Oracle® Communications Security Shield Cloud Service

What's New

F25146-16
February 2023

Oracle Communications Security Shield Cloud Service What's New,

F25146-16

Contents

About This Guide

What's New describes new features, known issues, caveats, and limitations for the Oracle® Communications Security Shield (OCSS) update.

Documentation Set

The following table describes the documents included in the Oracle® Communications Security Shield (OCSS) documentation set.

OCSS Installation and Maintenance Guide	Contains conceptual and procedural information for installing and maintaining the OCSS.
OCSS License Document	Contains information about the OCSS license.
OCSS Security and Privacy Guide	Contains conceptual and procedural information for securing the OCSS operations.
OCSS User's Guide	Contains the product overview along with conceptual and procedural information about using the OCSS Dashboard.
OCSS What's New	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.

Related Documentation

The following list describes related documentation for the Oracle® Communications Security Shield (OCSS). You can find the listed documents on http://docs.oracle.com/en/industries/communications/ in the "Session Border Controller Documentation" section.

ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Communications Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes Web GUI configuration used for the SIP Monitor and Trace application.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
Maintenance and Troubleshooting Guide	Contains information about Oracle Communications Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.

Revision History

The following table provides the revision history for this document. Oracle updates the whole documentation set with each software release. When one or more of the documents requires an update between software releases, Oracle issues an interim update limited to the affected documents.

Date	Revision
June 2020	20.0.0.0.0
July 2020	20.1.0.0.0
October 2020	20.2.0.0.0
February 2021	20.3.0.0.0
April 2021	Interim Documentation Update • Adds the Caveat that the Cloud Communication Service (CCS) does not support simultaneous use of the same CCS instance.
June 2021	21.0.0.0.0
August 2021	21.1.0.0.0
November 2021	21.2.0.0.0
February 2022	21.3.0.0.0
May 2022	22.0.0.0.0
August 2022	22.1.0.0.0
November 2022	22.2.0.0.0
February 2023	23.0.0.0.0

Documentation Accessibility

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

1

New Features and Enhancements

The following topics describe new features and enhancements for Oracle® Communications Security Shield releases.

Topics:

23.0.0.0.0 - February 2023

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield (OCSS) release.

The following table describes the new features and enhancements in the OCSS 23.0.0.0.0 release.

Features	Description
Enhanced User Alerts Notifications	The 23.0.0.0.0 release enhances notifications about threatening call activity by adding electronic messaging directly to subscribers by way of email, Slack, and PagerDuty services. The new Subscriptions sub-tab on the OCSS Notifications tab displays information about the subscribers configured to receive notifications when OCSS detects threat conditions. The Subscriptions sub-tab also displays the Create Subscription button to launch the configuration dialog, as well as filters for search operations. See "The Notifications Subscriptions Tab" in the *OCSS User's Guide*.

Features	Description
Additional Insights to Call Scores	The 23.0.0.0.0 release adds more information about call scores to the analytical reports by providing greater explanation of the reason codes and call behaviors. To help you see the additional information, Oracle added the new Call Insights attribute to the Total Calls Table canvas. Call Insights provides the following information: • Application-to-Person (A2P)—Reason codes specific to application-to-person messaging. For example, verification codes, appointment reminders, One Time Passcodes, verification messages, or other calls sent to a user. • Person-to-Person (P2P)—Reason codes specific to human-to-human calls. • Number Type—The line type or phone type information. • Activity—Reason codes related to the amount of activity OCSS observed for the number, compared to what is expected for a good user. For example, the number of communications transactions to or from the number, the quantity of unique numbers communicated with, and the number of accounts communicated with. A privileged administrator can add the Call Insights attribute to an existing canvas. See "Policy Results Statistics Attributes" and "Policy Results Threats Attributes" in the *OCSS User's Guide*.

22.2.0.0.0 - November 2022

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield (OCSS) release.

The following table describes the new features and enhancements in the OCSS 22.2.0.0.0 release.

Features	Description
Enhanced Analytics Reports	Oracle significantly enhanced the usability and focus of the OCSS analytics functionality. With one click of the new Analytics Reports button on the Dashboard, OCSS displays a single, new default Project (a collection of canvases) displaying commonly requested visualizations that provides real-time, interactive viewing capabilities. From the default Project, you can create customized Projects to which you add canvases and visualizations. You can export, duplicate, move, and save Projects. As before, you can export canvases, data, and images from the visualizations on the canvases. See the "Call Traffic Analytics" Appendix in the *OCSS User's Guide*.
Access Control List Enhancement	Oracle enhanced the Access Control List functionality to allow you to create policies based on calling number and called number. For example, you might want block or redirect specific calling numbers for specific destinations, such as company executives or to block harassing callers from reaching specific agents. Access Control Lists contain rules that you create for Calling and Called numbers. When you create a rule, you can specify the Calling Number, the Called Number, or both. You can add multiple numbers to a rule and you can specify ranges of numbers, the call direction, and the enforcement action. See "Add an Access Control List" and "Add a Rule to an Access Control List" in the *OCSS User's Guide*.
Manage Nonconforming Calling Numbers	When a calling number does not conform to E.164 phone number conventions, even after normalization, OCSS provides you with ways to specify call treatment and reports threats from nonconforming calling numbers to the Threats by Count tile on the Dashboard. Nonconforming call management applies to both the Standard and Premium editions. See "How OCSS Manages Nonconforming Calling Numbers" in the *OCSS User's Guide.*

Features	Description
Enhanced Access Control List Processing	OCSS processes Access Control Lists (ACL) independently from regular threat processing and an action taken due to an ACL match overrides decisions made due to threat analysis. Due to the override, previous versions of OCSS omitted threat processing of calls for which an ACL match was determined. As of the 22.2.0.0.0 release, calls that match an ACL rule will also be fully analyzed for threat status. The threat status will be reported as part of the OCSS Dashboard statistics and will be available in the analytics environment. OCSS reports both the ACL status and the threat status of the call, although the ACL decision still overrides.

22.1.0.0.0 - August 2022

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield (OCSS) release.

The following table describes the new features and enhancements in the OCSS 22.1.0.0.0 release.

Features	Description
Inbound Call Labeling	When an inbound call goes through OCSS, OCSS adds the P-OCSS-Call-Info header to the SIP INVITE. The information in the header can help you make more informed decisions about your network. For example, you might want to route certain types of calls to a particular queue, or require extra validation, or restrict the caller's options. See "Inbound Call Labeling" in the *OCSSC User's Guide*.
Notifications Tab	The 22.1.0.0.0 release adds the Notifications tab to the Web GUI. OCSS displays notifications when certain call-related conditions occur that might need your attention, for example, elevated risky call types and other kinds of calls from bad actors. On the Notifications tab, privileged users can view a watch list of notifications and configure notifications settings. See "The Notifications Tab" in the *OCSSC User's Guide*.

Features	Description
Enhanced Dashboard Update Behavior	Beginning with the 22.1.0.0.0 release, OCSS updates the Dashboard upon call initiation and other events rather than solely upon call termination. OCSS uses any available information upon call initiation and can update the Dashboard with new information as the call progresses. OCSS no longer restricts the display to reporting only about terminated calls. The result is better synchronization with the analytics reports, which report on calls when they arrive.
Emergency Number Treatment Description	When the Session Border Controller (SBC) receives a call with a calling number containing an emergency number (currently limited to 100, 108, 111, 112, 181, 911, and 999,) the SBC (SPL) will not invoke a query to OCSS. Emergency calls will proceed as normal.

22.0.0.0.0 - May 2022

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield (OCSS) release.

The following table describes the new features in the OCSS 22.0.0.0.0 release.

Features	Description
Support for Session Border Controller-to-Cloud High Availability	You can configure the Session Border Controller (SBC) to distribute Oracle® Communications Security Shield (OCSS) traffic to as many as three Cloud Communication Service (CCS) instances to provide continuity of service if one or more CCS instances stops responding or loses connectivity to the cloud. See "Support for SBC to Cloud High Availability" in the *Installation and Maintenance Guide*.
Subscription Suspension and Termination Process	If you do not renew your Oracle® Communications Security Shield (OCSS) subscription before the scheduled end date, Oracle provides a phased continuation process that allows you more time to renew before hard termination. See "Subscription Usage" and "Subscription Suspension and Termination Phases" in the *User's Guide*.
Support for Inbound Phone Number Normalization	The Oracle® Communications Security Shield (OCSS) uses the E.164 format for call validation from the Session Border Controller. Because OCSS may be used in environments that use number formats other than E.164, OCSS provides a way to normalize non-E.164 number format conventions to the E.164 convention. See "Inbound Phone Number Normalization" in the *User's Guide*.

Features	Description
Support for Creating Customized Analytics Reports	As a privileged user, you can create custom Oracle® Communications Security Shield (OCSS) analytics reports to display the type of data you want to see in the format you want. You can create custom OCSS analytics reports from call elements, filters, calculations, and formats that you choose. See "Create Customized Analytics Reports" in the *User's Guide*.

21.3.0.0.0 - February 2022

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield (OCSS) release.

The following table describes the new features in the OCSS 21.3.0.0.0 release.

Features	Description
OCI Identity Domain Support	The 21.3.0.0.0 release supports the Oracle Cloud Infrastructure (OCI) Identity Domain for new and existing customers. Oracle will migrate existing customers seamlessly without service impacts in the coming months. See "OCI Identity Domain: What OCI Identity Domain Customers Need to Know" and "OCI Identity Domain: What Oracle IDCS Customers Need to Know" in the *OCSS Installation and Maintenance Guide*.

Features	Description
Updates to Reputation Score call classifications	The 21.3.0.0.0 release updates the classifications shown in the Reputation Score Classification configuration and in the Dashboard tiles for Autonomous Threat Protection, Call Classifications and Top Targeted Enforcement Points. • Reputation Score Classification—In the Reputation Score Classification configuration, "Unclassified" is renamed "Acceptable" and "Regular" is renamed "Good." See "Reputation Score Classification" in the *User's Guide*. • Autonomous Threat Protection—The Autonomous Threat Protection Dashboard tile no longer counts or reports "Acceptable" (formerly "Unclassified") calls as detected threats. See "Autonomous Threat Protection" in the *User's Guide*. • Call Classification—The Call Classification Dashboard tile consolidates the former pair of graphs into one graph. To customize the display, you can click the items in the legend to show or hide their data according to what you want to see in the graph. See "Call Classifications" in the *User's Guide*. • Top Targeted Enforcement Points—The Top Targeted Enforcement Points Dashboard tile no longer counts or reports "Acceptable" (formerly "Unclassified") calls as detected threats. See "Top Targeted Enforcement Points" in the *User's Guide*.

21C - November 2021

The following information describes the new content and behavior delivered in the Oracle® Communications Security Shield (OCSS) 21C release.

The following table describes the new features in the OCSS 21C release.

Features	Description
Replace the Calling Number Identification	The 21C release adds support for specifying the phone number you want displayed to the called party in calling line identification. See "Outbound Calling Line Identification Management" in the *OCSS User's Guide*.

Features	Description
Support for Oracle Communications Session Router	The 21C release supports the Oracle Communications Session Router. The Oracle Communications Session Router works in environments that use Oracle Session Border Controllers to integrate withOCSS as well as environments that do not use Oracle Session Border Controllers to integrate with OCSS. See the Session Border Controller *Platform Preparation and Installation Guide* if you use Oracle Communications Session Border Controllers. If not, see the documentation for the device that you use.
Disable Mid-Call Updates	The 21C release adds a way to enable or disable mid-call updates by entering or omitting the WAN certificate and private key paths in the Cloud Communication Service (CCS) activate.pl script. See "Enable or Disable Mid-Call Updates" in the *OCSS Installation and Maintenance Guide*.
Updates to the CCS Configuration page on the Settings tab.	The 21C release adds the OCSS FQDN and IDCS FQDN elements to the information provided on the CCS Configuration page on the Settings tab. See "Cloud Communication Service Configuration Settings" in the *OCSS User's Guide*.
Block calls that do not pass STIR validation.	The 21C release adds the **Block Inbound Calls that Fail STIR Validation** parameter to the General Settings configuration on the Autonomous Threat Protection settings tab. When enabled, OCSS overrides the reputation score enforcement action configuration for a call that does not pass STIR verification and blocks the call. See "Autonomous Threat Protection Settings" and "Edit General Settings" in the *OCSS User's Guide*.
Session Plug-in Language (SPL) Show Commands	The 21C release adds a list of SPL show commands that you can access through the Acme Command Line Interface (ACLI). See "OCSS Sow Commands" in the *OCSS Installation and Maintenance Guide*.
The following functions that were present but not operational in the preceding release are now operational.	The 21C release supports the following operations: • Validating outbound calls • Adding P-Asserted Identity • Modifying FROM in the presentation number See "The Outbound Call Validation Tab" chapter in the *OCSS User's Guide*.

Features	Description
Call Type Classifications update	The 21C release updates the Call Type Classifications for low-value, no-value, and other unwanted incoming calls for Premium Subscribers. Go to the Settings tab and click the Call Type Classifications link to see the classification types, descriptions, and configurable enforcement actions. Go to the Dashboard tab to see the Threats by Count tile, which displays the number of threats received per classification type per period of time.

21B Update 1 - August 2021

The following information describes the new content and behavior delivered in the Oracle® Communications Security Shield (OCSS) 21B Update 1.

The following table describes the new features in the OCSS 21B Update 1.

Features	Description
Support for the Standard Subscription	21B Update 1 adds support for the Standard OCSS subscription. See "OCSS Service Plans Comparison" in the *User's Guide*.
Mitigate Call Flooding	OCSS can detect and mitigate call flooding by monitoring the inbound call rate per phone number and applying configurable enforcement actions when the rate exceeds the threshold you set. OCSS can detect call flooding caused by Telephony Denial of Service, Traffic Pumping, and Toll Fraud. See "Call Flooding Mitigation" in the *User's Guide*.
Create a List of Outbound Enterprise Calling Numbers	The OCSS GUI displays the Outbound Call Validation tab and allows you to create a list of outbound enterprise phone numbers with configurable attributes. **Note:** OCSS does not support applying the functionality of call validation and attribute use to call traffic at this time. See "The Outbound Call Validation Tab" chapter in the *User's Guide*.

Features	Description
Number Lookup Tab	The Number Lookup tab provides a way to search for a phone number across all of your OCSS phone number lists. The resulting display shows every list and states whether or not the number is on the list. The search results show the settings for the number per type of list. See "The OCSS Number Lookup Tab" chapter in the *User's Guide*.
Block Calls with "Anonymous" in FROM	OCSS adds support for blocking inbound calls that contain Anonymous in one or both of the FROM and P-Asserted Identity headers and one or both of the user name and host name parts. For example, suppose a fraudster removes the user identity and inserts anonymous@, private@, restricted@, user@example1.edu, null@ or other such entries in the FROM or the P-Asserted Identity (PAI) headers. The result makes the caller identification anonymous and unverifiable. You can block such calls. See "Edit General Settings" in the *User's Guide*.
Support for Multi-Factor Authentication	To make the Oracle® Communications Security Shield (OCSS) more secure, you can enable multi-factor authentication for user log on. See "Secure Access to OCSS with Multi-Factor Authentication" in the *Installation and Maintenance Guide*.

21B Release - June 2021

The following information describes the new content and behavior delivered in the Oracle® Communications Security Shield (OCSS) 21B release.

New Features

The following table describes the new features in the OCSS 21B release.

Features	Description
New user groups to support least privileged access	The 21B release adds a set of user groups to help you manage access to OCSS according to the least amount of privilege needed. The privileges of each group determine which tabs, links, and information the user can see and which actions the user can perform. See "User Groups and Privileges" in the *Installation and Maintenance Guide*.

Features	Description
Policy Decision Engine Relocation to the Oracle Cloud Infrastructure	The 21B release relocates the Policy Decision Engine (PDE) from an on-premises deployment to the Oracle Cloud Infrastructure (OCI). In the OCI, Oracle manages and maintains the PDE. Customers no longer need to install the PDE on premises. Oracle recommends that customers using a release prior to 21B, where the PDE is installed on-premises, uninstall the PDE to reduce the OCSS footprint on local resources.
Auto Refresh Rate for Dashboard Tiles	The 21B release adds the Auto Refresh control to the Dashboard for setting the rate at which the tiles refresh. You can use the default refresh rate or choose one from the menu that displays when you click Auto Refresh. See "The Dashboard Tab" in the *User's Guide*.
Change in the SPL Plug-in Download Method	The 21B release packages the SPL Plug-in with the Cloud Communication Service download. See "Download the OCSS Software" in the *Installation and Maintenance Guide*.
Call Rate Limiting for a TDoS Attack	The 21B release adds call rate limiting as an enforcement method when the OCSS detects a Telephony Denial of Service (TDoS) attack. You can specify the maximum rate of calls that you want the OCSS to allow as a way of mitigating a TDoS attack. When incoming calls exceed the specified call rate, the OCSS drops calls randomly such that the rate of calls allowed to traverse the SBC matches the configured Call Attempt Rate Limit that you set for the **Network-wide TDoS and Overload Protection** parameter in the Threat Vector Thresholds configuration. The 21B release removes call blocking as an available enforcement action for a TDoS attack. The remaining values are Allow and Rate Limit. See "Threat Vector Thresholds" in the *User's Guide*.

Behavioral Changes

The following information describes behavioral changes to the OCSS service.

Objects	Description
Threat Vector Thresholds parameters	• The Threat Vector Thresholds tab no longer displays the Toll-Free Traffic Pumping parameter because the 21B release does not support Toll-Free Traffic Pumping as a fraudulent call volume mitigation. • The 21B release renames the TDoS (Telephony Denial of Service) parameter as Network-Wide TDoS and Overload Protection. • The available enforcement actions for the Network-Wide TDoS and Overload Protection parameter are Allow and Rate Limit. The 21B release does not support the former Block enforcement action.
Toll-Free Traffic Pumping	The 21B release does not support the Toll-Free Traffic Pumping parameter for fraudulent call volume mitigation.

20B Update 3 - February 2021

The following information describes the new features and enhancements delivered in the Oracle® Communications Security Shield (OCSS) 20B - February 2021 update.

New Features

The following table describes the new features in the OCSS 20D - February 2021 update.

Features	Description
Activity Logging	OCSS adds a way to view user activity logs through the new Activity Log tab to help with troubleshooting and security audits. You can see activity such as configuration changes to access control lists, threshold parameters, and on-premises software components for periods of up to ninety days. The activity log supports search operations with various filters to help you find the logs you want to see, for example, Date Range, User, Category, and Action. The logs display the following information: Timestamp, User, Device, Category, Object ID, Action, and Activity Details.

Features	Description
No-value and low-value call detection for Premium Subscribers	To help Premium Subscribers get a more accurate understanding of the risks to their call centers and to help them to continuously improve responses to risky and unwanted calls, OCSS replaced the former rather general Risky calls category with an expanded set of no-value and low-value Call Type Classifications. The no-value and low-value Call Type Classifications provided for Premium subscribers include Scam, Other Fraud, Robocall, Telemarketing, and Invalid-Spoofing Number. For each of the new Call Type Classifications, you can set one of the following actions that you want OCSS to apply to these calls through the new Call Type Classifications dialog on the Settings page: Block, Redirect, and Continue. By applying actions to the call classifications, you can use OCSS to shield your customer service agents and other employees from calls that waste time, harm productivity, and cause unwanted expenses. Premium subscribers can see data about Call Type Classifications activity on the OCSS Dashboard in the Threats by Count tile and in the Autonomous Threat Protection tile because the OCSS reputation scoring operations will also use these classifications when determining call reputation scores.
Simulate a Call Lookup	On the Access Control Lists tab, the All Numbers List page adds the Simulate Look up button. Use Simulate Lookup when you want to know how the Policy Decision Engine will enforce access control on a particular phone number on your list. OCSS can process the phone number through a call simulator and return the result, which shows the call direction, the enforcement action that the Policy Decision Engine will apply, and the name of the list that contains the phone number. In this way, you can see whether or not the enforcement action is what you want and you can adjust it, if needed..

20B Update 2 - October 2020

The following information describes the new features and enhancements delivered in the Oracle® Communications Security Shield (OCSS) 20B - October 2020 update.

New Features

The following table describes the new features in the OCSS 20B - October 2020 update.

Features	Description
Access Control Lists	The 20B - October 2020 update replaces the previous list management with the new Access Control Lists tab and extends the functionality by allowing you to create, delete, and rename your own lists. In prior versions, the access control lists hard-coded the call direction and action for all numbers on a list. The new list management allows you to apply any direction or action to any number on any list. You can create up to ten Access Control lists. In the left pane of the Access Control Lists tab, the system displays the All Numbers List, which is a view of all of the phone numbers from all of your lists combined. The All Numbers view can make searching easier when you do not recall which list contains the number you want to find. From the view list, you can perform a simulated phone number lookup to see how the OCSS Policy Decision Engine will enforce access control on a specified phone number if it were used in a real call. See the "Access Control Lists" chapter in the User's Guide.

Enhancements

The following table describes the new enhancements in the OCSS 20B - October 2020 update.

Enhancements	Description
Reputation Score Classifications	The 20B - October 2020 update renames the call classifications and adds a unique set of call classifications for the Premium subscription level. The revisions also affect the Dashboard display. See "Standard Subscription Call Classifications" and "Premium Subscription Call Classifications" in the User's Guide.

20B Update 1 - July 2020

The following information describes the new features and enhancements delivered in the Oracle® Communications Security Shield (OCSS) 20B - July 2020 update.

New Features

Features	Description
Configuration Wizard	To help you set the initial configuration with minimal effort, the OCSS service provides a configuration Wizard. The Wizard asks you questions and uses your answers to set various parameters for managing and securing call traffic. You can use the Wizard for the initial set up as well as for subsequent changes that you want to make. After you run the Wizard you can customize the settings through the Dashboard. See "The OCSS Configuration Wizard" chapter in the User's Guide.

Enhancements

Enhancements	Description
Dashboard—Autonomous Threat Protection tile	• The Autonomous Threat Protection tile gains a link to the Configuration Wizard. Click the tile and click Edit to reach the link. See the "Configuration Wizard" chapter in the User's Guide. • The Autonomous Threat Protection tile no longer links to the Reputation Score Classification settings dialog. The link is relocated to the Settings page. See "Call Classifications" in the User's Guide.
Dashboard—Threats by Count tile	The Threats by Count tile on the Dashboard displays the new Risky Calls category, which is a composite of the High Risk, Suspicious, and Unclassified reputation scores. The tile no longer displays the Low and Medium labels due to the changes described in the following row in this table. See "Threats by Count" in the User's Guide.

Enhancements	Description
Dashboard—Call Classification tile	• The Call Classification tile on the Dashboard displays new visual elements and a different array of classifications to provide more descriptive information about the numbers and types of calls evaluated. • The OCSS 20B - July 2020 update replaces the former Low Risk label with the new Regular label. Regular calls, which are low risk, attained a reputation score from 61-90. The former Medium Risk label is replaced and divided among the new Suspicious, Not Attested, and Unclassified labels. Suspicious calls attained a reputation score from 41-60, Not Attested calls attained a score from 91-95, and Unclassified calls attained a reputation score from 96-100. (High Risk calls, which retains the same label, attain a reputation score from 0-40.) See "Call Classifications" in the User's Guide.
Dashboard—Top Targeted Enforcement Points tile	The Top Targeted Enforcement Points tile on the Dashboard adds the new Risky Calls category, which is a composite of High Risk, Suspicious, and Unclassified calls. The tile no longer displays the Low and Medium labels due to the changes described in the preceding row in this table. See "Top Targeted Enforcement Points" in the User's Guide.
Dashboard—Settings Page	• Reputation Score Classification—The Settings page gains a link to the Reputation Score Classification settings dialog, which you previously reached through the Autonomous Threat Protection Settings tile. (The link is removed from the Autonomous Threat Protection Settings tile.) See "Reputation Score Classification" in the User's Guide. • Configuration Wizard—The Settings page adds a link to the Configuration Wizard. See the "Configuration Wizard" chapter in the User's Guide.

2
Upgrade Information

The following topics provide important information you need to know the before an Oracle® Communications Security Shield upgrade. For some releases, you might need to perform certain tasks before the upgrade. Releases not listed required no upgrade documentation.

Topics:

Upgrade Information for the 22.1.0.0.0 Release

Oracle recommends that you review the following information about upgrades before using Oracle® Communications Security Shield (OCSS).

Edit the Cloud Communication Service Configuration (CCS) File After the Upgrade

Existing OCSS customers must edit the CCS configuration file for the 22.1.0.0.0 release.

> **Note:**
>
> New OCSS customers do not need to perform this update.

1. If you run call traffic at 150cps, set the value of the `Client-Session-Pool` parameter in the CCS configuration file /opt/oracle/ccs/cfg/cfg.json to 25. If you do not run calls at 150cps, you do not need to change the `Client-Session-Pool` value.

   ```
   Client-Session-Pool: 25
   ```

2. All customers must set the value of the `trans-limit` parameter in the CCS configuration file /opt/oracle/ccs/cfg/cfg.json to 500.

   ```
   Trans-Limit: 500
   ```

3. Execute the script /opt/oracle/ccs/perl/deactivate.pl. You must enter “y” to confirm and proceed.
4. Execute the script /opt/oracle/ccs/perl/activate.pl. You must enter “y” to confirm proceed.

Upgrade Information for the 22.0.0.0.0 Release

Oracle recommends that you review the following information about upgrades before using Oracle® Communications Security Shield (OCSS).

Save Custom Analytics Reports Before the Upgrade

When Oracle upgrades OCSS, the process may affect analytics reports stored in the OCSS folder in certain circumstances. The OCSS folder is the folder where OCSS automatically keeps the default analytics reports and initially any that you create. Under certain circumstances during an upgrade, OCSS overwrites the default reports and deletes any other reports in the OCCS folder.

You must take steps before the upgrade to preserve any reports that you want after the upgrade by moving them out of the OCSS folder. See "Save Analytics Reports Before an Upgrade" in the *User's Guide*.

Edit the Cloud Communication Service Configuration (CCS) File After the Upgrade

Existing OCSS customers must edit the CCS configuration file for the 22.0.0.0.0 release.

1. In the CCS configuration file /opt/oracle/ccs/cfg/cfg.json, edit the value for the Client-Session-Pool parameter to a new value of 15.

   ```
   Client-Session-Pool: 15
   ```

2. Execute the script /opt/oracle/ccs/perl/deactivate.pl. You must enter “y” to confirm and proceed.
3. Execute the script /opt/oracle/ccs/perl/activate.pl. You must enter “y” to confirm proceed.

> **Note:**
>
> New OCSS customers do not need to perform this update.

Reload the Web GUI Browser Page After the Upgrade

After an OCSS software upgrade, copies of the styles, javascript, and images stored in your web browser cache for the Web GUI will be out of sync with what is on the web server for the new release. You must reload the browser you use for the OCSS Web GUI with a hard refresh to load the newly upgraded version.

- Google Chrome, Mozilla Firefox, and Microsoft Edge—Hold the **Shift** key and click the **Reload** button next to the address bar. When you hold **Shift** and click **Reload** , the browser fully reloads the OCSS Web GUI with all of the latest HTML, images, styles, JavaScript code, and so on from the web server and re-displays the OCSS Web GUI.

> **Note:**
>
> If you click only **Reload**, the browser will load the HTML but not the images, styles, JavaScript code, and so on that you need to use the OCSSC Web GUI.

3

Known Issues, Caveats, and Limitations

The following topics list the known issues, caveats, and limitations for Oracle® Communications Security Shield (OCSS). Oracle updates this information regularly to distribute issue status changes or add new issues. Check the latest version of this document to stay informed about changes to known issues and caveats.

Topics:

- Known Issues—Known Issues describes issues that Oracle is aware of and may address in a future release. Known Issues contain descriptions of the issues and workarounds, when available.
- Caveats—Caveats explains certain behaviors that you might not expect, but which work as designed. Caveats do not include workarounds.
- Limitations—Limitations explains facts about functional or operational boundaries that you need to know. Limitations do not include workarounds.

Known Issues

Oracle recommends that you review the Known Issues before using Oracle® Communications Security Shield (OCSS). Known Issues describes issues that Oracle is aware of and may address in a future release. Known Issues contain descriptions of the issues and workarounds, when available. Check this document periodically to stay informed of updates and other new information.

Bad REST Request Received Alert

Issue: OCSS sends the alert when the Upper Threshold value for Traffic Pumping in Business Hour is greater than the value set for Telephony Denial of Service (TDoS) Threshold. The Upper Threshold for Traffic Pumping must always be less than the TDoS Threshold.

Workaround: After running the Config Wizard, verify the TDoS and Traffic Pumping settings and correct them, if needed.

Clear a Filter on an Analytics Visualization

Issue: After you filter data in a visualization or table in an analytics canvas by clicking on a particular data point, you can clear the filter to return the visualization to its previous state. One way to clear a filter is to move your cursor into the white space above the canvas (top, right). OCSS displays a second hamburger menu. Click "Clear All Filter Selections" from the hamburger menu. This method is currently out of service.

Workaround: To clear the filter, click in the white space in the visualization to which you applied a filter. OCSS returns the visualization to its previous state.

Allocate a Separate IP Address for Use By OCSS

Issue: Session Border Controller release 8.4.0 deletes ports when the HTTP client IP address has ports in a steering pool used by SIP.

Workaround: Oracle recommends allocating a separate IP address for use by OCSS, instead of sharing an IP address used by SIP.

Call History Time Stamp Issue

Issue: On the OCSS dashboard, the time stamp in the Call History data preview window usually displays a one hour time frame. For example: 9:00:00 AM - 9:59:59 EST. When the local time is in a time zone that is on the half hour (GMT +5:30) rather than an hour (GMT +5:00), the data preview time stamp displays only one half hour. For example, 9:30:00 AM - 9:59:59 AM IST instead of instead of 9:00:00 AM - 9:59:59 AM IST. Regardless of the time stamp, the data preview displays an hour's worth of data.

> **Note:**
>
> To see a data preview window, hover over a point on the Call History graph.

Oracle Analytics Reports Default to View-only

Issue: The OCSSAnalyticsEditor role allows the user to edit Oracle Analytics reports, but the Oracle Analytics landing page defaults to the presentation (view-only) mode which does not allow editing. The OCSSAnalyticsEditor must change the report mode (displayed in the URL) from the default "presentation" mode to the editing mode, called "full" mode. This issue applies to the Call Statistics report and the Call History report, which are linked to the respective tiles on the OCSS Dashboard.

Workaround:

1. Click **Analytics** on the Dashboard.
2. On the Oracle Analytics page, locate the word **presentation** in the URL.
3. Change **presentation** to **full**.

> **Note:**
>
> The URL change does not persist. For example, suppose you click the Call Statistics tile and edit the URL on the Oracle Analytics landing page. When you finish working with the Call Statistics report, suppose you go back to the Dashboard and click the Call History tile. You must edit the URL again on the Oracle Analytics landing page before you can edit the Call History report.

Multiple Users and Activity Log Viewing

Issue: When User1 is viewing the Activity Log and User2 makes changes to a configuration, User1 does not immediately see the changes.

Workaround: User1 must refresh the page to see User2's changes.

Empty Row for Terminated Calls in the Calls Table

Issue: In the Calls table, launched from the Call History tile, the table displays two rows for terminated calls. One row shows the Call End Time and Call Duration cells with no values. The other row correctly shows valid values in the Call End Time and

Call Duration cells. Disregard the row with no values in the Call End Time and Call Duration cells.

OCSS Tenant ID Gets Removed From the URL After Authentication

Issue: After authentication by way of Identity Authentication Management (IAM) completes, the system redirects the user to the OCSS Dashboard. In the redirection process, the URL displayed in the browser's address box is incorrect. The resulting URL is not sufficient for bookmarking the Dashboard. For example: To access the OCSS dashboard, you enter `https://iad.ocss.ocs.oraclecloud.com/ocss983945sol/admin/ui/` into the browser. After providing credentials for IAM, the Dashboard URL displays as `https://iad.ocss.ocs.oraclecloud.com/admin/ui/`.

Workaround: Manually add the missing part of the URL to the bookmark.

Tab Key Behavior

Issue: The tab key allows you to tab to each element on the Dashboard, whether the element is a link or not. The tab key should only move to linked elements on the page.

Caveats

Oracle recommends that you review the following Caveats before using Oracle® Communications Security Shield (OCSS). A Caveat explains certain behaviors that you might not expect, but which work as designed. Caveats do not include workarounds. Check this document periodically to stay informed of updates and other new information.

Outbound Call Validation List - Call Tags

When configuring a phone number for the Outbound Calling Number list, you can select an Internet Engineering Task Force (IETF) Call Tag attribute for the phone number. Note that the Call-Tag does not affect the outbound INVITE at this time, but setting the call tag does help to refine your searches at this time.

Cloud Communication Service Configuration

The Cloud Communication Service (CCS) does not support simultaneous use of the same CCS instance by different services,for example, OCSS and Oracle Session Delivery Manager Cloud (OSDMC). You must configure each CCS instance to support only one service.

The Dashboard Might Display Multiple Data Points for the Same Call

The OCSS evaluates a call based on multiple algorithms, such as Fraud, Reason Codes, and Reputation Score. The OCSS gives each call a reputation score and classifies the call as one of Critical Risk, Severe Risk, Significant Risk, Suspicious, Unclassified, or Regular. Whenever the OCSS identifies a call as a threat, for example TDoS, it is very likely that the call will be classified as one of the high risk categories based on the reputation score assigned to that call. Due to this behavior, you might see multiple threats reported on the Dashboard for the same call. For example, the call might be reported in both the TDoS and Critical Risk graphs. You might see the same behavior for threats categorized based on Reason Codes.

Limitations

The following information describes operational limitations of Oracle® Communications Security Shield (OCSS). Limitations explains the facts of functional or operational boundaries.

Limitations do not include workarounds. Check this document periodically to stay informed of updates and other new information.

Data Visualization Rendering in OCSS Dashboard and Analytics

When the stored call data volume increases, rendering the visualizations may take longer. Especially, the time it takes to load and update data for the Analytics Reports can take longer depending on the amount of data that OCSS needs to process and render.

Lookup Requests

By default, OCSS limits the rate of lookup requests to 50 per second. The lookup service rejects requests that exceed this rate. OCSS automatically allows calls with rejected lookup requests. You must contact your sales representative when you want a higher call rate supported

4
Documentation Changes

The following topics list and describe changes to the documentation, per release. Releases not listed contained no documentation changes.

Topics:

22.1.0.0.0 - August 2022

The following information describes changes to the documentation for the Oracle® Communications Security Shield (OCSS) 22.1.0.0.0 release.

OCSSC User's Guide

- Adds "The Notifications Tab" chapter.
- Moves some topics from the "Overview" chapter into the new "How OCSS Works" chapter.

OCSSC Installation and Maintenance Guide

- Adds the "Activate Debug in CCS" topic to the "OCSS Maintenance" chapter.

22.0.0.0.0 - May 2022

The following information describes changes to the documentation for the Oracle® Communications Security Shield (OCSS) 22.0.0.0.0 release.

OCSSC User's Guide

- Moves the "OCSS Enforcement Actions" topic from Appendix A to the "Overview" chapter.
- Adds Appendix B "Custom Analytics Reports".

21.3.0.0.0 - February 2022

The following information describes structural changes to the documentation for the Oracle® Communications Security Shield (OCSS) 21.3.0.0.0 update.

OCSS Installation and Maintenance Guide

- Adds the "Changes to IDCS and OCI Identity Domain Operations" Appendix.
- Adds the "Federated Sign-on" topic to the "Post Service Activation Tasks" chapter.
- Moves the "Session Router Support" topic to the "OCSS Deployment Overview" chapter.

OCSS User's Guide

- No structural changes

OCSS What's New

- Adds the "Upgrade Information" chapter.

21C - November 2021

The following information describes changes to the documentation for the Oracle® Communications Security Shield (OCSS) 21B Update 2 release.

OCSS Installation and Maintenance Guide

- Adds the "Session Router Support" topic to the "Post-Deployment Configuration Tasks" chapter.

OCSS User's Guide

- Adds the "Session Border Controller to OCSS Connectivity" topic to the "OCSS Overview" chapter.

21B Update 1 - August 2021

The following information describes changes to the documentation for the Oracle® Communications Security Shield (OCSS) 21B Update 1 release.

OCSS Installation and Maintenance Guide

- Adds references throughout to the Standard subscription.
- Adds the "Post-Deployment Configuration Tasks" chapter.
- Moves the "User Groups and Privileges" topic into the "Post-Deployment Configuration Tasks" chapter.
- Adds the "Configure Multi-Factor Authentication" topic to the "Post-Deployment Configuration Tasks" chapter.

OCSS User's Guide

- Adds references throughout to the Standard subscription.

- Adds the Outbound Call Validation Tab chapter.

> **Note:**
>
> Functionality is limited on the Outbound Call Validation tab. The documentation provides information about the current functionality, only.

- Adds the Number Lookup Tab chapter.

21B Release - June 2021

The following information describes changes to the documentation for the Oracle® Communications Security Shield (OCSS) 21B release.

OCSS Installation and Maintenance Guide

- Removes references to the Standard subscription because the 21B release does not support the Standard subscription.

OCSS User's Guide

- Removes references to the Standard subscription because the 21B release does not support the Standard subscription.