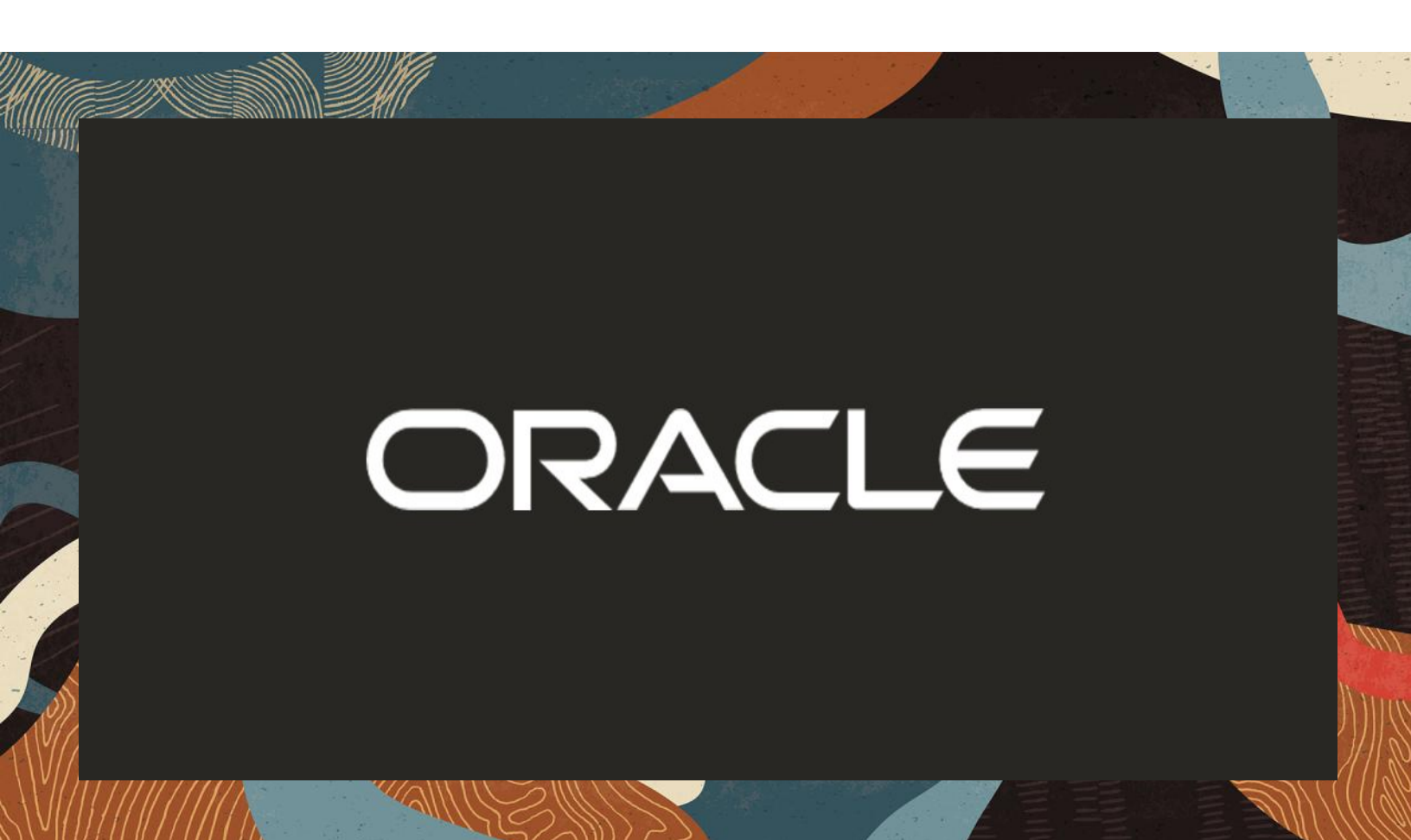




ORACLE

Oracle SBC Integration with ASC Neo Cloud SIPREC

Technical Application Note

ORACLE

COMMUNICATIONS



Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Contents

Revision History	4
1. Intended Audience	4
2. Document Overview	4
2.1 ASC Neo Cloud	4
2.2 Oracle SBC with ASC Neo Cloud SIPREC	5
3. Validated Oracle Software Versions	5
4. Related Documentation	6
5. Requirements	6
5.1 ASC Neo Cloud SIPREC Interworking Requirements	7
5.2 SIPREC Metadata Identity Requirements	7
5.3 SIPREC Signaling, Media, and VPN Considerations	7
6. AWS Environment and VPN Requirements	7
6.1 AWS PCH-SBC Instance	7
6.2 AWS Site-to-Site VPN	8
7. Network Architecture	8
8. Configuring the SBC	9
8.1 Configure SBC using Web GUI	9
8.2 SBC Objects for ASC SIPREC	9
8.3 Session Recording Servers	13
8.4 Session Recording Group	15
8.5 No Custom SIP Header Manipulation Required	16
9. SIPREC Signaling and Metadata Validation	16
10. Verify Connectivity	17
Appendix A - Sanitized SBC Configuration Excerpts	19

Revision History

Document Version	Description	Revision Date
1.0	Initial release	26-Aug-2026

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners, and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform and with SIPREC-based call recording.

2. Document Overview

This Oracle technical application note describes the Oracle Communications Session Border Controller (SBC) configuration used to interwork with ASC Neo Cloud using SIPREC. It focuses on the SBC configuration that establishes a separate SIPREC recording session toward ASC Neo Cloud through the AWS site-to-site VPN, delivers the associated media and metadata, and supports the deployment-specific recording and correlation requirements.

The configuration in this application note is limited to the ASC Neo Cloud SIPREC integration. The production call path, contact-center or call-control platform, carrier/PSTN connectivity, baseline network-interface configuration, ASC tenant policy, and baseline AWS VPN administration are assumed operational. The ASC configuration objects, AWS site-to-site VPN context, routing information, screenshots, and verification considerations supplied for this lab are retained in this note.

2.1 ASC Neo Cloud

ASC Neo Cloud is a cloud-native, enterprise-grade suite by [ASC Technologies](#) designed for compliant communication recording, quality management, and AI-powered analytics. In this integration, ASC Neo Cloud acts as the SIPREC Session Recording Server (SRS). This application note does not configure ASC applications or tenant policies. It documents the Oracle SBC SIPREC interface used to send recording sessions to ASC Neo Cloud over the private AWS site-to-site VPN.

For additional information, refer to ASC Neo Cloud documentation and the deployment-specific SIPREC interworking guidance.

2.2 Oracle SBC with ASC Neo Cloud SIPREC

The Oracle SBC acts as the SIPREC Session Recording Client (SRC). The original call remains on its normal signaling and media path, while the SBC establishes a separate SIPREC recording session to the ASC Neo Cloud SRS. The SIPREC session carries recording control, metadata, and media using the configured SBC policy.

For the activated configuration, the monitored genesys realm is associated with the ASC Session Recording Group ascsrc. The ASC recording server is configured as ascsrcs in the dedicated siprec realm. SIPREC signaling reaches the ASC SRS through the AWS site-to-site VPN.

Term	Description
SRC	Oracle SBC acting as the SIPREC Session Recording Client.
SRS	ASC Neo Cloud recording endpoint receiving the SIPREC recording session.
SIPREC	SIP-based recording mechanism carrying signaling, recording metadata, SDP, and media.
SIPREC participant and stream identifiers	Unique identifiers in SIPREC XML used to distinguish participants and media streams in each recording session.
ASC tenant/account context	Deployment-specific tenant or account information required by ASC for the target environment.

3. Validated Oracle Software Versions

The configuration in this application note was captured after the ASC SIPREC candidate was verified and activated on Oracle Enterprise Session Border Controller SCZ9.3.0 Patch 8 (Build 291). Verification recorded 0 critical issues and 0 errors. The SBC displayed one disk-capacity advisory warning.

This application note documents a virtual Oracle Enterprise Session Border Controller running in AWS.

However, Oracle SBC can be deployed on OCI, AWS, GCP and Azure depending upon the nature of your cloud deployment. Equivalent VPN configuration can also be performed on OCI as mentioned in this Application Note.

Refer to the Oracle documentation for the complete supported-platform and software-release matrix.

Acme Packet 1100

Acme Packet 3900

Acme Packet 3950

Acme Packet 4600

Acme Packet 4900

Acme Packet 6350 (Quad 10GbE NIU only)

Acme Packet 6400

The proof environment used an AWS-hosted virtual SBC. The AWS runtime state, VPN overview, and VPN tunnel status are shown in the following evidence sequence.

4. Related Documentation

Oracle SBC

[Oracle Enterprise Session Border Controller Documentation - S-Cz10.1.0](#)

[Oracle Enterprise Session Border Controller Release Notes - S-Cz10.1.0](#)

[Oracle Technical Application Notes](#)

ASC Neo Cloud

<https://www.ascstechnologies.com/solutions/technologies/recording-qm-analytics-cloud-services/>

5. Requirements

The following prerequisites must be available before validating the Oracle SBC-to-ASC Neo Cloud SIPREC integration:

- The production call path and the AWS site-to-site VPN are operational.
- ASC has provided the private SRS destination, supported SIP transport, and media policy.
- VPN routes, security policy, and target-network requirements permit the SBC to reach the ASC SRS.
- In the supplied PoC, the SRS destination is 10.213.0.76/32, the protected target network is 10.213.0.64/28, and SIPREC signaling uses TCP port 5060.
- The required SIPREC metadata, recording policy, and correlation behavior have been agreed with ASC for the target tenant.

The ASC Neo Cloud SIPREC integration in this application note uses the following Oracle SBC configuration objects:

Configuration Element	Purpose in this Integration
realm-config	Associates the monitored call realm with the ASC Neo Cloud recording group and defines the dedicated recording realm.
sip-interface	Existing SIP signaling interface used by the dedicated SIPREC realm. Baseline interface creation is not repeated in this note.
session-recording-server	Defines each ASC Neo Cloud Session Recording Server destination.
session-recording-group	Groups the ASC Neo Cloud recording servers and controls selection/redundancy behavior.
sip-manipulation	No ASC-specific SIP manipulation is attached to the active SIPREC realm in the supplied lab. Any future manipulation must be based on documented ASC requirements and validated against an outbound SIPREC INVITE.

5.1 ASC Neo Cloud SIPREC Interworking Requirements

SIPREC signaling must reach the ASC SRS through the private AWS site-to-site VPN using the agreed SIP transport and port.

The Oracle SBC must establish a separate SIPREC recording session for the applicable monitored calls.

Original call identity and dialog context should be preserved in the generated SIPREC metadata.

SIPREC metadata must contain unique participant and stream identifiers so ASC can distinguish participants and media streams for each recording session.

Any ASC tenant, account, or correlation information must follow the deployment-specific requirements agreed with ASC.

Reachability, redundancy, media handling, and failure behavior must be validated for the target production design.

Note: ASC uses SIPREC metadata to identify the participants and media streams for each recording session. Verify the deployment-specific tenant or correlation information with ASC. Do not substitute a fixed value for an interaction value that is expected to be dynamic.

5.2 SIPREC Metadata Identity Requirements

ASC Neo Cloud requires SIPREC metadata that identifies the recorded participants and media streams unambiguously. In the supplied lab context, unique participant and stream identifiers are a mandatory validation consideration before complete ASC recording acceptance can be asserted.

The active ASC SIPREC path does not add ASC-specific SIP headers or apply an outbound SIP manipulation. Preserve the Oracle SBC-generated SIPREC metadata and validate the resulting SIPREC XML only against documented ASC requirements and an outbound SIPREC INVITE capture.

For a deployment that requires supplemental metadata mapping, use the agreed source field and validate the mapped value in the outbound SIPREC INVITE and in ASC. Do not introduce a fixed tenant or correlation value unless ASC explicitly requires it.

Transfer and consultation-call behavior must be tested with ASC. Confirm that participant and stream identifiers, recording continuity, and any agreed correlation information remain valid through the call lifecycle.

5.3 SIPREC Signaling, Media, and VPN Considerations

Successful integration validation requires SIPREC signaling, metadata, media streams, and the private network path to operate together. The route-based IPsec VPN and the static routing shown in this note are operational prerequisites for the supplied lab topology.

Aspect	Design consideration for this integration
Interaction correlation	Use the ASC-provided SRS destination and agreed tenant/routing mechanism. The supplied lab sends SIPREC sessions through the AWS site-to-site VPN to the configured ASC SRS.
Original call metadata	Preserve Oracle SBC-generated SIPREC metadata and validate participant, stream, and any agreed ASC correlation information with ASC.
Media streams	Deliver the participant audio as separate streams within the same SIPREC session. Avoid unnecessary media manipulation or transcoding unless required by the target design.

Aspect	Design consideration for this integration
DTMF	Where the selected ASC Neo Cloud service consumes DTMF, preserve the received sequence, timing, and negotiated event method.
Transfers	Validate that the logical interaction remains correlated during transfer scenarios and that the agreed interaction identifier does not unexpectedly change.
Tenant and routing	Use the ASC-provided SRS destination and agreed tenant/routing mechanism. The supplied lab sends SIPREC sessions through the AWS site-to-site VPN to the configured ASC SRS.
Transport and security	Use the transport, certificate, encryption, firewall, and media requirements supplied for the target ASC Neo Cloud environment. The lab values shown in this note are examples, not universal defaults.

Note: Do not attach a header-manipulation rule to the active ASC SIPREC path unless ASC has provided a documented requirement and the resulting SIPREC INVITE has been validated.

6. AWS Environment and VPN Requirements

This section documents the AWS runtime and site-to-site VPN requirements used for the ASC Neo Cloud SIPREC proof environment. The AWS screenshots are retained here as AWS evidence and are not SBC configuration evidence.

6.1 AWS SBC Instance

The screenshot displays the AWS Management Console interface for an EC2 instance. The left sidebar shows navigation options like Dashboard, AWS Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, and Lifecycle Manager. The main content area shows the 'Instance summary for i-0f074e72751753173 (PCH-SBC)'. The instance is in a 'Running' state. Key details include: Instance ID i-0f074e72751753173, Public IPv4 address 52.73.224.232, Private IPv4 addresses 10.0.2.67, 10.0.3.101, 10.0.0.213, 10.0.1.11, and 10.0.4.143, Public DNS ec2-52-73-224-232.compute-1.amazonaws.com, Elastic IP addresses 100.25.184.18, 3.230.88.21, 34.234.107.130, and 52.73.224.232, and VPC ID vpc-06c7ea2a5e9cfdcf.

Figure 1 - AWS PCH-SBC instance running before SBC configuration capture.

6.2 AWS Site-to-Site VPN

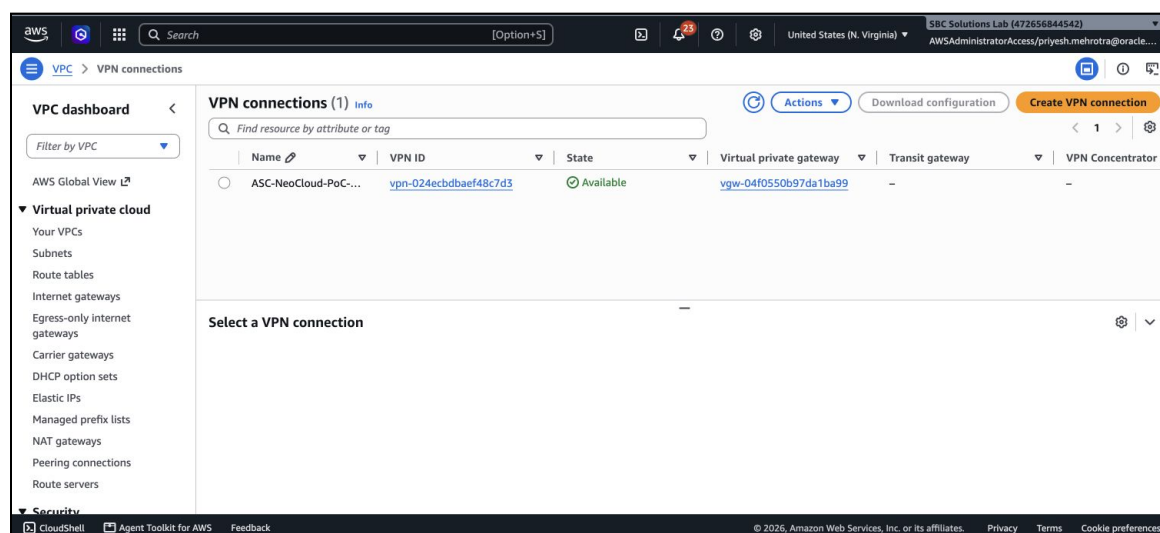


Figure 2 - AWS site-to-site VPN overview for ASC Neo Cloud SIPREC.

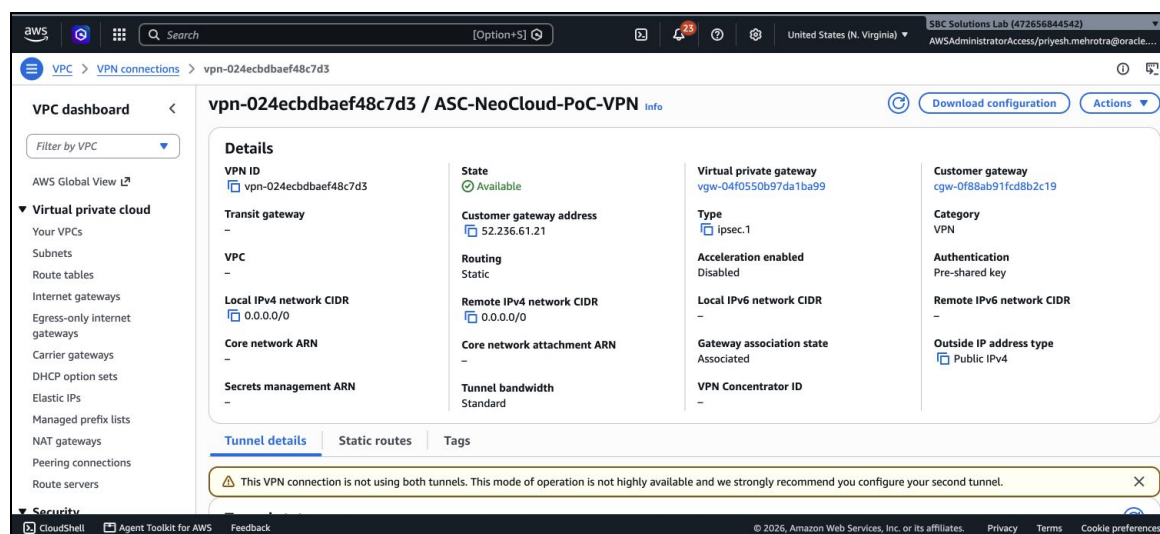


Figure 3 - AWS VPN tunnel status for the ASC Neo Cloud SIPREC proof environment.

The VPN uses route-based IKEv2 and IPsec. The ASC SRS private destination 10.213.0.76 is reached through the protected network 10.213.0.64/28.

The VPN status evidence shows one available tunnel in the proof environment. Validate a resilient tunnel design before production deployment.

7. Network Architecture

The logical architecture separates the monitored call session from the independently established SIPREC recording session. The Oracle SBC monitors the genesys realm and creates the SIPREC session through the dedicated siprec realm toward ASC Neo Cloud across the AWS site-to-site VPN.

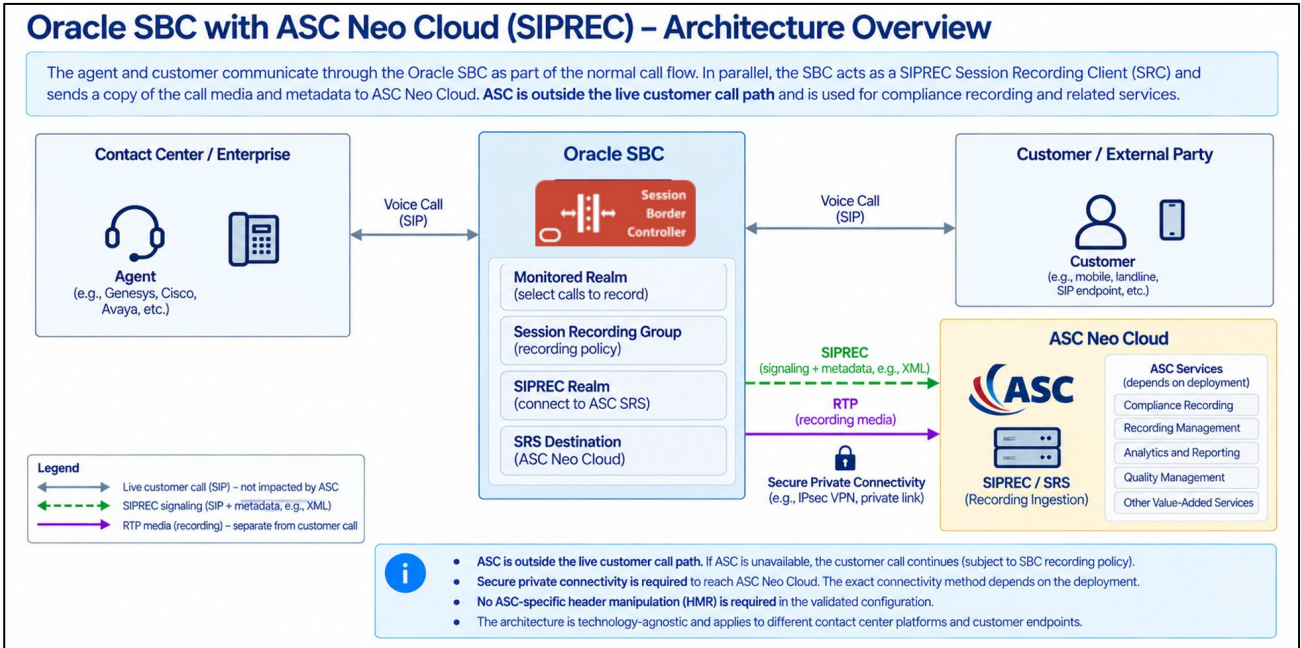


Figure 4 - Logical network architecture for the Oracle SBC and ASC Neo Cloud SIPREC proof environment.

The monitored call signaling and media remain on the call-facing path. The SIPREC INVITE, SDP, metadata, and replicated RTP use the separate recording path defined by ascsrs and ascsg.

8. Configuring the SBC

This section follows the captured SBC GUI configuration sequence: session agents, SIP interface, SIPREC network interface, monitored and recording realms, session recording server, session recording group, and the no-custom-header posture.

There are two methods for configuring the Oracle SBC: CLI or GUI. For the purposes of this application note, the Oracle SBC GUI is used for the configuration examples and the corresponding CLI path is provided for each configuration object. Any parameter not specifically identified below can remain at its Oracle SBC default value unless required by the target deployment.

8.1 Configure SBC using Web GUI

To access the Oracle SBC GUI, enter the management IP address in a web browser. When the login screen appears, enter the configured administrative credentials. Select the Configuration tab and use Expert mode to access the configuration objects described in this application note.

The configuration examples below show the live SBC GUI evidence for the ASC SIPREC path. The call-session objects establish the monitored realm, while the session-recording-server and session-recording-group objects establish the recording session.

8.2 SBC Objects for ASC SIPREC

Configure the SIPREC realm used for ASC recording. The realm identifies the SBC interface and policy used for the separate SIPREC session, while the ASC SRS is reached using the private route provided by the AWS site-to-site VPN.

Associate the monitored realm with the ASC SIPREC group. No outbound SIP manipulation is attached to the active ASC path because the supplied configuration does not require ASC-specific SIP header insertion.

The siprec realm uses siprecinterface:0.4. The interface has DNS domain telechat.o-test06161977.com and uses the SIPREC-facing address 10.0.3.101.

GUI Path: media-manager / realm-config

ACLI Path: configure terminal > media-manager > realm-config

Session Agents

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Session Agent' and contains a table with the following data:

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
☐		10.0.0.192		5080	enabled	SIP	occas	
☐		solawssbc.pstn.twilio...		5060	enabled	SIP	twilio	
☐		sollabawssbc.byoc....		5060	enabled	SIP	genesys	

At the bottom of the table, it says 'Displaying 1 - 3 of 3'. There are also buttons for 'Delete all Session Agent Items', 'Search', 'Show Configuration', 'Discard', 'Verify', and 'Save'.

Figure 5 - Oracle SBC GUI: call-session session agents. ASC SIPREC uses a session-recording-server rather than a session agent.

SIP Interface

ORACLE

Enterprise Session Border Controller

awspsbcb

10.0.0.213

SC293.0 Patch 8 (Build 291)

Dashboard

Configuration

Monitor and Trace

Widgets

System

Configuration

View Configuration

media-manager

security

session-router

access-control

account-config

filter-config

ldap-config

local-policy

local-routing-config

media-profile

response-code-and-phr...

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system

SIP Interface

Show Configuration

Delete all SIP Interface items

Search

Select	Action	State	Realm ID	Description	Carriers	Trans Expire	Initial Inv Trans Expire
☐		enabled	genesys				0
☐		enabled	occas				0
☐		enabled	siprec				0
☐		enabled	twilio				0

Show All

Displaying 1 - 4 of 4

Figure 6 - Oracle SBC GUI: SIP interface inventory including the SIPREC-facing interface.

SIPREC Network Interface

Name	siprecinterface	
Sub Port Id	0	(Range: 0..4095)
Description		
Hostname		
IP Address	10.0.3.101	
Pri Utility Addr		
Sec Utility Addr		
Netmask	255.255.0.0	
Gateway	10.0.3.1	
✓ Gw Heartbeat		
State	☐ enable	
Heartbeat	0	(Range: 0..65535)
Retry Count	0	(Range: 0..65535)
Retry Timeout	1	(Range: 1..65535)
Health Score	0	(Range: 0..100)
✓ Bfd Config		
Health Score	0	(Range: 0..100)
DNS IP Primary	8.8.8.8	
DNS IP Backup1	1.1.1.1	
DNS Domain	telechat.o-test06161977.com	
HiP IP List	10.0.3.101 ×	

Figure 7 - Oracle SBC GUI: siprecinterface configuration and DNS domain used by the SIPREC realm.

Realm Configuration

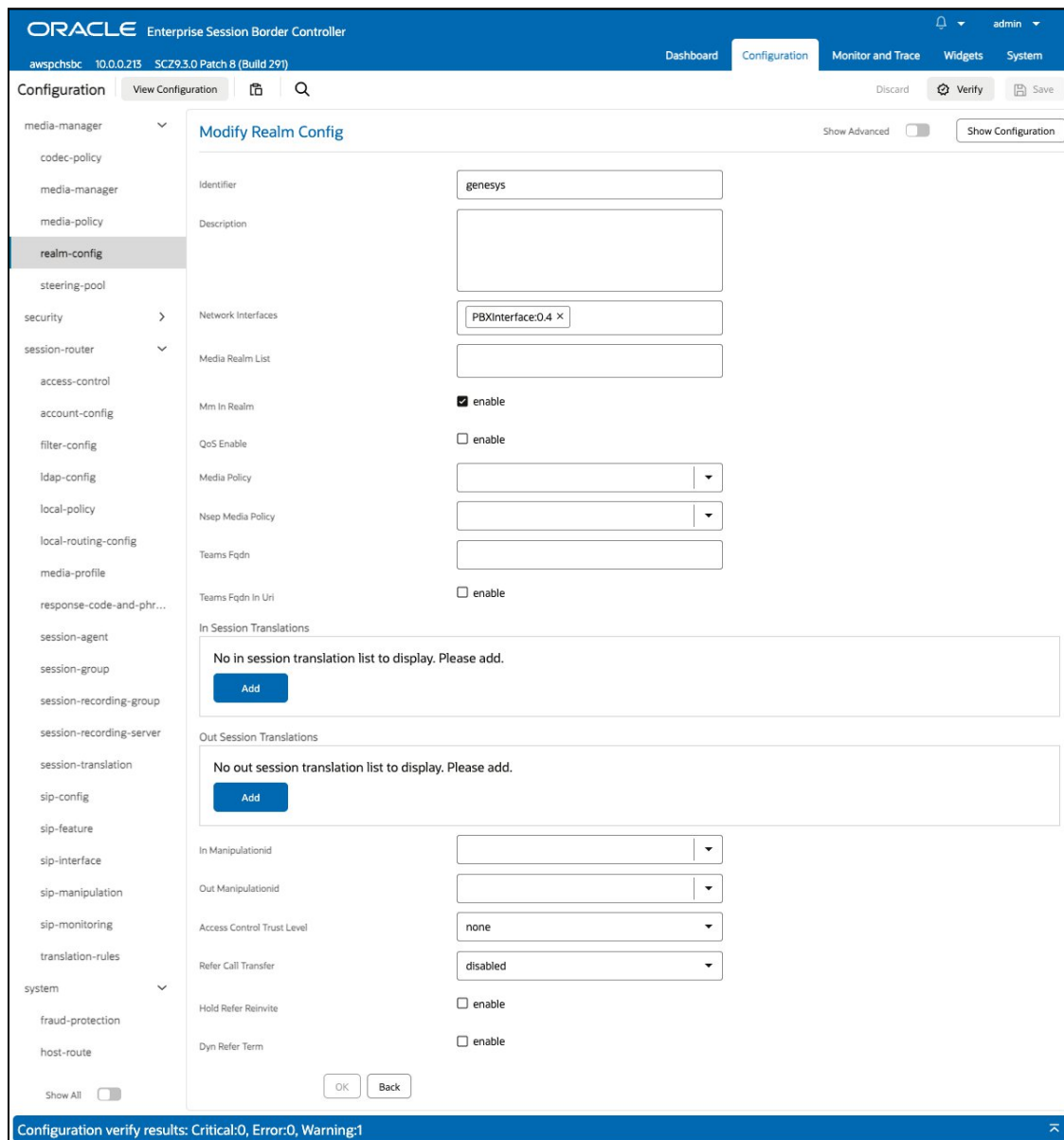


Figure 8 - Oracle SBC GUI: monitored genesys realm used for ASC recording association.

```
media-manager
  realm-config
    identifier      genesys
    session-recording-server SRG:ascsrcg

  realm-config
    identifier      siprec
    network-interfaces siprecinterface:0.4
```

8.3 Session Recording Servers

Create the ASC SIPREC session-recording server object using the ASC SRS private address and the agreed SIP transport. In the supplied lab, the server object ascsrcs points to 10.213.0.76 using TCP port 5060.

No session-agent object is required for the active ASC SIPREC path in the supplied configuration. The session-recording server object and SIPREC group provide the recording destination.

GUI Path: session-router / session-recording-server

ACL Path: configure terminal > session-router > session-recording-server

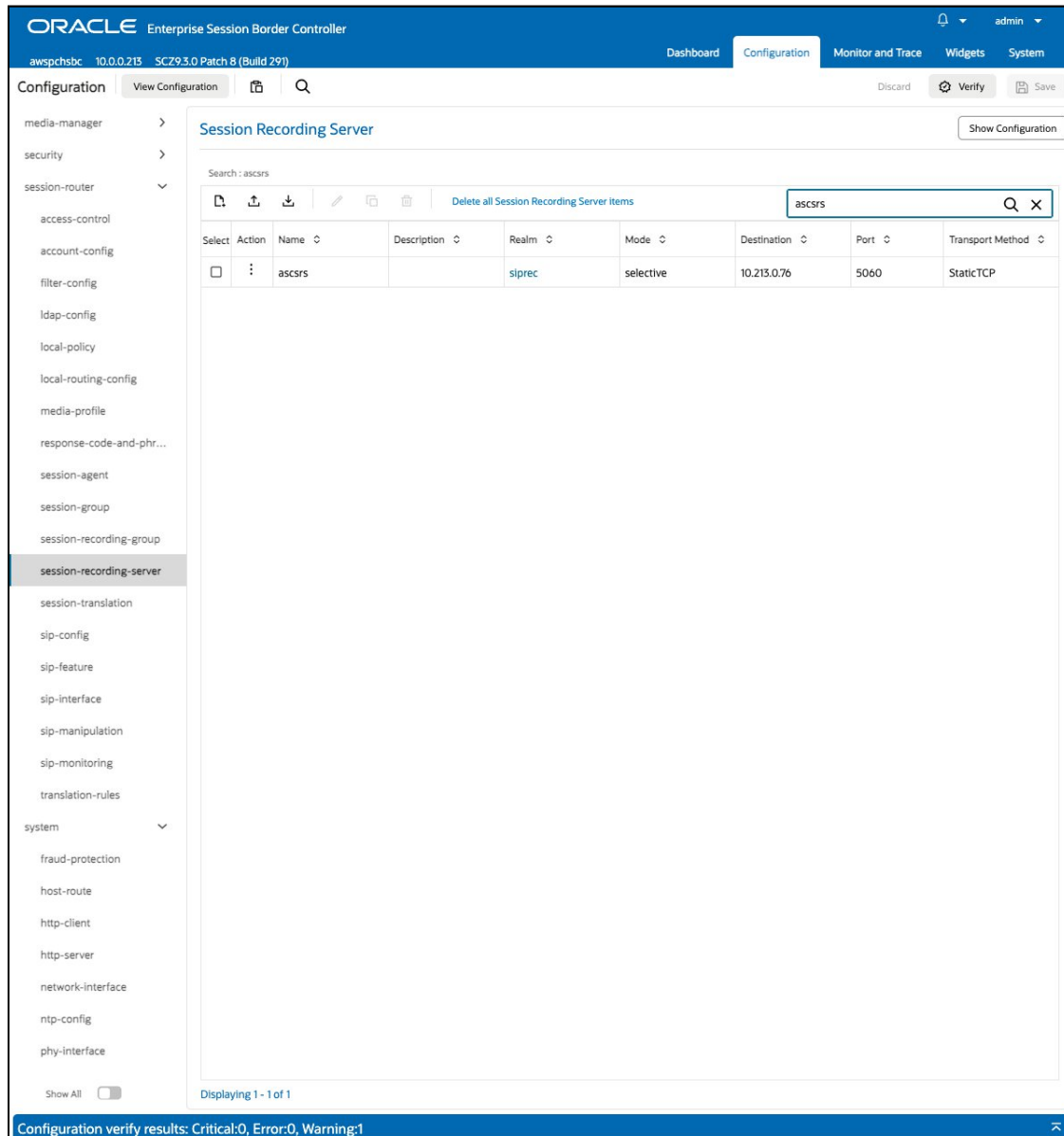


Figure 9 - Oracle SBC GUI: ASC session-recording-server ascsrs.

```
session-router
  session-recording-server
    name      ascsrs
    realm     siprec
    destination 10.213.0.76
    port      5060
    transport-method StaticTCP
    mode      selective
```

8.4 Session Recording Group

Create the ASC SIPREC group ascsrg and associate it with ascsrs. Associate the monitored genesys realm with SRG:ascsrg so applicable calls create the separate SIPREC recording session.

GUI Path: session-router / session-recording-group

ACL Path: configure terminal > session-router > session-recording-group

The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-recording-group' selected. The main content area, titled 'Session Recording Group', contains a table with the following data:

Select	Action	Name	Description	Strategy	Simultaneous Recording Servers	Session Recording Servers
☐		ascsrg		Hunt	1	ascsrs

Below the table, a 'Configuration verify results' section shows a warning: 'Disk size on this vSBC (14.6GB) is less than the recommendation'.

Figure 10 - Oracle SBC GUI: ASC session-recording-group ascsrg.

```
session-router
  session-recording-group
    name ascsrg
    session-recording-servers ascsrs
    strategy Hunt
    simultaneous-recording-servers 1
```

8.5 No Custom SIP Header Manipulation Required

No SIP manipulation or custom SIP header is configured on the active ASC SIPREC path. This is intentional because ASC does not require custom headers for this deployment.

GUI Path: session-router / sip-manipulation

ACL Path: configure terminal > session-router > sip-manipulation

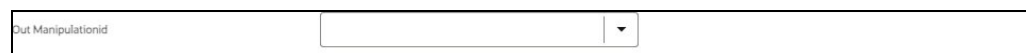


Figure 11 - Oracle SBC GUI: no outbound SIP manipulation configured for the ASC path.

Do not use header manipulation rules or custom SIP headers unless ASC has provided a documented requirement and the resulting SIPREC INVITE has been validated.

The Oracle SBC generates SIPREC metadata using its standard SIPREC behavior. Preserve the generated metadata and confirm participant identifiers, stream identifiers, call identity, and any agreed tenant or correlation information with ASC.

Note: The absence of ASC-specific SIP manipulation in the supplied lab is intentional. Any future metadata mapping must be approved by ASC and validated in both the outbound SIPREC INVITE and the ASC recording result.

No SIP manipulation is attached to the ASC SIPREC realm.
Validate unique participant and stream id values in SIPREC XML.
Add an HMR only if ASC documents and validates a future requirement.

9. SIPREC Signaling and Metadata Validation

The Oracle SBC initiates a SIPREC INVITE to the ASC SRS for applicable monitored calls. The INVITE contains SIPREC metadata and SDP describing the recording streams.

Field	Oracle SBC Source	Use / design consideration
SIPREC participant and stream IDs	Oracle SBC-generated SIPREC XML	Confirm unique participant and stream identifiers in the outbound SIPREC INVITE and in ASC.
Custom SIP headers	None configured on the ASC SIPREC path.	None in the supplied lab. Add only if ASC documents a requirement and the resulting SIPREC INVITE is validated.
Request-URI / To	Oracle SBC SIPREC signaling and configured ASC SRS destination 10.213.0.76:5060.	Oracle SBC SIPREC signaling to the configured ASC SRS destination through the AWS site-to-site VPN.
Original call identity	Original call information carried in SIPREC metadata where available.	Preserve calling/called context and agreed metadata rather than reconstructing it.
SIPREC XML and SDP	Oracle SBC-generated recording session.	Participant/stream association, codec/media description, and metadata validity.
Recorded media	Forked media associated with the SIPREC session.	Validate separate participant streams and ASC service-specific media requirements.

In the supplied ASC lab path, the Oracle SBC sends SIPREC sessions through the ASC SIPREC group to 10.213.0.76 using TCP port 5060. No ASC-specific SIP headers are added. Validate the outbound SIPREC XML and the resulting ASC recording against the agreed deployment requirements.

This application note documents the supplied configuration and validation approach. It does not by itself assert an end-to-end production recording pass. Complete the verification steps in this note before accepting the integration.

Preserve original call identity and dialog context in the SIPREC metadata. Confirm that participant and stream identifiers remain unique and that any agreed ASC correlation information is represented as required.

Transfer and consultation-call scenarios require additional validation. Confirm recording continuity, participant and stream correlation, and any agreed ASC metadata behavior across the call lifecycle.

10. Verify Connectivity

Run a controlled SIPREC test call through the AWS site-to-site VPN. Confirm that the Oracle SBC creates the SIPREC session, the ASC SRS is reachable at the configured private destination, and ASC receives the signaling, metadata, and media expected for the target deployment.

The following commands are useful during validation:

```
show rec
show configuration realm-config
show configuration session-recording-server
show configuration session-recording-group
show configuration network-interface siprecinterface
```

```
show rec
show configuration realm-config
show configuration session-recording-server
show configuration session-recording-group
show configuration network-interface siprecinterface
```

Configuration View Configuration Discard Verify Save

Session Recording Group Show Configuration

Select	Action	Name	Description	Strategy	Simultaneous Recording Servers	Session Recording Servers
☐	⋮	ascsrc		Hunt	1	ascsrcs

Configuration verify results: Critical:0, Error:0, Warning:1

Severity	Message	Object	Attribute Name	Other Object
WARNING	Disk size on this vSBC (14.6GB) is less than the recommendation			

Figure 12 - Oracle SBC configuration verification after ASC changes: 0 critical, 0 errors, and one disk-size advisory warning.

Validate the following during the controlled test:

SIPREC signaling reaches the ASC SRS through the AWS site-to-site VPN.

The SIPREC metadata contains unique participant and stream identifiers, and any ASC tenant or correlation information follows the agreed deployment requirements.

The ASC SRS accepts the SIPREC session at the configured private address and transport.

Original call identity and dialog context are preserved in the SIPREC metadata.

Recorded media, stream association, DTMF behavior, and any required recording policy are validated with ASC.

Transfer, consultation, and multi-party scenarios are validated separately, including recording continuity and participant/stream correlation.

Appendix A - Sanitized SBC Configuration Excerpts

The following sanitized excerpt consolidates the relevant captured SBC configuration for the ASC SIPREC proof path. It includes the call-session objects, the monitored and recording realms, the SIPREC interface, and the session recording server and group. Secrets, VPN pre-shared keys, certificates, and management credentials are omitted.

A.1 Active Call and SIPREC Recording Configuration

Configuration-derived excerpt captured after ASC SIPREC activation. Validate all local interface names and routing values before applying this example to another SBC.

The call-session entries represent the captured Genesys and Twilio call-facing topology. The ASC SIPREC recording path is established by the genesys realm association with SRG:ascsrc and the dedicated siprec realm.

```
# Captured call-session agents
session-router
  session-agent
    hostname  sollabawssbc.byoc.usw2.pure.cloud
    port      5060
    realm-id   genesys
  session-agent
    hostname  solawssbc.pstn.twilio.com
    port      5060
    realm-id   twilio

# Captured SIPREC-facing interface
system
  network-interface
    name      siprecinterface
    sub-port-id  0
    ip-address 10.0.3.101
    netmask    255.255.0.0
    gateway    10.0.3.1
    dns-ip-primary  8.8.8.8
    dns-ip-backup1  1.1.1.1
    dns-domain  telechat.o-test06161977.com

# Monitored call realm and SIPREC recording realm
media-manager
  realm-config
    identifier      genesys
    network-interfaces  PBXInterface:0.4
    session-recording-server  SRG:ascsrc
    # no out-manipulationid
  realm-config
    identifier      siprec
    network-interfaces  siprecinterface:0.4
    # no out-manipulationid

# ASC SIPREC recording session
session-router
  session-recording-server
    name      ascsrcs
    realm      siprec
    destination 10.213.0.76
    port      5060
    transport-method  StaticTCP
    mode      selective
  session-recording-group
    name      ascsrcg
    session-recording-servers  ascsrcs
    strategy    Hunt
    simultaneous-recording-servers 1
```

Back up the Oracle SBC configuration before making changes. Apply configuration changes in a controlled maintenance window and validate the SIPREC recording result with ASC before production deployment.

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/oracle
- x.com/oracle
- oracle.com

ORACLE

Oracle Corporation, World Headquarters

2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries

Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

Integrated Cloud Applications & Platform Services

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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. 0615

