Oracle® Cloud Native Session Border Controller

Release Notes

Release 1.26.0
G44181-02
May 2026

Oracle Cloud Native Session Border Controller Release Notes, Release 1.26.0

G44181-02

Contents

About this document

The Oracle Communications Cloud Native Session Border Controller (Cloud Native SBC) is designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Cloud Native SBC helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

This document provides information about new features in the Cloud Native SBC.

My Oracle Support

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

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

- For technical issues such as creating a new Service Request (SR), select **1**.
- For non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking, and Solaris Operating System Support, select **3**.

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

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

Revision History

This section provides a revision history for this document.

Date	Description
April 2026	Initial Release
May 2026	• Updates to Red Hat Openshift Container Platform version in RedHat Specifications and Services • Updates to known issues and resolved known issue

1

Introduction

Oracle Cloud Native Session Border Controller Release Notes provides following information:

- Overviews of the new features
- Technical Specifications and additional details
- Known issues and caveats
- Documentation Set

2

Technical Specifications

Following are the Cloud Native SBC technical specifications.

RedHat Specifications and Services

Following are the prerequisites for the RedHat platform. This list contains the mandatory services for the Cloud Native SBC.

Table 2-1 Prerequisites

Software Package	Version/Release	Description
Red Hat OpenStack Platform	17.1 or later	Cloud computing platform where the Cloud Native SBC is deployed.
Red Hat Openshift Container Platform	4.18 with patch 4.18.19 or later	Container platform where the Cloud Native SBC is deployed. **Note:** Refer to Red Hat's official documentation and select the appropriate RHEL version based on the compatibility matrix published by Red Hat.
Red Hat Enterprise Linux	9.4 or later	Operating system for the Cloud Native SBC.
Kubernetes	1.31 or later	Container orchestration platform for the Cloud Native SBC.
Prometheus or Thanos	As per platform	Collects and stores the Cloud Native SBC metrics.
Alert Manager	As per platform	Manages and monitors the Cloud Native SBC alerts generated by Prometheus monitoring system.
Grafana	As per platform	It is used to view the pre-configured Cloud Native SBC dashboards.
Logging Stack (EFK or LokiStack)	As per platform	Log visualization dashboard for the Cloud Native SBC logs.
NFS CSI Provisioner	As per platform	To enable the dynamic provisioning of RWX volume
Jaeger	As per platform	Distributed tracing platform for the Cloud Native SBC call traces.
cert-manager	As per platform	Used for automated TLS certificates via Certificate Authority, etc.

Table 2-1 (Cont.) Prerequisites

Software Package	Version/Release	Description
Core-dump management	As per platform	Manages core dump files. **Note -** The Cloud Native SBC toolset includes a core dump manager, designed to handle Cloud Native SBC core dump files, especially on platforms without built-in solutions for core dump management.
Openshift Router and Nginx	As per platform	It is used for Ingress management and external route handling.
Helm	As per platform	Used to deploy the Cloud Native SBC.
OpenShift Data Foundation Storage	As per platform	It is used to manage shared storage for the Cloud Native SBC.

Supported NICs and Drivers

In private virtual infrastructures, Cloud Native SBC supports the following interface input-output modes, ethernet controller, drivers, and traffic type based on input-output modes.

Supported Interface Input-Output Modes for Private Virtual Infrastructures

- Para-virtualized
- SR-IOV

Supported Ethernet Controller, Driver, and Traffic Type based on Input-Output Modes

The following table lists supported Ethernet Controllers (chipset families) and their supported driver that Oracle supports for the Cloud Native SBC deployments. Reference the host hardware specifications, where you run your hypervisor, to learn the Ethernet controller in use.

> **Note**
>
> The Cloud Native SBC does not support media interfaces when media interfaces of different NIC models are attached to the same pod(Signaling/Media/Transcode Engine) in a SR-IOV network mode.

Supported Virtual Network Interfaces and Drivers for Paravirtualization

For paravirtualization network mode, the following vNIC types are supported. You can use any make/model NIC card on the host as long as the hypervisor presents it to the virtual machine as one of these vNIC types.

Table 2-2 Virtual Network Interface

Virtual Network Interface	DPDK Driver	Interface
KVM (PV)	virtio	Media Interface

Supported Ethernet Controllers and Drivers for SR-IOV

For accelerated media/signaling using SR-IOV mode use the following card types.

Table 2-3 Ethernet Controller

Ethernet Controller	Driver	SR-IOV
Intel X710 / XL710 / XXV710	iavf	Media Interface
Intel E810	iavf	Media Interface

Supported Codec Types

The Cloud Native SBC supports a comprehensive set of industry-standard codecs for transcoding between codecs, ensuring compatibility and optimal media quality across a variety of network scenarios and endpoints. The table below details the currently supported codecs, associated bit rates, RTP payload types, and packetization intervals (ptime). Supported ptime values provide flexibility for different application requirements. Packetization times (ptime) up to 60 ms are supported for select codecs.

Codec	Supported Bit Rate (kbps)	RTP Payload Type	Default Ptime (ms)	Supported Ptime (ms)
G.711 PCMU	64	0	20	10, 20, 30, 40, 50, 60
G.711 PCMA	64	8	20	10, 20, 30, 40, 50, 60
G.722	48, 56, 64	9	20	20, 40, 60
G.723.1	5.3, 6.3	4	30	30, 60
iLBC	13.33	96-127	30	20, 30, 40, 60
	15.2	96-127	20	20, 30, 40, 60
G.729/A/B	8	18	20	10, 20, 30, 40, 50, 60
AMR	4.75, 5.15, 5.90, 6.70, 7.40, 7.95, 10.2, 12.2	96-127	20	20, 40, 60
AMR-WB (G.722.2)	6.6, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05, 23.85	96-127	20	20, 40, 60
G.726	16,24,32,40	2,96-127	20	10,20,30,40,50
EVS	5.9 to 128	96 - 127	20	20,40,60

Protocol and Stack Compatibility Matrix

The Protocol and Stack Compatibility Matrix provides an overview of supported network protocols and IP versions across different network interfaces in Cloud Native SBC. This matrix helps customers quickly determine which protocols are compatible with various network segments, including the internal Kubernetes pod network, service (signaling/media) networks, and external load balancer networks. Where a protocol is not relevant for a specific interface, it is denoted as N/A (Not Applicable). Use this table as a reference to ensure optimal deployment and interoperability with your network infrastructure.

Table 2-4 Protocol Stack Compatibility Matrix

Protocol	Primary Network(Kubernetes Internal Pod Network)	Service Network (Signaling/Media)	Kubernetes External Load balancer network
Inter-Pod communication	IPv4, IPv6	N/A	N/A
SIP over UDP/TCP/TLS	N/A	IPv4, IPv6	N/A
RTP	N/A	IPv4, IPv6	N/A
RTCP	N/A	IPv4, IPv6	N/A
SRTP	N/A	IPv4, IPv6	N/A
DNS	IPv4, IPv6	IPv4, IPv6	N/A
Lawful Intercept (X1 interface)	N/A	N/A	IPv4, IPv6
Lawful Intercept (X2 interface)	N/A	IPv4, IPv6	N/A
Lawful Intercept (X3 interface)	N/A	IPv4, IPv6	N/A
Configuration Manager's REST/HTTPS	N/A	N/A	IPv4, IPv6
Console GUI's HTTPS	N/A	N/A	IPv4, IPv6
CLI HTTPS	N/A	N/A	IPv4, IPv6
STIR/SHAKEN	N/A	IPv4, IPv6	N/A
CDR/SFTP	IPv4, IPv6	N/A	N/A
Core Dump Manager/ SFTP	IPv4, IPv6	N/A	N/A
Cloud Native SBC Operator to OpenStack Controller	IPv4, IPv6	N/A	N/A
Automated Test Suite GUI HTTPS	N/A	N/A	IPv4, IPv6
Automated Test Suite REST/HTTPS	N/A	N/A	IPv4, IPv6

3
New Features

Backup and Restore

The Backup and Restore Operator has been introduced to automate the backup and restore of Cloud Native SBC application configurations, enabling faster disaster recovery to ensure business continuity and minimize downtime. This feature supports both scheduled and on-demand backups, enabling enhanced data protection and operational flexibility. The entire backup and restore lifecycle—including task scheduling, verification, and secure storage in object storage—is managed via newly introduced custom resource definitions (CRDs). The administrators can perform seamless backups of configurations, LRT files, and CA certificate files. The Backup and Restore Operator is part of the Cloud Native SBC Operator component, and its lifecycle—including install, upgrade, rollback, and uninstall—is managed through the Cloud Native SBC Operator Helm chart.

Restoration is a one-time activity and temporarily restricts application upgrades during execution. For detailed setup instructions, refer to the Oracle Cloud Native Session Border Controller Installation Guide.

In addition, the Cloud Native SBC Console supports periodic and on-demand backups using Helm. For periodic backups, update the backup parameters in the Console values YAML file. Then run a Helm upgrade to apply the changes. For on-demand backups, create and apply a Kubernetes YAML manifest in the Console namespace. On-demand restore of the Console is currently not supported.

For more information about disaster recovery, refer to the Disaster Recovery chapter of the Oracle Cloud Native Session Border Controller Disaster Recovery Guide.

Overlapping IP Address Support Across VLANs

The Cloud Native SBC solution supports overlapping IP address ranges across multiple VLANs on a single interface by utilizing 802.1q VLAN tagging for both IPv4 and IPv6. Each physical network supports a maximum of 500 tagged service networks, with an overall limit of 1,500 tagged service networks across all physical networks. Service networks and the VLAN tagged networks are configurable through Cloud Native SBC Console GUI and Cloud Native SBC applications REST API. Any changes to service networks configuration takes effect after successful activation. Additionally, overlapping IP address functionality remains available during high availability switchovers, ensuring continuous operation, scalability, and manageability in line with other Cloud Native SBC Console features.

> **Note**
>
> The Service Network parameters have been moved from the Cloud Native SBC application values YAML file to the Cloud Native SBC Console GUI.

To learn more about overlapping IP support and the types of service network, refer to the Service Network Element chapter in the Oracle Cloud Native Session Border Controller User Guide.

To learn more about the REST APIs associated with the service network, refer to the Oracle Cloud Native Session Border Controller Application REST API Guide.

SIPREC Functionality

The Cloud Native SBC's SIPREC(Session Initiation Protocol Recording) functionality offers a targeted call recording solution designed to enhance both media and signaling efficiency on recording servers. It enables selective recording capabilities, and effectively isolates the Recording Server (RSS) from the active communication session.

To learn more about the SIPREC functionality, refer to the Selective Call Recording SIPREC chapter in the Oracle Cloud Native Session Border Controller User Guide. For information on the metrics and alerts associated with SIPREC, see the Oracle Cloud Native Session Border Controller Observability Guide.

Emergency Location Identification Number (ELIN) Support

The Cloud Native SBC supports Emergency Location Identification Number (ELIN) gateways for integration with E911 service providers. The gateway replaces VoIP extension URIs with ELIN numbers during emergency calls, enabling accurate location identification and reliable user callbacks. The Cloud Native SBC supports ELIN numbers, employing intelligent reuse to accommodate multiple concurrent E911 calls. An internal mapping table retains ELIN-to-extension associations for a configurable period, ensuring Public Safety Answering Point (PSAP) callbacks reach the correct caller.

For more information about ELIN support, refer to the Emergency Location Identification Number (ELIN) Gateway Support chapter in the Oracle Cloud Native Session Border Controller User Guide.

SNMP Support for Prometheus Alert Manager

The Cloud Native SBC supports Management Information Base (MIB) files, enabling seamless integration of Prometheus Alert Manager webhook support for SNMP traps. This feature allows you to leverage SNMP-based alerting and enhances observability and operational responsiveness within the Cloud Native SBC. The Cloud Native SBC requires Prometheus Alert Manager for alarm management and does not support observability tools that do not integrate with Prometheus. SNMP v2 and v3-compatible MIB files define all alert rules, simplify trap receiver configuration, and ensure smooth integration with observability systems. Each SNMP trap includes unique Object Identifiers (OIDs) mapped to Cloud Native SBC alerts, supporting efficient categorization and troubleshooting in trap receiver logs.

For more information about SNMP alerts, refer to Alert Manager chapter in the Oracle Cloud Native Session Border Controller User Guide.

Integration of Cloud Native SBC with Microsoft Teams

The Cloud Native SBC can integrate with Microsoft Teams, allowing organizations to securely connect on-premises telephony systems with Teams. This supports Microsoft Teams integration in Non-media bypass mode only, providing a secure and interoperable bridge between legacy telephony infrastructure and Microsoft 365. Proper configuration and Microsoft certification for Direct Routing are required.

For more information about integration of Cloud Native SBC with Microsoft Teams, refer to the Configuring Objects to integrate MS Teams section in the Realms and Nested Realms chapter of the Oracle Cloud Native Session Border Controller User Guide.

Enhanced Support for Virtualized Cloud Environments with Intel E810 Network Interface

For accelerated media and signaling workloads using SR-IOV mode, Cloud Native SBC supports the Intel E810 Ethernet controller with the iavf driver, providing optimized performance for media interfaces in high-throughput environments. This enhancement enables organizations to leverage the latest generation of optical network interfaces from Intel, supporting performance, compatibility, and future-ready scalability.

To learn more about Intel E810 network interface card (NIC), refer to the Supported NICs and Drivers section in the Oracle Cloud Native Session Border Controller Release Notes.

Cloud Native SBC Bare Metal Deployment on Red Hat Openshift

The Cloud Native SBC supports deployment on Red Hat Openshift environments running on bare metal infrastructure. This enables carriers and enterprises to reduce complexity and lower total cost of ownership by running Cloud Native SBC workloads on Openshift deployed on bare metal. All Cloud Native SBC components—including the Cloud Native SBC application, Cloud Native SBC Console, Cloud Native SBC Operator, Automated Test Suite, and Data Collector—are fully supported in Openshift bare metal environments. SR-IOV network mode is supported with Openshift bare metal. Organizations running previous releases of Cloud Native SBC can upgrade to this release. Orchestration tooling remains unchanged, with continued support for Prometheus exposition format, OpenTelemetry, and Multus for multiple vNIC assignments. All features are available on Openshift bare metal, with platform-specific validation provided as needed.

For detailed information about preparing the platform to install Cloud Native SBC, refer to the Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift on Bare Metal. For instructions on installing Cloud Native SBC for OpenShift on bare metal, refer to the Oracle Cloud Native Session Border Controller Installation Guide

Documentation Changes

The following information outlines the documentation changes included in this release.

- The book previously titled Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift has been renamed to Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift on OpenStack.
- The book previously titled Oracle Cloud Native Session Border Controller GUI Guide has been renamed to Oracle Cloud Native Session Border Controller Console GUI Guide.
- The Oracle Cloud Native Session Border Controller Platform Preparation Guide OCCNE has been removed from the Cloud Native SBC documentation package.
- The Cloud Native SBC documentation package includes two new books titled as below:
  - Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift on Bare Metal
  - Oracle Cloud Native Session Border Controller Troubleshooting Guide

4

Known Issues

The following topics list the known issues for the Cloud Native SBC. Oracle updates this document to distribute issue status changes. Check the latest revision of this document to stay informed about these issues.

Bug Severity

The Cloud Native SBC adopts the following four general definitions for bug severity

- Severity 1 - Critical/Complete loss of service.
- Severity 2 - Significant/Major/Severe loss of service.
- Severity 3 - Standard/Minor/Minimal loss of service.
- Severity 4 - Minimal/Informational/Minor error/No loss of service/Cosmetic.

Known Issues

Review the known issues before using the Cloud Native SBC. ORACLE is aware of these known issues and may resolve these in future releases. Refer the workarounds if available to handle the known issue and review this section periodically for updates.

Table 4-1 Known Issues

ID	Description	Severity	Found In
Internal bug	Any VLAN-tagged transcoding call flow that requires detecting RFC 2833 to interwork with other DTMF methods (RFC 2833, SIP-INFO, or inband) may fail because no DTMF is transcoded out.	2	• 26.0.0
Internal bug	Call rejections returned by an overloaded Media Engine may not be handled correctly by the Signaling Engine due to a race condition under sustained call load. This can occur when the Media Engine enters an overload state and then receives a new call request within the Signaling Engine–Media Engine registration refresh interval.	3	• 26.0.0

Resolved Known Issues

The following table provides a list of previous Known Issues that are now resolved.

Table 4-2 Resolved Known Issues

ID	Description	Severity	Found In	Fixed In

Internal bug	Deployment of Signaling, Media or Transcode Engine as a part of the Cloud Native SBC application package fails. The pod fails to reach the **Ready** state and displays an error in the vNIC injection job pod.
	
	`ERROR: Interface name not found for mac address xx:xx:xx:xx:xx:xx`
	
	Workaround: Run this command to delete the Cloud Native SBC Application pod that failed to reach **Ready** state.
	
	`kubectl delete pod <CNSBC application failed pod name> - n <namespace>`
	
	<namespace> is the Cloud Native SBC application namespace.
		2	• 25.1.0	• 25.1.0

Internal bug	Reviewing configurations changes for access-control element is not supported in Cloud Native SBC GUI.	3	• 25.1.0	• 25.1.1

Table 4-2 (Cont.) Resolved Known Issues

ID	Description	Severity	Found In	Fixed In
Internal bug	The Cloud Native SBC does not support sending STIR requests to an STI server located on a routed external network.	2	• 25.1.0	• 25.1.1
Internal bug	While the Transcode Engine processes moderate volume of media traffic in para-virtualized mode, intermittent DPWD crashes may occur. This could result in a minimal call impact.	2	• 25.1.0	• 25.1.1
Internal bug	In the Cloud Native SBC GUI, under **sip-manipulation > cfg-order**, the **Move Up** or **Move Down** option to re-order the manipulation rule does not appear on the first mouse click. This option is available under the **action** column, represented by a horizontal ellipsis icon. **Workaround:** Click the **actions** icon(represented by the horizontal ellipsis icon) twice to view the **Move Up** or **Move Down** option.	3	25.1.0	26.0.0
Internal bug	After a failover occurs in a high-availability (HA) setup, existing Denial of Service (DoS) entries for the previously active Signaling Engine do not reflect in the newly active Signaling Engine.	3	25.1.0	26.0.0

Table 4-2 (Cont.) Resolved Known Issues

ID	Description	Severity	Found In	Fixed In
Internal bug	Traces are not generated when the following conditions are met in sip-adv-log-trace element. • match-type is request-type • match procedure is exact-match or regex-match • match-value is any one of these - REGISTER, ACK, BYE, CANCEL, PRACK, OPTION, INFO, SUBSCRIBE, NOTIFY, REFER, UPDATE, MESSAGE, PUBLISH.	3	25.1.0	26.0.0
Internal bug	Advanced logs are not generated when the following conditions are met in sip-adv-log-trace element. • match-type is request-type • match procedure is exact-match or regex-match • match-value is any one of these - ACK, BYE, CANCEL, PRACK, INFO, REFER	3	25.1.0	26.0.0

Table 4-2 (Cont.) Resolved Known Issues

ID	Description	Severity	Found In	Fixed In
Internal bug	The Transcode Engine may go into disabled state when it takes on the active role during a Transcode Engine failover. Once disabled, it remains in that state until the pod is restarted. **Workaround:** Use the TEDisabledStateDetected application alert to learn more about the Transcode Engine's state. **Note:** Refer to the Oracle Cloud Native Session Border Controller Observability Guide to learn more about this alert - TEDisabledStateDetected.	3	26.0.0	26.0.1

Caveats

Review the caveats before using the Cloud Native SBC. These caveats talk about the Cloud Native SBC's unexpected behavior as per design. ORACLE is aware of these caveats that do not have a workaround. Review this section periodically for updates.

Transcoding Caveats

Software-based transcoding on the Cloud Native SBC is only supported on servers with INTEL CPUs.

CPU Resource Configuration Unavailable in Cloud Native SBC Console Database

The Cloud Native SBC Console database does not support CPU resource configuration.

Console Core URL

If you update the **coreStaticIpAddress** parameter in the Console values YAML file and upgrade the Console, then manually update the IP address of the Console Core in the home URL for your client **sbc** from the IAM's UI(Clients page).

Large Configuration Limitation

It is advisable to operate within a limit of 50,000 configuration objects and attributes to ensure optimal performance and minimize the risk of service degradation. This number can vary

depending on the mix of various configuration element types. For large configurations, it is recommended to save and activate configuration during times of low traffic. Future updates are road mapped to further enhance performance and will allow for higher configuration limits.

It is also recommended to configure a minimum of 3 minutes for both **clientTimeout** and **serverTimeout** when setting up timeouts in load balancer during platform preparation.

For more information on the factors that influence the activation of configurations, refer to the Oracle Cloud Native Session Border Controller Console GUI Guide.

ARP Limitation

Any Signaling, Media, or Transcode Engine pod can support a maximum of 4000 ARP entries at any time. This limit applies regardless of the number of service networks configured.

VLAN Limitation

A maximum of 500 tagged service networks is supported per physical network. A total of 1500 tagged service networks are supported across all physical networks.

Signing Certificate Storage Restrictions in Cloud Native SBC Application Namespace

Signing certificates, including private Root CAs or Intermediate CAs, should not be stored within the Cloud Native SBC application namespace. If these certificates are present, the Configuration Manager may display them in the list of end-entity certificates, and configuration activation with these certificates will not be successful. Attempting to use such certificates within a TLS profile will cause the activation of the configuration to fail, including for Automated Test Suite, as signing certificates cannot function as end-entity certificates.

Rollback from Cloud Native SBC Console 1.26.0 to 1.25.X Not Supported

Perform an in-service software upgrade of the Cloud Native SBC Console from releases 1.25.X to 1.26.0 as supported. Do not attempt an in-service software rollback from 1.26.0 to releases 1.25.X, as this is not supported due to uplifts in the Console IAM. If a rollback is necessary, follow the disaster recovery procedure to back up and reinstall the Console component. Refer to the Oracle Cloud Native Session Border Controller Disaster Recovery Guide for detailed instructions.

Manual removal required for older alert rules when upgrading to 1.26.0

When upgrading from release 1.25.1 to 1.26.0, alert rules are now managed by the helm chart instead of manual deployment through YAML files. As a result, existing alert rule CRs created manually in prior versions are not upgraded or removed automatically during the upgrade process. You must manually uninstall older alerting rules before or after upgrading to ensure proper alert management and avoid duplication or conflicts.

Refer to the Oracle Cloud Native Session Border Controller Installation Guide for detailed information on alert rules files.

Two-Factor Authentication (2FA) Not Supported on Cloud Native SBC Console IAM

Two-factor authentication (2FA) is currently not supported on the Cloud Native SBC Console IAM.

5

Documentation Set

The Oracle Communications Cloud Native Session Border Controller documentation set includes the following:

Table 5-1 Documentation Set

Document Name	Document Description
Oracle Cloud Native Session Border Controller Release Notes	Contains information about the current documentation set release, including new features and technical specifications.
Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift on OpenStack	Contains information about preparing your RedHat OpenShift platform on OpenStack for installing the Cloud Native SBC.
Oracle Cloud Native Session Border Controller Platform Preparation Guide for OpenShift on Bare Metal	Contains information about preparing your RedHat OpenShift platform on Bare Metal for installing the Cloud Native SBC.
Oracle Cloud Native Session Border Controller Installation Guide	Contains information about the prerequisites, customizations required and steps on how to install, uninstall, rollback, upgrade and maintain the Cloud Native SBC.
Oracle Cloud Native Session Border Controller Operator Guide	Contains information about the components of the Cloud Native SBC Operator and how to troubleshoot the Operator.
Oracle Cloud Native Session Border Controller Application REST API Guide	Contains a list of all REST endpoints in the Cloud Native SBC API and how to configure the system using those endpoints.
Oracle Cloud Native Session Border Controller IAM REST API Guide	Contains a list of all REST endpoints in the Identity Access Management API and how to manage access tokens using those endpoints.
Oracle Cloud Native Session Border Controller Console GUI Guide	Contains information about how to configure the Cloud Native SBC using the Console GUI.
Oracle Cloud Native Session Border Controller User Guide	Contains information about the Cloud Native SBC's distributed architecture and its various components along with the various features.
Oracle Cloud Native Session Border Controller Console Guide	Contains information about the various components of the Cloud Native SBC Console, how to access it and the roles available to manage the Cloud Native SBC configurations.
Oracle Cloud Native Session Border Controller Automated Test Suite Guide	Contains information about how to install and use the Automated Test Suite.
Oracle Cloud Native Session Border Controller Transcoding Guide	Contains information about the transcoding architecture, supported code types, transcoding configurations and many more.
Oracle Cloud Native Session Border Controller Observability Guide	Contains information about the Cloud Native SBC metrics, alerts and Grafana dashboards.
Oracle Cloud Native Session Border Controller Header Manipulation Rules Guide	Contains information about the Cloud Native SBC's SIP manipulation language called Header Manipulation Rules (HMR).

Table 5-1 (Cont.) Documentation Set

Document Name	Document Description
Oracle Cloud Native Session Border Controller Disaster Recovery Guide	Contains information on how to recover the Cloud Native SBC during various disaster scenarios.
Oracle Cloud Native Session Border Controller Security Guide	Contains information about the security best practices required for deploying and operating the Cloud Native SBC securely in a cloud native environment.
Oracle Cloud Native Session Border Controller License Document	License document for the Cloud Native SBC.
Oracle Communications Cloud Native Session Border Controller X123 Guide	Contains information on how the Cloud Native SBC implements standards-based X1/X2/X3 lawful intercept (LI) in VoIP and VoLTE networks.
Oracle Cloud Native Session Border Controller Troubleshooting Guide	Contains information to help you efficiently identify and resolve common issues encountered when using the Cloud Native SBC.