Oracle® Communications Security Shield Cloud Service

What's New

F25146-23
May 2024

Oracle Communications Security Shield Cloud Service What's New,

F25146-23

Contents

About This Guide

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

Documentation Set

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

Security Shield Installation and Maintenance Guide	Contains conceptual and procedural information for installing and maintaining the Security Shield.
Security Shield License Document	Contains information about the Security Shield license.
Security Shield Security and Privacy Guide	Contains conceptual and procedural information for securing the Security Shield operations.
Security Shield User's Guide	Contains the product overview along with conceptual and procedural information about using the Security Shield Dashboard.
Security Shield 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 Cloud Service (Security Shield). 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 update limited to the affected documents.

Dates	Release Numbers and Revisions
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	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
May 2023	23.1.0.0.0
August 2023	23.2.0.0.0
November 2023	23.3.0.0.0
December 2023	23.3.0.0.0 Updates the following topics in the *Installation and Maintenance Guide* to include Podman for Oracle Linux 8: • Install, Configure, and Activate the Cloud Communication Service • Deactivate the Cloud Communication Service • Update the Cloud Communication Service
January 2024	23.3.1.0.0.0 • Adds the Trusted Enterprise Call subscription
February 2024	24.0.0.0.0
May 2024	24.0.4.0.0

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 Cloud Service releases.

Topics:

24.0.4.0.0 May 2024

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

The following table describes the enhancements in the Security Shield 24.0.4.0.0 release.

Table 1-1 New Features and Enhancements

Features and Enhancements	Description
Cloud Communication Service Supports TLS 1.3	The Cloud Communication Service (CSS) supports TLS 1.3 in addition to the versions currently supported. • Customers installing CCS for the first time do not need to do anything specific. • Existing customers who are updating their CCS version need to modify their cfg/cfg.json file with the following changes, marked in bold, before activating the new CCS. **Instructions for Modifying the cfg/cfg.json File** "LAN": { "Server-Addr": "0.0.0.0", "Server-Port": 8000, **"TLS-Cipher-Suite": "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384", <<<------ Weak ciphers are removed "TLSv13-Cipher-Suite": "TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384", <<<------ New line added** "TLS-Server-Cert": "./ssl/lan-cert.pem", "TLS-Server-Key": "./ssl/lan-key.pem", "TLS-Server-DH": "./ssl/dh2048.pem", "TLS-Client-CA-Path": "./ssl/ca", "TLS-Client-Verify": true, "API-Key-Verify": true }, "WAN": { "Server-FQDN": "ccs.tesla.com", "Server-Addr": "0.0.0.0", "Server-Port": 443, "TLS-Cipher-Suite": "ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384", **"TLSv13-Cipher-Suite": "TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384", <<<------ New line added** "TLS-Server-Cert": "./ssl/wan-cert.pem", "TLS-Server-Key": "./ssl/wan-key.pem", "TLS-Server-DH": "./ssl/dh2048.pem", "TLS-Client-CA-Path": "./ssl/ca", "TLS-Client-Verify": true, "IDCS-FQDN": "idcs.oraclecloud.com", "IDCS-Port": 443, "IDCS-Tenant-ID": "idcs-tenant-id", "IDCS-Verify": true }

24.0.0.0.0 February 2024

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

The following table describes the new features and enhancements in the Security Shield 24.0.0.0.0 release.

Table 1-2 New Features and Enhancements

Features and Enhancements	Description
Updated User Interface (continued)	Oracle continued updating the Security Shield User Interface (UI) to align with Oracle styles and standards. You may notice slight variations in behavior, which are documented in the *User's Guide* along with new screen captures of the affected UI.
New Scoreboard for Trusted Enterprise Calls	Oracle added the new Answered Outbound Calls scoreboard metric card to the Dashboard to support the Trusted Enterprise Calls subscription. The Answered Outbound Calls scoreboard metric card displays the number of outbound calls that were answered, and when selected, a dashboard with the following content displays: • Call answer rate—Shows the percentage of the number of outbound calls that were answered in the last 24 hours. • Top outbound numbers by call volume—Shows the top fifteen attested outbound phone numbers and the top fifteen unattested outbound phone numbers that were answered in the last 24 hours. • Average call duration by type—Shows the average duration of attested and unattested calls in minutes and notes the percentage of difference between the two in the last 24 hours. See "The Dashboard" chapter in the *User's Guide*.
Short Number Processing Enhancement	To provide better results from phone number lookups, Oracle enhanced the lookup behavior for inbound calls as follows: • When a phone number contains fewer than seven digits, Security Shield will not perform the number lookup. In this way Security Shield avoids generating a lookup response with a high risk because the number does not comply with number plans, which can reduce false positive results.
Always Send the P-OCSS-Call-Info Header	Security Shield includes the P-OCSS-Call-Info header regardless of the lookup response so you can rely on the P-OCSS-Call-Info header for call treatment. See "P-OCSS-Call-Info Header Codes" in the *User's Guide*.

Table 1-2 (Cont.) New Features and Enhancements

Features and Enhancements	Description

New SPL Options for Inbound and Outbound Calls	The 24.0.0.0.0 release adds new SPL options to send only inbound or outbound calls to the Security Shield cloud.
	The SPL option "ocssEnabled" can allow the Session Border Controller to send both inbound and outbound calls to Security Shield for policy lookup. The SPL package provides the flexibility to choose whether you want to send only inbound calls or only outbound calls to Security Shield for policy lookup by way of the new "inboundOnly" and "outboundOnly" spl-option configurations.
	Configuration options:
	• spl-options ocssEnabled, inboundOnly—Allows only inbound calls
	• spl-options ocssEnabled, outboundOnly—Allows only outbound calls
	• spl-options ocssEnabled—Allows both inbound and outbound calls
	Configuration Examples:
	realm-config
	`spl-options ocssEnabled,inboundOnly`
	realm-config
	`spl-options ocssEnabled,outboundOnly`
	About the New SPL Package
	SPL version: 1.15.0.0 (Package Build : 1.14_20240124223927)
	Customers currently using Security Shield must upgrade their Session Border Controllers to the latest released SPL, but only after upgrading their tenant to the latest Security Shield release. Get the latest version available for download from Oracle Software Delivery Cloud or My Oracle Support. Install the SPL on the external-facing realm.

23.3.1.0.0 January 2024

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

The following table describes the new features and enhancements in the Security Shield 23.3.1.0.0 release.

Features and Enhancements	Description
Trusted Enterprise Calls	To help you achieve higher answer percentages and longer connection times for your outbound enterprise calls, Security Shield can optionally provide call signing and phone number attestation for trusted outbound enterprise calls. You can use the call attestation service completely through Security Shield or you can use your own call signing and attestation vendor in conjunction with Security Shield. You can use Trusted Enterprise Calls as a standalone subscription or you can use it with the Standard or Premium subscriptions. For North American customers, only. See "Trusted Enterprise Calls" in the *User's Guide*.

23.3.0.0.0 - December 2023

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

The following table describes the new features and enhancements in the Security Shield 23.3.0.0.0 release.

Features and Enhancements	Description
Support for Podman with Oracle Linux 8	Security Shield adds support for the Podman container engine for Oracle Linux 8. When you install the Cloud Communications Service during your Security Shield configuration, you can now choose either Podman or Docker as the container engine. In the *Installation and Maintenance Guide* see: • Install, Configure, and Activate the Cloud Communication Service • Deactivate the Cloud Communication Service • Update the Cloud Communication Service

23.3.0.0.0 - November 2023

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

The following table describes the new features and enhancements in the Security Shield 23.3.0.0.0 release.

Features and Enhancements	Description
Updated User Interface	Oracle updated the Security Shield User Interface (UI) to align with current styles and standards. You may notice slight variations in behavior, which are documented in the *User's Guide* along with new screen captures of the UI. For example, • Configuration dialogs are now called drawers because they slide out from the side of the page rather than pop up, as before. • Search fields support using supplied filter chips to help you narrow your search. • Navigation to the main pages occurs through a menu rather than by way of tabs, as before. • Information about your subscription displays when you click your initials on the banner rather than by way of a tile on the Dashboard, as before.
Changes to Reputation Score Classification Mappings	There are now only three classifications on the Reputation Score Classification page: Low Risk, Medium Risk, and High Risk. **Standard Subscription** • Former High Risk still maps to High Risk • Former Suspicious Risk now maps to Medium Risk • Former Acceptable Risk and Good Risk now map to Low Risk **Premium Subscription** • Former Critical Risk and Severe Risk now map to High Risk • Former Significant Risk and Suspicious Risk now map to Medium Risk • Former Acceptable Risk and Good Risk now map to Low Risk

Features and Enhancements	Description
Changes to Enforcement Action Mappings for Existing Tenants	The following changes apply to existing tenants following an upgrade. Existing tenants show six classifications, but will show only three after the upgrade. Security Shield merges existing classifications into the new ones as follows and gives precedence to the enforcement action noted with the asterisk. • Good and Acceptable combine to form Low Risk. • Significant Risk and Suspicious combine to form Medium Risk. • Severe Risk and Critical Risk combine to form High Risk. For example: Suppose you had set Block for Significant Risk and Allow for Suspicious in your existing configuration. After you upgrade, Security Shield combines those classifications into the new Medium Risk classification and prefers the enforcement action set for Suspicious. In this example, Security Shield displays Allow for the enforcement action for the Medium Risk classification. Note: After the upgrade, you can reset the enforcement action for the new classifications on the Reputation Score Classification page. Choices include Allow, Block and Redirect.
Enforcement Action Defaults for New Tenants	The following behavior applies to new tenants: • The High Risk enforcement action defaults to Block. • The Low Risk and Medium Risk enforcement actions default to Allow.

23.2.0.0.0 - August 2023

The following information describes the new content and behavior delivered in the latest Oracle® Communications Security Shield Cloud Service release.

The following table describes the new features and enhancements in the Oracle® Communications Security Shield Cloud Service 23.2.0.0.0 release.

Features and Enhancements	Description
Tenant-Based Exclusion List	You may have other departments, company locations, trusted affiliates, trusted partners, and other trusted entities that call you frequently. You can exclude phone numbers for those parties from risk assessment using a new enforcement action called "Exclude". Such high-frequency numbers may otherwise generate high-risk responses resulting in blocked calls, even though the numbers are trusted. To enable customers to exclude certain trusted high-frequency numbers from risk scoring, Oracle modified the behavior of the Allow enforcement action and added the new Exclude enforcement action. Allow—Oracle® Communications Security Shield Cloud Service ignores the risk assessment and allows the call with no further threat detection evaluation. Oracle® Communications Security Shield Cloud Service classifies the call as "Good." Exclude—Oracle® Communications Security Shield Cloud Service ignores the risk assessment and still evaluates the call against TDoS, Traffic Pumping, Spoofing, and Toll Fraud threat detection. Fraud Risk, Spam Risk and Call Center detection is bypassed. See "Access Control List Enforcement Actions" in the *Oracle® Communications Security Shield Cloud Service User's Guide.*

Features and Enhancements	Description
Analytics Reports Enhancement	Oracle created a new version of the Project Workbook and Data Set for the Oracle® Communications Security Shield Cloud Service Analytics reports for enhanced performance when loading the data set. The enhanced Project workbook and Data Set, called OCSS 2.0, contains all the same default reports and data points as before with no additions. Unlike the previous Project workbook, OCSS 2.0 uses materialization to pre-compute the data set. The advantage of materialization is faster loading times compared to querying the base table view of the data, which is especially beneficial for large data sets. Oracle recommends that you use filters to limit the data that is loaded for even greater efficiency. If you set the filters to the full 30 days, with all other filters disabled, loading times may be longer because the loading time is a function of the data size. Note: The materialization process updates the data set every five minutes, so you may notice that some new calls do not appear in the results right away. You can still use the original analytics Project Workbook and Data Set, called OCSS on the UI, with no modification required, for at least the duration of the 23.2.0.0.0. release. If you have existing reports based on the OCSS Project Workbook and Data Set, Oracle recommends moving them to the OCCS 2.0 Project because the OCSS Project Workbook and Data Set will reach end-of-life in the not distant future. Important: From the 23.2.0.0.0 release and forward, when you create a custom analytics Project, you must use OCSS 2.0. See "Call Traffic Analytics" in the *Oracle® Communications Security Shield Cloud Service User's Guide*.

Features and Enhancements	Description
Support for Multi-Factor Authentication to Cloud Account (OCI Console)	As part of continuous efforts to improve the security of Oracle Cloud Infrastructure (OCI), Oracle started the next phase of the Multi-Factor Authentication plan for the OCI Console. The new policy is designed specificity to help prevent the compromise of customer cloud accounts (OCI Console). It is not for access to the Oracle® Communications Security Shield Cloud Service Dashboard and analytics. To learn more about the policy, see About the "Security Policy for OCI Console" Sign-On Policy. **New Customers** All new Identity Access Management (IAM) domains and Identity Cloud Service (IDCS) stripes now include a sign-on policy named "Security Policy for OCI Console" seeded in the active state. **Existing Customers** After a two-week period of seeding the policy in a disabled state, Oracle will activate the policy for existing customers who do not activate it themselves. The Appendix at the end of this document explains the enforcement rules Oracle will apply. The new policy is in effect. Oracle is activating the "Security Policy for OCI Console" by default. If you want to opt out of Oracle automatically activating the policy, delete the "Security Policy for OCI Console" sign-on policy using REST APIs. See Delete a Policy For information about the enforcement rules Oracle applies to activating the new Multi-Factor Authentication policy for the OCI Console, see Appendix-A for What's New 23.2.0.0.0.
Cloud Communication Service (CCS) Patch Released	Oracle pushed Cloud Communication Service release 1.3.0.1 to My Oracle Support (MOS) as 1.12.10 (Program Increment 12, Patch 12). Ensure that your deployment uses the version of CCS in the 1.12.10 package. There are no CCS changes for Program Increment 13 (23.2.0.0.0).

Appendix-A for What's New 23.2.0.0.0

Oracle will not activate the Multi-Factor Authentication policy for Oracle Cloud Infrastructure (OCI) when an active external IDP (SAML/Social or X.509) is configured in the IAM domain or IDCS Stripe. When no external IDP is configured, the enforcement rule in the following table applies.

Table 1-3 Activation Rules

Tenancy Type	Sign-on Policy "Security Policy for OCI Console" status	The customer has defined its own sign-on policy for the OCI Console or has explicitly assigned the OCI Console to the default sign-on policy	Sign-on policy "Security Policy for OCI Console" status after forced activation
With IAM Domain (All domain types)	Present and enabled	N/A. When the customer has a sign-on policy in place, there is no change.	No Change.
	Present and disabled	No	Change the policy to Present and enabled
	Present and disabled	Yes	No Change. Oracle will not overwrite a customer-defined policy.
	Deleted	N/A	No change.
With IDCS Stripes Enabled (All IDCS Types)	Present and enabled	N/A. When the customer has a sign-on policy in place, there is no change.	No Change.
	Present and disabled	No	Change the policy to Present and enabled.
	Present and disabled	Yes	No Change. Oracle we will not overwrite a customer-defined policy.
	Deleted	N/A	No Change.

23.1.0.0.0 - May 2023

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

The following table describes the new features and enhancements in the Security Shield 23.1.0.0.0 release.

Features	Description
Policy Updates	Oracle streamlined how the Session Border Controller learns of policy updates after an initial response from OCSS, so that you no longer need to provision a network device to allow traffic into your network.

2

Upgrade Information

The following topics provide important information you need to know the before an Oracle® Communications Security Shield Cloud Service (Security Shield) upgrade. For some releases, you might need to perform certain tasks before the upgrade.

New Version

For enabling your Session Border Controller or Session Router to pull policy updates from Security Shield for calls, you must upgrade to the relevant S-Cx release and patch levels. SCz9.1.0p6 (or higher, when on 9.1.x release) or SCz9.2.0p1 (or higher, when on 9.2.x release). See your Customer Support Representative for more information.

Older Versions

Older versions rely on Security Shield pushing updates to your session Border Controller or Session Router in separate API calls originated by Security Shield. The pulling capabilities allow you to simplify your network configuration, including firewalls and proxies, because you do not need to create pinholes that might allow unexpected API calls to reach your network.

3

Known Issues, Caveats, and Limitations

The following topics list the known issues, caveats, and limitations for Oracle® Communications Security Shield Cloud Service (Security Shield). 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 Cloud Service (Security Shield). 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.

Limit to the Number of CSV Records Exported from DIS

Issue: Oracle observes unpredictability and errors when exporting a .csv file of more than two million records from DIS per attempt.

Workaround: Limit the export to fewer than two million records per attempt. Oracle recommends using multiple batches of fewer records per attempt. You can use the date range filter to create smaller batches.

Redundant Search Filter Suggestions on the Activity Log Page

Issue: When you click in the Search field on the Activity Log page, you may see the filter choices repeated in the list that Security Shield displays.

Workaround: None.

Redundant Search Filter Suggestions on the Notifications Page Subscriptions Tab

Issue: When you click in the Search field on the Subscriptions tab on the Notifications page, you may see the filter choices repeated in the list that Security Shield displays.

Workaround: None.

Intermittent Refresh Button Behavior

Issue: On the Dashboard page, the Auto Refresh button may occasionally not display.

Workaround: Refresh the page by clicking the browser refresh button. You may need to try more than once before the Auto Refresh button re-displays.

The Save Button May Disable on the Notifications Settings Page

The Save button may become inactive or not display at all when changing the settings back and forth on the Notifications Settings page.

Analytics Report Error Message

Issue: When you click View Analytics Report, the Dashboard displays an error message that says "Something Went Wrong". The error message displays when you click Analytics Report on the Security Shield UI or when you refresh the browser.

Workaround: Click OK on the error message, then click Projects and Reports.

Allocate a Separate IP Address for Use By Security Shield

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 you upgrade the Session Border Controller software to release 9.x. If you need to stay on release 8.4., allocate a separate IP address for use by Security Shield, instead of sharing an IP address used by SIP.

Call History Time Stamp Issue

Issue: On the Security Shield 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.

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.

Security Shield 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 Security Shield 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 Security Shield 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.

Caveats

Oracle recommends that you review the following Caveats before using Oracle® Communications Security Shield Cloud Service (Security Shield). 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.

Cloud Communication Service Configuration

The Cloud Communication Service (CCS) does not support simultaneous use of the same CCS instance by different services, for example, Security Shield 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

Security Shield evaluates calls based on multiple algorithms, such as Fraud, Reason Codes, and Reputation Score.Security Shield gives each call a reputation score and classifies the call as High, Medium, or Low risk. Whenever Security Shield identifies a call as a threat, for example Toll Fraud, 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 Toll Fraud and High 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 Cloud Service (Security Shield). 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 Security Shield 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 Security Shield needs to process and render.

Lookup Requests

By default, Security Shield limits the rate of lookup requests to 50 per second. The lookup service rejects requests that exceed this rate. Security Shield 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:

23.3.1.0.0 - January 2024

The following information describes structural changes to the documentation for the Oracle® Communications Security Shield Cloud Service (Security Shield) 23.3.1.0.0 update.

Security Shield User's Guide

Overview Chapter

- Added “Trusted Enterprise Calls” to the list of what Security Shield does.
- Added new topic: “Other Security Shield Subscriptions”.

Common Controls and Actions Chapter

- Edited the existing topic: "Descriptions of Common Controls and Actions" with an updated image of the avatar panel to show how it looks with the Trusted Enterprise Calls subscription present.

Phone Number Formatting Chapter

- Edited existing topic: “Security Shield Phone Number Format Requirements”.
  - Added: “Important” note for Trusted Enterprise Calls subscribers.

The Dashboard Chapter

- Added bullet #5 about viewing your subscription details.

Outbound Number Management Chapter

- Edited existing topic: “Outbound Number Management” with Trusted Enterprise Call info.
- Edited existing topic: “Outbound Number Management Controls and Actions”.
  - Updated the two screen shots for Trusted Enterprise Calls.

  - Added the two notes about what displays for the Trusted Enterprise Calls subscribers.
- Added new topic: “Trusted Enterprise Calls.”
- Added new topic: “Outbound Call Signing”.
- Added new topic: “Phone Number Format Rules for Outbound Call Signing.”
- Edited existing topic: “Search Operations on the Outbound Numbers List”.
  - Under the “Search with Filter Chips” section, added “Call Signing Enabled”.
- Edited existing topic: “Add a New Phone Number to the Outbound Number Management List”.
  - Added: “Enable Call Signing” attribute to the configuration.
  - Added: “Only the CGBU OCSS Administrator can add, modify, or remove the API key.”
  - Added: “When you enable a phone number for Outbound Call Signing, allow about fifteen days for the service to take effect.
  - Added: “Note: Neustar Customers: When you add a Presentation Number in this configuration, you must also add it to your Neustar list.”
- Edited existing topic: “Edit Phone Number Attributes on the Outbound Number Management List”.
  - Added “Enable Call Signing”.
  - Added:” Only the CGBU OCSS Administrator can add, modify, or remove the API key.”
- Edited existing topic: “Configure Outbound Number Management Settings”.
  - Added the “Trusted Enterprise Call - Attested Call API Key” attribute for BYOL users.

23.3.0.0.0 - November 2023

The following information describes changes to the documentation for the Oracle® Communications Security Shield Cloud Service (Security Shield) 23.3.0.0.0 release.

Security Shield User's Guide

Technical Information Services made the following changes to the *User's Guide*:

- Updated screen captures and text throughout the guide to synchronize with design changes Oracle applied to the Security Shield User Interface.
- Added new topics to the "How Security Shield Works" chapter and updated some existing topics.
- Added the new "Phone Number Formatting" chapter.
- Added the new "Common Controls and Actions" chapter.
- Moved the "Custom Analytics Report" chapter from the Appendix into the main body of the guide.

22.1.0.0.0 - August 2022

The following information describes changes to the documentation for the Oracle® Communications Security Shield Cloud Service (Security Shield) 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 Security Shield Works" chapter.

OCSSC Installation and Maintenance Guide

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

22.0.0.0.0 - May 2022

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

OCSSC User's Guide

- Moves the "Security Shield 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 Cloud Service (Security Shield) 21.3.0.0.0 update.

Security Shield 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 "Security Shield Deployment Overview" chapter.

Security Shield User's Guide

- No structural changes

Security Shield 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 Cloud Service (Security Shield) 21B Update 2 release.

Security Shield Installation and Maintenance Guide

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

Security Shield User's Guide

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

21B Update 1 - August 2021

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

Security Shield 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.

Security Shield 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 Cloud Service (Security Shield) 21B release.

Security Shield Installation and Maintenance Guide

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

Security Shield User's Guide

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