amount of space that the audit log can consume on the ECB in MB. • Minimum: 0 • Maximum: 32 (default)
Percentage full	Use in conjunction with Max storage space to specify the percent of the Max storage space that triggers file transfer. This determines when a file transfer occurs unless the File transfer time or Max file size triggers the transfer first. • Minimum: 0, which disables this percentage full function. • Maximum: 99 • Default: 75

Attributes	Instructions
Max file size	Set the maximum size in Mega Bytes that the audit log can be before the system transfers the file. This determines when a file transfer occurs unless the Max storage space or Max file size triggers the transfer first. • Minimum: 0, which disables this maximum file size function. • Maximum: 10 • Default: 5
Push receiver	Add a push receiver and configure the following parameters for sending audit log files from the ECB to the receiver: • Server—Enter the IP address of the FTP/SFTP server to which you want the ECB to push audit log files. Default: 0.0.0.0. • Port—Enter the port number on the FTP/SFTP server to which the ECB will send audit log files. Range:1-65535. Default: 22 • Remote path—Enter the pathname to send the audit log files to the push receiver. Files are placed in this location on the FTP/SFTP server. Value: <string> remote pathname. • Filename prefix—Enter the filename prefix to prepend to the audit log files that the ECB sends to the push receiver. The ECB does not rename local files. Values: <string> prefix for filenames. • Username—Enter the username the ECB uses to connect to this push receiver. • Auth type—Select the authentication methodology. Password (default) or public key. • Do one of the following: Password—If you set the Auth type to password, click **Set** to enter and confirm the password used to access this push receiver. Public key—If you set the Auth type to public key, select the public key profile that you want from the drop-down list.

3. Click **OK**.
4. Save and activate the configuration.

License Widget

This release includes a widget that allows users to add, remove and view licenses. The **Widget** tab's **System** list includes this new **License Table** widget. When opened, this widget displays a list box showing each license's:

- License Name
- Session Count
- Install Date
- Begin Date

- Expire Date

Table controls include standard **Add** and **Delete** links. When the user clicks the **Add** link, the system displays The **Add License** dialog, from which the user can enter a license name and key. The **Delete** link allows the user to delete the selected license after command confirmation.

Issues Resolved

Documented issues resolved between Release PCZ2.0 M2 and Release PCZ2.0 M3 are listed below.

- ?

4

PCZ2.0 M4

This chapter provides descriptions, explanations, and configuration information for the contents of Maintenance Release PCZ2.0 M4. Maintenance Release content supercedes that distributed with the previous point release.

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.5
- C3.0.7
- P1.0.0

Current patch baseline: PCZ2.0.0 M2p1

Content Map

The following table identifies the new content in this PCZ2.0 M4 Maintenance Release documentation.

Content Type	Description
Adaptation	Software—Upgrades the software from a 32-bit kernel to a 64-bit kernel.
Adaptation	Policy—Adds the capability to apply a policy to the User table for more granular control over where a policy gets applied to runtime routing decisions.
Adaptation	SIP Monitor and Trace—Adds new objects to the SIP Interface configuration that change how you enable SIP Monitor and Trace, and adds the capability to filter notable events.

Content Type	Description
Adaptation	SIP Session Summary—Replaces the Ingress Realm and Egress Realm labels with Realm, which is the system generated "ECB" realm. Adds the Source Context label, which displays the source context configured for the session.

64-bit Upgrade

The Oracle Enterprise Communications Broker (ECB) software is upgraded from a 32-bit kernel to a 64-bit kernel. This upgrade enables the ECB application software to use most of the 4GB of memory addressable by a 32-bit process due to moving the kernel out of the memory space.

> **Note:**
>
> When you install the PCZ200M4 64-bit bzimage, you must upgrade the boot loader because the system requires the boot loader and the bzimage versions to match.

Hardware Requirements

No changes. Netra X3-2 remains the only supported hardware.

Virtual System Requirements

CPU Cores - No change: 2

Memory - Increase to 8GB RAM

Hard drive - No change: 40GB

Interfaces - No change: 4

Platform Boot Loaders

Oracle Oracle Enterprise Communications Broker (ECB) platforms require a boot loader to load the operating system and software.

All ECB platforms require that the boot loader and the software image match per release. For example, if the software image filename is nnPCZ200m3.bz, use the corresponding boot loader file named nnPCZ200m3.boot.

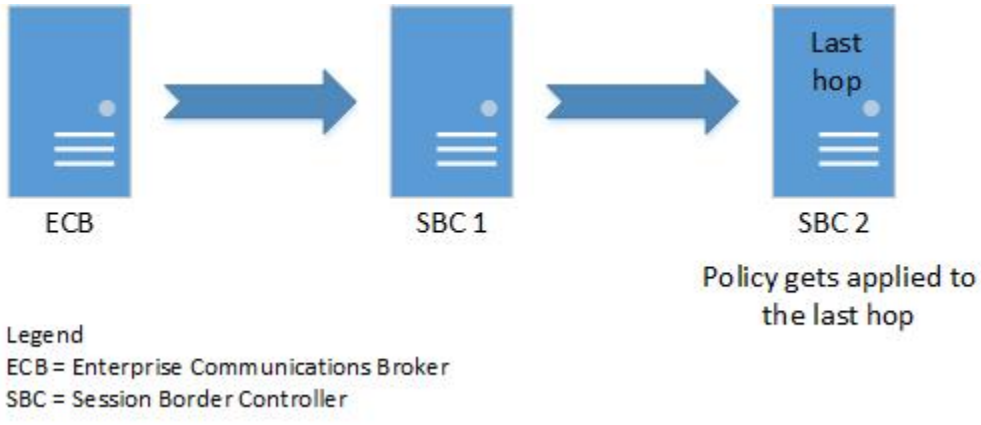
You must install the boot loader file as /boot/bootloader on the target system. When you plan to upgrade the system image, upgrade the boot loader before booting the new system image.

Apply a Policy to the User Table

You can apply a policy to the Oracle Enterprise Communications Broker (ECB) user table for more granular control over where a policy gets applied to runtime routing decisions.

Applying a policy to the user table provides more granularity than the routing table can because user table entries allow individual phone numbers and phone number ranges.

The ECB applies policies from the user table to the last hop on the route list specified in the routing table.



> **Note:**
>
> The system uses the policy applied to the called number from the user table.

You can use policies from the user table and the routing table together. When used together, the system obeys the policy in the user table first and the routing table second.

To apply a policy to the user table:

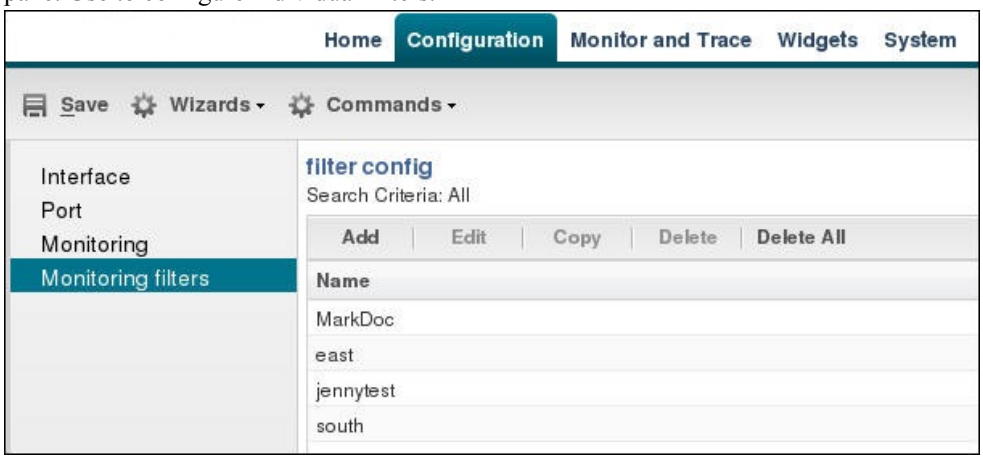
1. Add the policy to the ECB.
2. Add the policy to a user entry in the user table.

SIP Monitor and Trace Filter Configuration

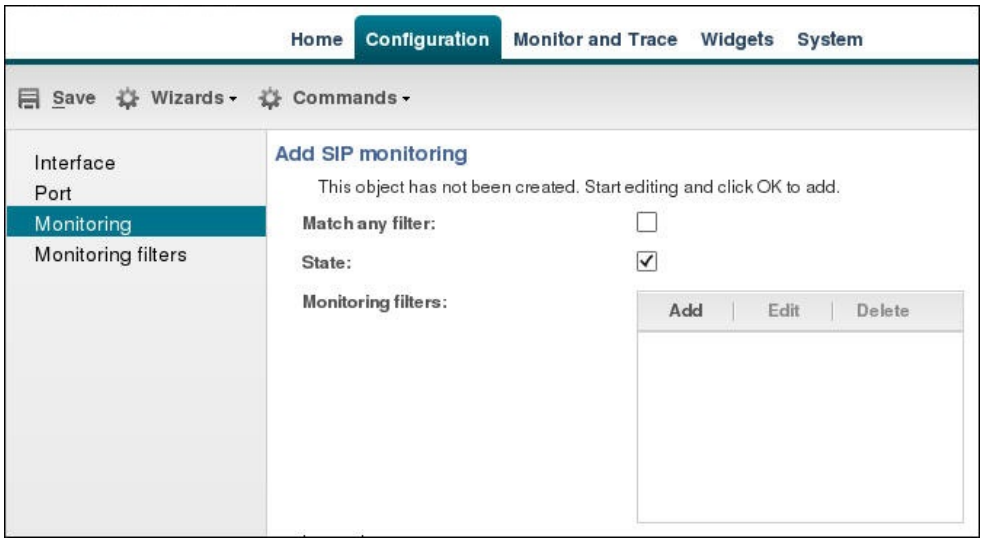
The SIP Monitor and Trace function allows you to monitor SIP sessions for notable events and display the results in the Oracle Enterprise Communications Broker (ECB) SIP Notable Events summary. Such information may help you perform troubleshooting. For more targeted monitoring, you can configure filters on particular users and addresses on the ECB, and on a specific agent.

As of PCZ200M4, the ECB includes the following changes:

- The SIP Interface configuration page adds the **Monitoring filters** object to the navigation pane. Use to configure individual filters.



- The pre-existing **Monitoring** object on the SIP interface configuration page adds the **Monitoring filters** element to the dialog. Use to apply filters to the ECB.



- The Add Agents configuration page adds the**Monitoring filters** configuration element to the Advanced section. Use to apply filters to an agent.

- When you upgrade to PCZ200M4, note that the system does not support the former "Enable SIP Monitor and Trace" setting. You must re-configure SNMP event traps through the dialogs described above. See "Caveats" for more information.

Use the following filter configuration process for both new installations and upgrades.

1. Create one or more filters in the Monitoring Filters object. You may use an asterisk character as a filter, if you want to monitor all session data.
2. Add one or more filters to the Monitoring object.
3. (Optional) Add one or more monitoring filters to an agent that you want to monitor.

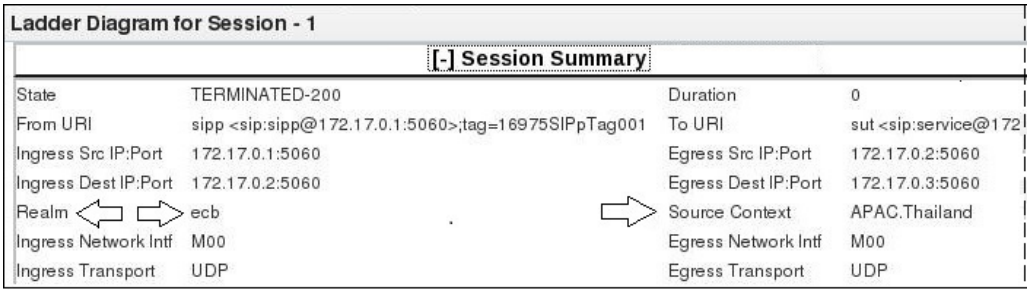
SIP Session Summary Changes

The SIP Session Summary associated with a Monitor and Trace Ladder Diagram displays the following changes regarding Realm and Source Context.

The session summary no longer displays references to ingress and egress realms. The summary displays the Realm label instead, which the system populates with the built in realm called "ecb."

The SIP Session Summary shows the Source Context that is applied to the session.

The following illustration shows an example of the SIP Session Summary displaying Realm and Source Context.



A

Known Issues and Caveats

Known Issues and Caveats - M1

Known Issues

Be aware of the following known issues when deploying the Oracle Enterprise Communications Broker (ECB). Oracle is working to resolve these issues in a subsequent release.

The following table lists known issues in Release PCZ2.0 M1. The information includes explanations of the impact of the issue and, if applicable, a workaround to the issue.

Issue	Workaround
The Broker widget does not show outbound translation information.	None
The HMR split and join headers function does not work in this release.	None
Using the Registration Widget to display more than 100,000 registrations degrades system performance.	None
Although enabling HA is not dynamically configurable, the system does not prompt the user to reboot.	Manually issue a reboot after enabling HA.
The LST Editor does not indicate that a file it is opening has encryption enabled.	Leave the current password field empty when setting the secret for non-encrypted LST files.
The support Info log contains unsupported commands, including **check-space-remaining code**, **check-space-remaining opt** and **show sipd spl**. The system's response to these commands is **command not found**.	None
The system displays duplicate error messages for an incorrectly referenced LST when the user verifies their configuration.	None
When the user completes a record editing procedure from a live multi-instance table, the system does not set focus (item selection) to that record in the table.	None

Issue	Workaround
The system's Session Monitor and Troubleshooting (SMT) tool captures ECB Sync data.	None
The system does not generate Interim-Update records for Accounting.	None
The **Set boot parameters** wizard displays a reboot information dialog box whenever the user clicks the Complete button. This is true even if the user has not made and changes.	None
The SMT tool reports Ingress/Egress transport for a TLS call as TCP.	None
The **Set boot parameters** wizard does not warn the user if the configured boot file does not exist.	None
The Oracle ECB does not forward an in-dialog ACK request when the host part of the request-uri is a configured SIP registrar domain.	None

Caveats

Be aware of the following behavior when deploying the Oracle Enterprise Communications Broker version P-CZ2.0.0 M1.

- Ensure that phone numbers in the LDAP database are unique. If the Oracle Enterprise Communications Broker encounters multiple records with the same number, the lookup fails.
- In some environments, there may be Cisco equipment that issues NOTIFY messages for which the Oracle Enterprise Communications Broker does not have a subscription. The Oracle Enterprise Communications Broker replies with 481 error messages to these NOTIFYs per RFC 3561 rather than forward the NOTIFY. For environments that need to have these non-compliant NOTIFYs forwarded, Oracle has built an SPL that allows the Oracle Enterprise Communications Broker to forward them. This SPL is available via your support representative.
- The system does not support network upgrade (network boot) via the GUI when operating over OVM. The GUI appears to allow this, but upgrade attempts fail.
- The system resets all local passwords to the default settings during an upgrade to the P-CZ2.0.0M1 release.
- Local password encryption differs between P-CZ2.0.0M1 and earlier versions. This affects system behavior when establishing an HA configuration in a downgrade scenario. For example, if you install P-CZ2.0.0M1 and downgradThe Cisco equipment expects a reply to these NOTIFYs even though standard behavior assumes a subscription.e to any prior release, the system retains the P-CZ2.0.0M1 password encryption behavior. Ramifications include the **Set initial configuration** wizard's configuration synchronization task being unable to work from an P-CZ2.0.0M1 system if the system from which you attempt to acquire the configuration has not been upgraded to P-CZ2.0.0M1, at least temporarily. This is because the acquisition target uses the old encryption method.

> **Note:**
>
> This P-CZ2.0.0M1 password behavior does not affect redundancy operations. A redundant pair can synchronize with different password methods.

- The Oracle Enterprise Communications Broker's SIP responses widget only displays error responses generated by ECB.

Limitations

Be aware of the following limitations in Release PCZ2.0 M1.

- High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.

Known Issues and Caveats - M2

Known Issues

Be aware of the following known issues when deploying the Oracle Enterprise Communications Broker (ECB). Oracle is working to resolve these issues in a subsequent release.

The following table lists known issues in Release PCZ2.0 M2. Information includes explanations, impact and workaround, if applicable.

Issue	Workaround
The system does not react correctly when it receives an error from a REFER target. Instead of completing its REFER process with those targets, the system continues to send INVITEs to them.	None
LDAP group configurations only perform lookups to the first LDAP server at which it finds a match. Even if the match to that LDAP server does not identify a target, the system does not continue looking for matches in the list.	None
Enabling ICMP when the interface is configured with a VLAN stops the ECB from handling any calls.	A system reboot is required after enabling ICMP on an interface with a configured VLAN.
The following commands do not present the correct data when issued from the CLI portal: • Sessions all • DNS cache entry • SPL	None

Issue	Workaround
When the called number in the broker widget input is found in the registration cache, the system displays the "dial plan lookup results", "agent lookup results" and "policy results" twice.	None
The system strips the "+" character when routing calls via Country Codes that are not configured within a Geographic Dialing context.	The default system configuration does not include every country as a Geographic Dialing context. Enter country codes, as needed.
The system's **verify-config** function fails to identify incorrect target group names configured on agents and sip registrar configurations.	None
SIP Monitor and Trace (SMT) incorrectly display a route table entry as "LDAP" when the system configuration includes a disabled **LDAP config**.	None
Changing a **Username** setting in an **LDAP Config** requires a system reboot.	None
When running the system on OVM, the **show platform cpu-load** command does not display the same utilization as the **xentop** command.	None
In some cases, SMT does not display terminated sessions as terminated.	None
The **From-header-manipulation** feature only works on endpoints derived from the Active directory. If the session also involved endpoints derived from the system's registration cache, the system forwards the incoming INVITE to the registered endpoints with the From-header unchanged.	None
The HMR split and join headers function does not work in this release.	None
Using the **Registration** Widget to display more than 100,000 registrations degrades system performance.	None
Although enabling HA is not dynamically configurable, the system does not prompt the user to reboot.	Manually issue a reboot after enabling HA.
The LST Editor does not indicate that a file it is opening has encryption enabled.	Leave the current password field empty when setting the secret for non-encrypted LST files.
The support Info log contains unsupported commands, including **check-space-remaining code**, **check-space-remaining opt** and **show sipd spl**. The system's response to these commands is **command not found**.	None
The system displays duplicate error messages for an incorrectly referenced LST when the user verifies their configuration.	None

Issue	Workaround
The system's Session Monitor and Troubleshooting (SMT) tool captures ECB Sync data.	None
The SMT tool reports Ingress/Egress transport for a TLS call as TCP.	None
The **Set boot parameters** wizard does not warn the user if the configured boot file does not exist.	None
The system does not populate the **Modify LDAP Config**'s **FROM header replacement** field with valid LDAP queries as documented.	The user must type in the attribute name of the desired **LDAP query** in the **FROM header replacement** field. The system's verify config function notifies the user if the attribute name is incorrect.

Caveats

Be aware of the following behavior when deploying the Oracle Enterprise Communications Broker version P-CZ2.0.0 M2.

- Ensure that phone numbers in the LDAP database are unique. If the Oracle Enterprise Communications Broker encounters multiple records with the same number, the lookup fails.
- In some environments, there may be Cisco equipment that issues NOTIFY messages for which the Oracle Enterprise Communications Broker does not have a subscription. The Oracle Enterprise Communications Broker replies with 481 error messages to these NOTIFYs per RFC 3561 rather than forward the NOTIFY. For environments that need to have these non-compliant NOTIFYs forwarded, Oracle has built an SPL that allows the Oracle Enterprise Communications Broker to forward them. This SPL is available via your support representative.
- The system does not support network upgrade (network boot) through the GUI when operating over OVM. The GUI appears to allow the upgrade, but upgrade attempts fail.
- The system resets all local passwords to the default settings during an upgrade to the P-CZ2.0.0M1 release.
- The Oracle Enterprise Communications Broker SIP responses widget displays only error responses generated by ECB.

Limitations

Be aware of the following limitations in Release PCZ2.0 M2.

- High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.

Known Issues and Caveats - M3

Known Issues (M3)

Be aware of the following known issues when deploying the Oracle Enterprise Communications Broker (ECB). Oracle is working to resolve these issues in a subsequent release.

The following table lists known issues in the P-CZ2.0.0 M3 release. Information includes explanations, impact and workaround, if applicable.

Issue	Workaround
The system does not react correctly when it receives an error from a REFER target. Instead of completing its REFER process with the target, the system continues to send INVITEs.	None
LDAP group configurations perform lookups only to the first LDAP server on which it finds a match. Even if the match to that LDAP server does not identify a target, the system does not continue looking for matches in the list.	None
Enabling ICMP when the interface is configured with a VLAN stops the ECB from handling any calls.	A system reboot is required after enabling ICMP on an interface with a configured VLAN.
The following commands do not present the correct data when issued from the CLI portal: • Sessions all • DNS cache entry • SPL	None
When the called number in the broker widget input is found in the registration cache, the system displays the "dial plan lookup results", "agent lookup results" and "policy results" twice.	None
The system strips the "+" character when routing calls via Country Codes that are not configured within a Geographic Dialing context.	The default system configuration does not include every country as a Geographic Dialing context. Enter country codes, as needed.
The system's **verify-config** function does not identify incorrect target group names configured on agents and sip registrar configurations.	None
SIP Monitor and Trace (SMT) incorrectly display a route table entry as "LDAP" when the system configuration includes a disabled **LDAP config**.	None

Issue	Workaround
Changing a **Username** setting in an **LDAP Config** requires a system reboot.	None
When running the system on OVM, the **show platform cpu-load** command does not display the same utilization as the **xentop** command.	None
Sometimes, SMT does not display terminated sessions as terminated.	None
The **From-header-manipulation** feature works only on endpoints derived from the Active directory. If the session also involved endpoints derived from the system's registration cache, the system forwards the incoming INVITE to the registered endpoints with the From-header unchanged.	None
The HMR split and join headers function does not work in this release.	None
Using the **Registration** Widget to display more than 100,000 registrations degrades system performance.	None
Although enabling HA is not dynamically configurable, the system does not prompt the user to reboot.	Manually issue a reboot after enabling HA.
The LST Editor does not indicate that a file it is opening has encryption enabled.	Leave the current password field empty when setting the secret for non-encrypted LST files.
The support Info log contains unsupported commands, including **check-space-remaining code**, **check-space-remaining opt** and **show sipd spl**. The system's response to these commands is **command not found**.	None
The system displays duplicate error messages for an incorrectly referenced LST when you verify their configuration.	None
The system Session Monitor and Troubleshooting (SMT) tool captures ECB Sync data.	None
The SMT tool reports Ingress/Egress transport for a TLS call as TCP.	None
The **Set boot parameters** wizard does not warn you when the configured boot file does not exist.	None
The system does not populate the **Modify LDAP Config**'s **FROM header replacement** field with valid LDAP queries as documented.	You must type the attribute name of the **LDAP query** that you want in the **FROM header replacement** field. The

Issue	Workaround
	verify config function notifies you if the attribute name is incorrect.
The upgrade schema results in a dial pattern verify config error.	Reboot solves the issue.
In a High Availability (HA) configuration, when you configure NTP and reboot either member of the pair, the rebooted member comes back up as "out of service."	Oracle recommends performing the following procedures during a maintenance window. **For hardware:** 1. Delete the configuration on the Secondary, and reboot. 2. When the Secondary is restored to service, Configure the Web GUI. 3. Save and Activate. 4. Configure NTP to match the Primary through either the ACLI or the Web GUI. 5. Save and Activate. 6. Run the Initial Setup wizard on the Secondary, and configure it as a Standby. 7. Reboot the Primary after the Secondary acquires and activates the configuration from the Primary, and begins rebooting. When the Primary and Secondary re-establish service, each ECB operates in its appropriate HA role. **For Virtual Machines (VM):** 1. Set the VM Host with the appropriate NTP server 2. Confirm that the time is synchronized. 3. Point the ECB to the VM Host. 4. Confirm that the ECB time is the same time as the VM NTP Host.
Changing the wancom1 IP address on the Primary ECB might make the systems unstable.	Oracle recommends performing the following procedure during a maintenance window. 1. Delete the configuration on the Secondary ECB, and reboot.

Issue	Workaround
	2. Revert the wancom1 IP on the Primary ECB back to 169.254.1.1 and 169.254.1.2. 3. Configure the Web GUI. 4. Save and Activate the configuration on the Primary, and reboot. 5. When the Primary is up and active, run the initial setup wizard on the Secondary and set it up as Standby. When the Secondary ECB comes up as Standby, the system should be back in Normal HA mode. 6. Change the Wancom1 IP on the Primary ECB and follow the on-screen warning message.

Caveats (M3)

Be aware of the following behavior when deploying the Oracle Enterprise Communications Broker (ECB) version P-CZ2.0.0 M3.

- The ECB media interface does not support management traffic for NTP and ENUM. When configuring connectivity to these resources, do not configure these resources within a media interface's subnet range.
- Ensure that phone numbers in the LDAP database are unique. When the ECB encounters multiple records with the same number, the lookup is unsuccessful.
- In some environments, there may be Cisco equipment that issues NOTIFY messages for which the ECB does not have a subscription. The ECB replies with 481 error messages to these NOTIFYs per RFC 3561 rather than forward the NOTIFY. For environments that need to have these non-compliant NOTIFYs forwarded, Oracle built an SPL that allows the ECB to forward them. This SPL is available by way of your support representative.
- The system does not support network upgrade (network boot) through the GUI when operating over OVM. The GUI appears to allow the upgrade, but upgrade attempts do not succeed.
- The system resets all local passwords to the default settings during an upgrade to the P-CZ2.0.0M1 release.
- The ECB SIP responses widget displays only error responses generated by the ECB.
- When upgrading from PCZ200M1 or PCZ200M2, you must upgrade to PCZ200M2P1 before upgrading to PCZ200M3. After upgrading to PCZ200M3, save, activate, and reboot.

Known Issues and Caveats - M4

Known Issues (M4)

Be aware of the following known issues when deploying the Oracle Enterprise Communications Broker (ECB). Oracle plans to resolve these issues in a subsequent release.

The following table lists known issues in the P-CZ2.0.0 M4 release. Information includes explanations, impact, and workaround, if applicable.

Issue	Workaround
The ECB loses sync connectivity when the transmitter and receiver are configured for High Availability.	None.
After you configure Early Media Inhibit, you must reboot the system.	None.

Caveats (M4)

Be aware of the following behavior when deploying the Oracle Enterprise Communications Broker (ECB) version P-CZ2.0.0 M4.

- Direct upgrade from nnPCZ200m2p1 to nnPCZ200m4 is not supported. To upgrade from nnPCZ200m2p1 to nnPCZ200m4, you must go through an upgrade to nnPCZ200m3.
- If you enabled Monitor and Trace in a previous release, note that the P-CZ2.0.0 M4 release disables Monitor and Trace due to configuration changes. You must re-enable Monitor and Trace through the new Monitoring and Monitoring Filters objects added to the SIP Interface configuration. The new objects enhance Monitor and Trace by providing notable event filtering. Formerly, you selected the "Enable SIP Monitor and Trace " check box on the SIP Interface configuration to enable Monitor and Trace, but the system did not provide the capability to filter the information. The SIP interface no longer displays the "Enable SIP Monitor and Trace " check box. See "SIP Monitor and Trace Filter Configuration."
- P-CZ2.0.0 M4 upgrades the software from a 32-bit kernel to a 64-bit kernel. This upgrade enables the ECB application software to maximize memory utilization. When you install the P-CZ2.0.0 M4 64-bit bzimage, you must upgrade the boot loader because the system requires the boot loader and the bzimage versions to match. For example, if the software image filename is nnPCZ200m4.bz, use the corresponding boot loader file named nnPCZ200m4.boot. You must install the boot loader file as /boot/bootloader on the target system. When you plan to upgrade the system image, upgrade the boot loader before booting the new system image.
- When performing an ECB sync with more than 20,000 entries in the user database, the system may become unstable.

B

CLI Portal Reference

This appendix provides reference for the output the system generates with the Oracle Enterprise Communications Broker's CLI Portal widgets. It includes widgets, applicable arguments and output description.

About

This command displays credit information including version number for the device. It also shows current third party licenses applicable to the software image you are running. There are no arguments.

Accounting

This command displays a summary of statistics for all configured external accounting servers. Entered without any arguments, the command displays the global Accounting Status Summary, returning the equivalent of the accounting all argument.

Arguments include:

- IP address:port — With the supplied IP address and port of a configured accounting server, the statistics for that object will be displayed on the screen.
- All — Display the all accounting servers statistics.

Acks

This command displays ACK method traffic counters. Output includes server and client counts of:

- ACK requests
- Retransmissions
- Transaction Timeouts
- Locally Throttled

Agent

This command displays statistics related to specified SIP session agents.

Arguments, which are required, include:

- Agent name — Enter the agent name as an argument to display statistics for that specific agent.

Agent group

This command displays statistics related to all defined agent groups. Arguments are ignored. Output fields are presented below.

Inbound and Outbound 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

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

Agent summary

This command displays statistics related to all defined SIP session agents. Arguments are ignored. Output fields are presented below.

Inbound and Outbound 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

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

Arp

This command displays the current Internet-to-Ethernet address mappings in the ARP table. The first section of the Arp command displays the Link Level ARP table including:

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

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

- interface
- VLAN
- IP Address
- MAC address
- time stamp
- type

The third section of the Arp command shows general ARP table information.

Arp info

This command displays the size and number of entries in the device's layer two and interface tables.

Arp statistics

This command displays receive, transmit and internal arp traffic statistics, including adds, deletes, errors and drops.

Byes

This command displays BYE method traffic counters. Output includes server and client counts of:

- BYE requests
- Retransmissions
- 200 OK
- Transaction Timeouts
- Locally Throttled

Cancel

This command displays CANCEL method traffic counters. Output includes server and client counts of:

- CANCEL requests
- Retransmissions
- 481 Does not exist
- Transaction Timeouts
- Locally Throttled

Client trans

Display statistics for SIP client events when the device is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

Information displayed includes:

- 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 device 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

Clock

This command displays the current date and time for your device.

Configuration

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

Arguments include:

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

- account-config — Show account-config configuration
- auth-params — Show the auth-params configurations
- authentication — Show the authentication configuration
- dns-config — Show all dns-config configurations
- enum-config — Show the enum-config configuration
- host-route — Show all host-route configurations
- local-policy — Show all local-policy configurations
- network-interface — Show all network-interface configurations
- network-parameters — Show all network-parameters configurations
- ntp-config — Show ntp-config configuration
- phy-interface — Show all phys-interface configurations
- qos-constraints — Show the qos-constraints configurations
- redundancy-config — Show redundancy-config configuration
- session-agent — Show all session-agent configurations
- session-group — Show all session-group 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
- snmp-community — Show all snmp-community configurations
- static-flow — Show all static-flow configurations
- system-config — Show system-config configuration
- 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

- session-constraints — Show all session-constraint configurations
- inventory — Display an inventory of all configured elements on the device

DNS

This command displays DNS statistics

Arguments include:

- Stats — Show the statistics for the dns configuration
- Cache-entry [entry] — Look in the DNS cache for a specific entry

For cache 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

ENUM

This command displays ENUM statistics. Arguments include:

- all — Shows stats summary of all ENUM Agents
- cache-entry — Look in the ENUM cache for a specific entry
- 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
- rate — Displays the transaction rate of ENUM messages
- stats — Show the statistics for the dns configuration
- cache-entry — Look in the DNS cache for a specific entry

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

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.

The following information may be displayed for each output:

- 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/session; or c) a BYE initiated by the device 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 device
- 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
- CAC BW Drop — Number of call admission control session setup failures due to insufficient bandwidth
- Lifetime — Displays 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

Features

This command shows the currently enabled features based on product entitlements.

Forked sessions

This command shows active, period and total counts of sessions the system has forked and forks that have been rejected. Statistics displayed includes:

- Forked Sessions
- Forked Sessions Rejected

Info

This command displays INFO method traffic counters. Output includes server and client counts of:

- INFO requests
- Retransmissions
- 200 OK
- 480 Unavailable
- Transaction Timeouts
- Locally Throttled

Interface

This command shows the total and period counts of traffic that has passed via the system interface. The command requires the argument "ECB".

Interface summary

This command shows the total and period counts of sessions that has passed via the system interface.

Interfaces

The interfaces command shows information on the device's interfaces, including:

- 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

Arguments include:

- Brief — Allows you to view key running statistics about the interfaces within a single screen. This is an optional argument.

IP

This command displays IP statistics for your device. Arguments include:

- Statistics — Display detailed IP statistics
- Connections — Display all TCP and UDP connections
- SCTP — Display all SCTP statistics
- TCP — Display all TCP statistics
- UDP — Display all UDP statistics

Executing the IP command with no arguments returns the IP statistics command output.

> **Note:**
>
> The command list includes "IP tcp" and "IP udp". These produce the same output as the IP command using those suffixes as arguments.

LDAP

This command shows active and period counts of traffic between the device and configured LDAP servers.

Memory

This command displays statistics related to the memory within the device.

Arguments include:

- usage — Display system-wide memory usage statistics. If the 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

Message

This command displays MESSAGE method traffic counters. Output includes server and client counts of:

- MESSAGE requests
- Retransmissions
- 200 OK
- Transaction Timeouts
- Locally Throttled

NAT by index

Display the entries in the NAT table.

NTP server

This command displays information about NTP servers configured for use with the system. Information includes the quality of the time being used in terms of offset and delay measurement; maximum error bounds are also displayed.

NTP status

Display information about configuration status, NTP daemon synchronization, NTP synchronization in process, and whether or not if NTP is down.

Platform all

This 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.

Information displayed includes:

- cpu — Display summary CPU information
- cpu—load — Display current CPU load
- errors — Display Servicepipe write errors
- 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

Prack

This command displays PRACK method traffic counters. Output includes server and client counts of:

- PRACK requests
- Retransmissions
- 200 OK

- Transaction Timeouts
- Locally Throttled

Processes

The 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 include:

<Process> — The following is a list of each process argument:

- sysmand — Display sysmand process statistics related to the system's startup tasks
- acliSSH0 — Show acliSSH0 process statistics
- acliSSH1 — Show acliSSH1 process statistics
- acliSSH2 — Show acliSSH2 process statistics
- acliSSH3 — Show acliSSH3 process statistics
- acliSSH4 — Show acliSSH4 process statistics
- acliTelnet0 — Show acliTelnet0 process statistics
- acliTelnet1 — Show acliTelnet1 process statistics
- acliTelnet2 — Show acliTelnet2 process statistics
- acliTelnet3 — Show acliTelnet3 process statistics
- acliTelnet4 — Show acliTelnet4 process statistics
- lid — Show lid process statistics
- pusher — Show pusher process statistics
- snmpd — Show snmpd process statistics
- cliworker — Show CliWorker 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 device is using RADIUS
- algd — Display algd process statistics
- sipd — Display sipd process statistics
- acliConsole — Display acliConsole 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 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
- 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 device. The following fields explain the output of the 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 device, categorized on a per task/process basis. The following fields explain the output of the processes cpu command:

- Task Name — Name of the device 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 device was last rebooted
- Now — CPU usage in the last second

All — concatenate the process command for all running processes.

Redundancy

The redundancy command displays HA statistics for a redundant device.

Arguments include:

- mbcd — Display the synchronization of media flows for the members of an HA device pair
- algd — Display the synchronization of MGCP signaling for the members of an HA device pair
- sipd — Display the synchronization of SIP signaling for the members of an HA device pair
- config — Display the synchronization of configuration information for the members of an HA device pair
- collect — Display the Collect redundancy statistics
- link — Display the Link 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 device.

The following HA statistics are shown for the Period and Lifetime monitoring spans.

- Queued entries — Number of transactions not yet sent to standby device peer
- Red Records — Total number of HA transactions created
- Records Dropped — Number of HA transaction records lost because the standby device fell behind in synchronization
- Server Trans — Number of HA transactions in which the device acted was the server
- Client Trans — Number of HA transactions where the device was the client

The following HA transaction statistics are shown for the Lifetime monitoring span.

- Requests received — Number of HA requests received by the device, acting as server
- Duplicate requests — Number of situations in which an HA request was received by the device, and (acting as the server side in the client-server relationship) the device 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 an error response to the client
- Request sent — Number of HA requests that were sent by the standby device
- 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 device in an HA pair
- Errors received — Number of errors received in response to HA requests
- Transaction timeouts — Number of HA transactions that timed out

The numerical identifier for the last redundant transaction processed is also displayed in the redundancy output.

Refer

This command displays REFER method traffic counters.

Register

This command displays REGISTER method traffic counters. Output includes server and client counts of:

- REGISTER requests
- Retransmissions
- 200 OK
- Transaction Timeouts
- Locally Throttled

Registration

This command displays the registrations currently active and lifetime on the device.

Routes

This command displays the device's current routing table.

Running-config

This command displays the configuration currently active on the configuration. The user can reduce the command output to specific configuration elements by appending the command with that configuration element key field (element name) as an argument.

See the Configuration command for applicable arguments.

SIP

The sip command displays SIP statistics on your device. Statistics displayed include:

- 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 device
- 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

Server trans

Display statistics for SIP client events when the device is acting as a SIP server in its B2BUA role. Period and Lifetime monitoring spans are displayed.

Information displayed includes:

- 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 device 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

Sessions

This command displays the number of SIP sessions and dialogs handled by the system on an active, period and lifetime basis. Counters include:

- Sessions
  - Initial
  - Early
  - Established
  - Terminated
- Dialogs
  - Early
  - Confirmed
  - Terminated

SNMP community table

The SNMP community table command displays all information for configured SNMP communities including request and responses for each community.

SPL (SBC Programming Language)

The spl command displays the version of the SPL engine, The filenames and version of the SPL plugins currently loaded on the device, the signature state of each plugin, and the system tasks that each loaded plugin interacts with enclosed in brackets.

SPL memory

This command displays the statistics of the Spl Engine Memory usage on the system.

SPL options

This command lists the SPL-specific options registered by an SPL on the system.

Subscribes

This command displays SUBSCRIBE method traffic counters. Output includes server and client counts of:

- SUBSCRIBE requests
- Retransmissions
- 200 OK
- Transaction Timeouts
- Locally Throttled

System state

Displays the system state, either online or offline.

Timezone

This command displays the timezone set including the name of the timezone, its minutes from UTC, and the start and stop date and hours for daylight saving time.

The timezone command also displays the DST settings. If rules-based DST configuration is used, the device converts the rule into the absolute DST start or end time for the current year.

Trap receiver

The trap-receiver command displays trap receiver information for each configured SNMP community.

Updates

This command displays UPDATE method traffic counters. Output includes server and client counts of:

- UPDATE requests
- Retransmissions
- 200 OK
- 480 Unavailable
- Transaction Timeouts
- Locally Throttled

Uptime

The 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.

Users

The users command displays all users currently logged into the device by index number. Other display information includes:

- Task-ID
- remote IP address — Only displayed for telnet or SSH connections
- IdNumber
- Duration of connection
- Connection Type
- State — Denotes the current connection

Version

The 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.

Version boot

The version boot command shows information on the bootloader, BIOS and mainboard. shows a detailed info of cpu version. detailed info of the hardware version. detail of the type of the build and brief detail of the boot parameter

Version CPU

The version boot command shows detailed info on the CPU version.

Version hardware

The version boot command shows detailed info of the hardware version.

Version image

The version boot command shows detail on the type of the build and brief detail on the boot parameter.

Wancom

Displays negotiated duplex mode and speed for all system control interfaces.